Приложение
к постановлению МПА СНГ
от 23.11.2012 г. № 38-20

Межпарламентская Ассамблея государств – участников Содружества Независимых Государств

РЕКОМЕНДАЦИИ
по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Актуальность разработки Рекомендаций

Информационная глобализация, динамичное развитие процессов интеграции в рамках Содружества Независимых Государств, формирование единого экономического пространства, интенсификация процессов миграции населения и необходимость решения задач в социальной сфере влекут за собой расширение договорно-правовой базы межгосударственного сотрудничества. Обновляются стратегии и концепции национальной безопасности государств – участников СНГ. Это ставит перед правовой системой новые задачи и делает актуальным разработку Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности (далее – Рекомендации).

Рекомендации направлены на установление общих подходов государств – участников СНГ к правовому регулированию обеспечения информационной безопасности, укреплению и обеспечению сбалансированности национальных правовых систем в условиях информатизации общества, на развитие международного информационного обмена, обеспечение безопасности информационных условий экономического и таможенного сотрудничества, на стимулирование использования информационно-коммуникативных технологий в социальной и культурной сфере.

Предлагаемый в Рекомендациях подход к решению проблем правового регулирования в области обеспечения информационной безопасности может способствовать развитию сотрудничества государств – участников СНГ по противодействию другим вызовам и угрозам.

1.2. Правовое основание для разработки Рекомендаций

Правовым основанием для разработки настоящих Рекомендаций послужило ее включение в Комплексный план мероприятий по реализации Концепции сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности на период с 2008 по

2010 год. Разработка Рекомендаций также предусмотрена Перспективным планом модельного законотворчества в Содружестве Независимых Государств на 2011–2015 годы.

Концептуальные подходы к разработке настоящих Рекомендаций основываются на изучении и анализе нормативных актов, основополагающих документов стратегического планирования государств – участников СНГ в сферах обеспечения национальной безопасности, информационной безопасности, защиты государственных секретов, развития информационного общества, противодействия преступлениям в информационной сфере, развития информационной инфраструктуры, деятельности средств массовой информации и др. В основу разработанных концептуальных подходов положены принятые Межпарламентской Ассамблеей государств – участников СНГ (далее – МПА СНГ) модельные законодательные акты, национальное законодательство стран Содружества, а также международно-правовые акты в сфере обеспечения информационной безопасности (в том числе принятые в рамках международных структур: Евразийского экономического сообщества, Шанхайской организации сотрудничества, членами которых являются государства – участники СНГ).

2. ЦЕЛИ И ПРИНЦИПЫ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Цели совершенствования законодательства в сфере обеспечения информационной безопасности

Совместная деятельность государств – участников СНГ в сфере обеспечения информационной безопасности преследует своей целью более эффективную защиту их законных интересов в информационной сфере. Такая деятельность направлена, прежде всего, на создание правовых условий для системной реализации и обеспечения защиты сбалансированных интересов личности, общества и государства в рамках государственной политики развития информационного общества.

Задачи правового регулирования отношений в сфере обеспечения информационной безопасности:

1) выработка наиболее эффективных правовых механизмов комплексного обеспечения информационной безопасности, укрепления законности и правопорядка;

2) совершенствование взаимодействия государств – участников СНГ по обеспечению информационной безопасности, реагирования на информационные вызовы и угрозы;

3) создание условий для равноправного участия государств – участников СНГ в мировых информационных отношениях.

В свете решения указанных задач исключительно важным является вопрос проработки и однозначного толкования правовых дефиниций для сферы информационной безопасности.

2.2. Принципы совершенствования законодательства в сфере обеспечения информационной безопасности

Общими принципами совершенствования **международного (межгосударственного, регионального в рамках Содружества Независимых Государств)** законодательства являются:

– учет и обеспечение интересов государств – участников СНГ в информационной сфере, совместимость с задачами поддержания международной безопасности и стабильности;

– направленность правового регулирования отношений по обеспечению информационной безопасности на обеспечение социального и экономического развития государств;

– обеспечение незыблемости суверенитета и юрисдикции каждого государства – участника СНГ;

– паритетное участие государств – участников СНГ в отношениях по обеспечению информационной безопасности;

– развитие норм международного права в системе законодательства государств – участников СНГ;

– добровольное принятие и исполнение каждым государством – участником СНГ обязательств, касающихся совместного обеспечения информационной безопасности;

– взаимное неприменение мер информационной агрессии и информационной экспансии в межгосударственном сотрудничестве;

– направленность на обеспечение авторитета Содружества Независимых Государств в межгосударственных отношениях при взаимодействии с другими государствами и международными организациями.

Принципами развития **национального** законодательства государств – участников СНГ в сфере информационной безопасности являются:

– сбалансированность прав, свобод и обязанностей личности, общества и государства в сфере обеспечения информационной безопасности;

– свобода создания, сбора, хранения, использования и распространения информации любым законным способом;

– укрепление правовой основы борьбы с преступностью в информационной сфере и противоправным использованием информационно-коммуникационных технологий в экономической и таможенной сферах;

– согласованность норм национального законодательства и норм международного права, регулирующих отношения в сфере обеспечения информационной безопасности;

– гармонизация и интеграция с международными системами информационной безопасности;

– открытость деятельности по обеспечению информационной безопасности, предусматривающая информирование общества об обеспечении информационной безопасности с учетом ограничений, установленных законодательством.

Специальным принципом совершенствования законодательства государств – участников СНГ является «*безопасность через развитие*», что предполагает динамичное совершенствование правовых методов обеспечения информационной безопасности по мере развития информационного общества.

Поскольку в качестве общей угрозы информационной безопасности могут рассматриваться недостаточный уровень сформированности интересов личности, общества и государства или отставание в темпах их формирования, в качестве одного из показателей информационной безопасности следует рассматривать стабильную положительную динамику социальных индикаторов реализации базовых интересов личности, общества и государства. В частности, достижение намеченного уровня индикаторов оценки информационного обеспечения реализации государственной политики будет свидетельствовать о ее эффективности.

3. ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ СОТРУДНИЧЕСТВА ГОСУДАРСТВ – УЧАСТНИКОВ СНГ В ЦЕЛЯХ СОВЕРШЕНСТВОВАНИЯ И ГАРМОНИЗАЦИИ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Синхронизация механизмов обеспечения информационной безопасности

Гармонизацию законодательства в сфере обеспечения информационной безопасности предлагается рассматривать на трех уровнях:

1) концептуально-научном (в рамках выработки концепций, рекомендаций, доктрин информационной безопасности);

2) международном и региональном (разработка модельного законодательства, подготовка и заключение межгосударственных договоров и соглашений);

3) национальном (развитие и совершенствование национального законодательства в соответствии с общими концептуальными подходами, приведение его в соответствие с модельным законодательством МПА СНГ, ратификация достигнутых соглашений).

Интересы сотрудничества государств – участников СНГ требуют обеспечения совместимости национальных векторов информационного развития и приоритетных направлений обеспечения информационной безопасности. Анализ действующего национального законодательства государств – участников СНГ, модельного законодательства МПА СНГ, а также международных документов и соглашений в области информационной безопасности позволяет сделать вывод о целесообразности совершенствования законодательства государств – участников СНГ по следующим направлениям:

– обеспечение правового регулирования в информационной сфере;

– соблюдение конституционных прав и свобод человека и гражданина в области поиска, получения и использования информации;

– развитие безопасного информационного обмена;

– совершенствование информационного обеспечения развития гражданского общества;

– совершенствование информационного обеспечения межгосударственного сотрудничества;

– совершенствование механизмов согласования юрисдикций в глобальном информационном пространстве;

– совершенствование информационного обеспечения инновационного развития;

– совершенствование информационной инфраструктуры, обеспечение ее безопасности;

– обеспечение безопасности критически важных объектов информационно-телекоммуникационной инфраструктуры;

– защита государственных секретов и противодействие иностранным техническим разведкам.

Механизмы правового регулирования обеспечения информационной безопасности необходимо выстраивать в согласовании с методологией правового регулирования обеспечения национальной (региональной, международной) безопасности. Система обеспечения информационной безопасности государств – участников СНГ должна строиться в контексте глобальных тенденций развития экономических отношений и социальных процессов.

Важными задачами являются: обеспечение функционирования средств массовых коммуникаций, культурного обмена и формирование совместных структур в этой области; создание средств защиты от информации, способной нанести ущерб социально-психическому здоровью граждан (включая оказание возможного влияния на качество контента в Интернет-среде); обеспечение взаимного признания документов, подтверждающих право на получение образования и полученную квалификацию граждан в научно-образовательных системах учреждений государств – участников СНГ и др.

3.2 Унификация понятийно-категориального аппарата

3.2.1. Расширение и углубление сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности сопровождается расширением соответствующей терминологии. Свои позиции и планы действий в области международной информационной безопасности государства – участники СНГ определяют также в рамках других международных организаций (Евразийского экономического сообщества, Организации Договора о коллективной безопасности, Шанхайской организации сотрудничества и др.). За два десятилетия существования Содружеств Независимых Государств разработано и принято большое число модельных законодательных и иных правовых актов. При этом терминологическое многообразие и слабая определенность используемого в различных документах понятийного аппарата становится все более актуальной проблемой. Термины и их определения приводятся, как правило, «*в целях настоящего нормативного акта*», что чревато коллизиями норм. Опре-

деленные трудности для практической деятельности создают также многоязычие и отсутствие на сегодняшний день поверенного аутентичного перевода полноценных информационных баз национальных правовых актов.

Для согласованных политических действий и в целом конструктивного межгосударственного взаимодействия требуются определенность и однозначность понятийного аппарата. Следовательно, необходимы разработка общей системы терминов и их определений, закрепление их в нормативных актах и общественном обращении, а также их толкование. С учетом этого в ноябре 2011 года Экспертный совета МПА СНГ – РСС принял решении о подготовке Глоссария в сфере обеспечения информационной безопасности.

3.2.2. В целях настоящих Рекомендаций необходимы унификация и единообразная трактовка в нормативно-правовой базе государств – участников СНГ основных терминов и понятий, используемых в процессе нормативно-правового регулирования и сотрудничества в области обеспечения информационной безопасности. На основе анализа доктринальных положений и норм национального законодательства следует сформировать общий понятийный аппарат и опереться на него при разработке Стратегии информационной безопасности для государств – участников СНГ. Особое внимание при этом следует уделить содержательному наполнению таких основных понятий, как «информационная сфера», «информационная среда», «информационное пространство», «информационная безопасность», «обеспечение информационной безопасности».

В настоящее время нормативно-правовая база Содружества Независимых Государств включает в себя два отличающихся друг от друга определения понятия «информационная безопасность». Модельный закон МПА СНГ «О международном информационном обмене» (2002 год) определяет информационную безопасность как «*состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства*».

Концепция сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, утвержденная Советом глав государств СНГ в 2008 году, трактует информационную безопасность как «*состояние защищенности от внешних и внутренних угроз информационной сферы, формируемой, развиваемой и используемой с учетом жизненно важных интересов личности, общества и государства*». (Внимание здесь акцентируется, в первую очередь, на объект – информационную сферу).

В указанной Концепции превалирует узкий, «технократический», подход, при котором сама проблема информационной безопасности искусственно сужается до задач защиты информации. (Показательно, что первой в перечне угроз информационной безопасности при этом указана угроза осуществления действий в интересах «*получения несанкционированного доступа к информации*».) Большинство понятий в тексте Концепции относятся, прежде всего, к задачам защиты информации. В связи с этим необходимо исходить из того, что информационная безопасность является принципиально более широким понятием.

В свете задач обеспечения информационной безопасности, стоящих перед государствами – участниками СНГ, наиболее адекватным решением может стать использование содержательного наполнения понятия «информационная безопасность» в трактовке, закрепленной в тексте Соглашения между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 2009 год): «Информационная безопасность – состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве».[1]

Это базовое понятие охватывает наиболее актуальные угрозы социально-гуманитарного плана, в частности угрозу распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде государства. Источниками подобных угроз могут являться как государственные, так и негосударственные структуры, а также частные лица. Признаки таких угроз – появление и тиражирование в средствах массовой информации (включая электронные), в сетях информационного обмена (Интернет и др.) информации, которая искажает представление о политической системе, общественном строе, внешней и внутренней политике, важных политических и общественных процессах в государстве, духовных, нравственных и культурных ценностях его населения; информации, которая пропагандирует идеи терроризма, сепаратизма и экстремизма, разжигает межнациональную, межрасовую и межконфессиональную вражду.

3.2.3. Обеспечение информационной безопасности традиционно рассматривается как непрерывная деятельность соответствующих органов, организаций и уполномоченных лиц, состоящая в реализации комплексных правовых, организационных, технологических и технических мер, предусматривающих безопасное функционирование всей информационной инфраструктуры, государственного управления, а также средств информационно-коммуникационных технологий, которыми пользуются граждане и другие субъекты гражданского общества каждого государства – участника СНГ и структуры, обеспечивающие информационное взаимодействие этих государств между собой.

Информационное общество понимается как общество гражданское, социальное, демократическое и правовое. В силу этого в условиях глобализации и открытых телекоммуникаций большую роль в обеспечении информационной безопасности призваны сыграть институты гражданского общества. Состояние информационной безопасности во многом будет зависеть от уровня информационной культуры гражданского общества. Необходимым условием устойчивого развития является медиа- и информационная грамотность населения.

3.2.4. Исходя из парадигмы: «***общие лексические формы — базис для взаимопонимания***», учитывая возрастание опасности информационной преступности и информационного терроризма в национальном и международном

[1] В числе подписавших Соглашение государств пять стран – участниц СНГ: Республика Казахстан, Кыргызская Республика, Российская Федерация, Республика Таджикистан и Республика Узбекистан.

масштабе и повышение актуальности проблем международной информационной безопасности, представляется целесообразным дополнить Концепцию сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, включив в нее дополнительно **ряд понятий из области международной информационной безопасности**.

В число таких понятий целесообразно включить, как минимум, следующие (приводятся в алфавитном порядке):

информационная война;
информационная инфраструктура;
информационная преступность;
информационное оружие;
информационное пространство;
информационный терроризм;
критически важные структуры;
международная информационная безопасность;
неправомерное использование информационных ресурсов;
несанкционированное вмешательство в информационные ресурсы[2]

Унификация понятийно-категориального аппарата должна рассматриваться как одно из приоритетных направлений совершенствования законодательства и правоприменения. При этом унификацию терминов следует осуществлять в отношении всех нормативных правовых актов, предметом правового регулирования которых являются информационные отношения и обеспечение информационной безопасности. При толковании понятий, которые еще не включены в национальное законодательство, но уже содержатся в модельных законодательных актах, представляется рациональным рекомендовать государствам – участникам СНГ использовать положение последних.

При уточнении содержательного наполнения (и возможном расширении перечня) понятий, согласовании, одобрении и переводах на национальные языки, а также дополнении перечня понятий терминами, используемыми в национальном законодательстве, может быть сформирован многоязычный терминологический словарь по информационной безопасности для государств – участников СНГ. Наличие такого словаря-тезауруса представляется исключительно полезным, прежде всего для законотворческой деятельности и правоприменительной практики.

3.3. Совершенствование правовых механизмов обеспечения информационной безопасности

3.3.1. В качестве концептуальной основы правового регулирования в сфере обеспечения информационной безопасности предлагается рассматривать за-

[2] Определение этих понятий закреплены в тексте Соглашения между правительствами государств – членов Шанхайской организации сотрудничества.

щиту конституционных прав и интересов всех субъектов правовых отношений. Для гражданина – это, прежде всего, возможность реализации его конституционных прав и свобод. Для общества – это развитие гражданского общества в информационной сфере, его социальная функция. Для государства – эффективная реализация государственной политики и международного сотрудничества. Одним из важнейших направлений взаимодействия государств – участников СНГ является обеспечение безопасности международного информационного обмена (включая его электронные формы).

Основным правовым средством согласования, гармонизации механизмов правового регулирования информационных отношений представляется объединение правового регулирования по определенным направлениям в единый правовой статус (личности, общества и государства). Правовой информационный статус понимается как интегрированная совокупность возможностей реализации субъектом своих прав и обязанностей во всех видах информационных отношений.

3.3.2. Правовой информационный статус личности предусматривает:

– реализацию конституционных прав и свобод гражданина в области получения информации и пользования ею;

– обеспечение права на получение, хранение и распространение полной, достоверной и своевременной информации любым законным способом;

– защищенность от незаконного вмешательства в личную жизнь;

– обеспеченность реализации права на использование и защиту персональных данных при соблюдении правил самоидентификации личности;

– возможность реализации и защиты прав интеллектуальной собственности;

– право на информационное участие в государственном управлении;

– возможность реализации права на «электронную занятость»;

– возможность реализации права на дистанционное («электронное») образование;

– возможность реализации права на «электронное здравоохранение»;

– обеспечение реализации права на социальную защиту и др.

3.3.3. Правовой информационный статус «безопасное информационное общество» должен иметь следующие черты:

– способствовать укреплению демократии; сохранять духовные и нравственные ценности (традиции, культурные ценности) общества, развивать его интеллектуальный и духовно-нравственный потенциал;

– способствовать реализации институтами гражданского общества своей деятельности и свободному распространению в обществе информации о данной деятельности;

– обеспечивать получение общедоступной информации о социальных, экономических и политических процессах, состоянии окружающей среды, демографической обстановке и др.;

– способствовать ведению бизнеса с использованием информационно-коммуникационных технологий, безопасному развитию электронной торговли;

– противостоять деструктивному информационному влиянию на общественное и индивидуальное сознание, насаждению чуждых ценностей и ориентиров.

Согласование и гармонизация механизмов правового регулирования информационных отношений в целях обеспечения безопасности должны осуществляться с учетом стратегий национальной безопасности государств – участников СНГ.

3.3.4. Правовой информационный статус субъектов, обеспечивающих безопасность государства и его суверенитет в информационном пространстве, определяет самостоятельность государства – участника СНГ в осуществлении своих функций в области соблюдения законных прав и свобод граждан, обеспечения национальной и коллективной безопасности. Этот статус нацелен:

– на информационное обеспечение реализации государственной политики, повышение эффективности и безопасности функционирования государственных институтов;

– информационное обеспечение международного сотрудничества, укрепление правовой основы реализации информационной политики, реальное расширение равноправного участия государств – участников СНГ в мировых информационных процессах и создании интегрированной системы обеспечения информационной безопасности;

– реализацию законности правоотношений в информационной сфере, соблюдение законов информационного общества: уважение интеллектуальной собственности, прав на доступ к информации, порядка информационного обмена, законности информационных экономических сделок и др.

– обеспечение инновационного развития государств на основе создания современных информационных технологий, инфраструктуры и производства информационных услуг и других видов информационного взаимодействия;

– построение и безопасное развитие информационной инфраструктуры, создающей технологическую основу государственного управления (в мирное время, в чрезвычайных ситуациях и в военное время) и способствующей взаимодействию государств – участников СНГ в информационной сфере;

– обеспечение безопасности функционирования информационных технологий на критически важных объектах информационно-телекоммуникационной инфраструктуры, способных обеспечить надежность и устойчивость функционирования таких объектов;

– обеспечение сохранности государственных секретов государств − участников СНГ.

3.3.5. Средством согласования и гармонизации безопасности механизмов обеспечения информационной безопасности является комплексная интегрирующая категория «стандарт информационной безопасности». Под стандартом информационной безопасности понимается совокупность правовых, организационных, технических и технологических средств и методов, результатом применения которых является надлежащее обеспечение безопасности информационной инфраструктуры.

Средства, методы и формы правового и организационного взаимодействия в процессе обеспечения совершенствования законодательства в области обеспечения информационной безопасности должны быть нацелены на решение следующих задач:

а) согласование хода работы по сближению и совершенствованию законодательства государств в области обеспечения информационной безопасности;

б) установление единых правил учета и систематизации угроз, форм их реализации, степени нарушения законодательства и рейтинга эффективности обеспечения информационной безопасности;

в) разработка общей модели классификации операций и процедур разрешения возникающих разногласий при обсуждении и принятии решений в области обеспечения информационной безопасности.

Динамичное развитие информационных средств и технологий со всей очевидностью требует эволюции стандартов информационной безопасности, их правового оформления, а также обязательности применения. В связи с этим перспективными представляются следующие практические подходы.

1. Использование матричной формы классификации предметных областей информационных отношений, учета рисков правонарушений в области обеспечения информационной безопасности.

С ориентацией на формирование информационных стандартов и законодательства может быть построена примерная матрица правового регулирования групп информационных отношений. Этот метод анализа позволит выявить пробелы и противоречия в регулировании обеспечения информационной безопасности.

Работа в сфере обеспечения информационной безопасности должна быть в большей степени ориентирована на модельное законодательство МПА СНГ. На этом пути системное дополнение национального законодательства государств – участников СНГ может реализовываться в соответствии с общим (разработанным и принятым в рамках Содружества Независимых Государств) межгосударственным (региональным) стандартом правового регулирования безопасности личности, общества и государства.

2. Создание единой автоматизированной системы управления (АСУ обеспечения информационной безопасности) в целях автоматизации учета, анализа и оценки состояния и динамики борьбы с правонарушениями в области информационной безопасности.

3. Системное обобщение и заимствование передового зарубежного опыта в области правового обеспечения информационной безопасности.

В рамках осуществления деятельности по совершенствованию и гармонизации законодательства государств – участников СНГ в сфере обеспечения информационной безопасности целесообразно усилить научно-методическую составляющую, а также разработать правовую форму межгосударственного и межведомственного обмена информацией о методах обеспечения информационной безопасности. В этих целях представляется полезной разработка Соглашения о сотрудничестве по организации межгосударственного обмена инфор-

мацией в сфере обеспечения информационной безопасности, мониторинга законодательства и практики правоприменения.

4. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЕ РЕШЕНИЯ

1. Рекомендации предполагают организационное и методологическое обоснование взаимосвязи функции гражданского строительства информационного общества и функции обеспечения информационной безопасности. Исходя из такого подхода, представляется целесообразным:

– проработать вопрос о создании организации национальных субъектов, отвечающих за обеспечение информационной безопасности;

– разработать типовой регламент административных процедур, осуществляемых уполномоченными органами в сфере информационной безопасности.

2. Принимая во внимание, что система отношений по обеспечению информационной безопасности вторична по отношению к базовым системам экономических, политических и социальных отношений государств – участников СНГ, представляется целесообразным построение системы информационной безопасности соотносить с векторами развития базовых систем, что позволит преодолеть существующий методологический вакуум и создать модель динамического отслеживания угроз, вызовов и запросов общества. Необходимость построения в интересах государств − участников СНГ гармонизированной системы обеспечения информационной безопасности требует укрепления связей в области доктринального, концептуального и политико-правового обеспечения информационной безопасности.

Для придания правовым мерам обеспечения информационной безопасности целенаправленности следует использовать подходы стратегического планирования и начать подготовку Стратегии обеспечения информационной безопасности для государств – участников СНГ. Концептуально такая Стратегия должна быть нацелена на обеспечение решения задач устойчивого развития информационных отношений, на обеспечение надежной защиты и препятствование реализации угроз жизненно важным интересам личности, общества и государства в информационной сфере, на обеспечение способности и готовности базовых систем экономических, политических, социальных и иных отношений государств − участников СНГ продуктивно использовать технологический и человеческий потенциал в развитии своих стран и Содружества в целом.

Для разработки и реализации Стратегии информационной безопасности для государств – участников СНГ видится целесообразным создание рабочего органа – Комиссии по информационной безопасности.

3. В целях совершенствования межгосударственного взаимодействия представляется актуальной разработка модельного регламента административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников СНГ. Такой регламент может включать процедуры, связанные:

− с организацией безопасного документооборота;

− с защитой охраняемой информации;

− с обеспечением прав граждан на участие в государственном управлении, на здравоохранение, образование, социальную защиту, права на обращение в государственные органы;

− с защитой от деструктивного информационного воздействия;

− со свободой поиска и распространения информации, в частности с обеспечением свободы средств массовой информации;

− с профилактикой и противодействием преступлениям против информационной безопасности, включая разработку классификаторов угроз, мониторинг индикаторов оценки состояния информационной безопасности и др.

4. Наряду с разработкой Стратегии информационной безопасности для государств – участников СНГ представляются актуальными подготовка модельного закона «О критически важных объектах информационно-коммуникационной инфраструктуры», внесение изменений в модельный закон «Об информации, информатизации и защите информации» и дополнений в модельный Уголовный кодекс для государств – участников Содружества Независимых Государств.

В целях создания гармонизированного законодательства по борьбе с киберпреступлениями действенной правовой мерой сближения и совершенствования законодательства государств – участников СНГ могла бы стать криминализация в модельном Уголовном кодексе отдельных видов деяний, направленных против порядка эксплуатации объектов информационной инфраструктуры. Преступления против информационной безопасности представляется рациональным выделить в отдельную главу модельного Уголовного кодекса для государств – участников Содружества Независимых Государств.

5. В силу того, что информационная безопасность это многоаспектная категория, интегрирующая результаты функционирования разновекторных систем, актуальным в настоящее время является насыщение правоохранительных структур квалифицированными кадрами (в частности, актуальна задача обучения судей, прокуроров и сотрудников правоохранительных органов по вопросам противодействия киберпреступности, использования электронных доказательств и др.). В связи с этим, с учетом новизны и прогрессирующей тенденции роста киберпреступности, не теряет своей актуальности разработка типовых образовательных стандартов (программ) в сфере подготовки, переподготовки и повышения квалификации кадров в области информационной безопасности.

Приняты на тридцать восьмом
пленарном заседании
Межпарламентской Ассамблеи
государств – участников СНГ
(постановление № 38-20 от 23 ноября 2012 года)