П О С Т А Н О В Л Е Н И Е

Парламентской Ассамблеи
Организации Договора о коллективной безопасности

О проекте
Рекомендаций по сближению и гармонизации национального законодательства государств – членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности

Парламентская Ассамблея Организации Договора о коллективной безопасности п о с т а н о в л я е т:

1. Принять Рекомендации по сближению и гармонизации национального законодательства государств – членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности (прилагаются).

2. Направить Рекомендации по сближению и гармонизации национального законодательства государств – членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности (далее – Рекомендации) в парламенты государств – членов ОДКБ и рекомендовать их для использования в работе по совершенствованию законодательства государств – членов Организации в соответствующей сфере.

3. Разместить Рекомендации на сайте и опубликовать в печатных материалах Парламентской Ассамблеи ОДКБ.

Председатель
Парламентской Ассамблеи ОДКБ **С. Е. Нарышкин**

Санкт-Петербург
27 ноября 2014 года
№ 7-6

Приложение
к постановлению ПА ОДКБ
от 27 ноября 2014 г. № 7-6

РЕКОМЕНДАЦИИ
по сближению и гармонизации национального законодательства государств – членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности

I. Общие положения

1.1 Основание для разработки Рекомендаций

Правовым основанием для разработки проекта Рекомендаций по совершенствованию и гармонизации национального законодательства государств – членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности (далее — Рекомендации) служит включение их разработки в Комплексный план мероприятий Программы деятельности ПА ОДКБ по сближению и гармонизации национального законодательства государств – членов ОДКБ на 2011-2015 гг.

Концептуальные подходы к разработке Рекомендаций выработаны на основе анализа действующих нормативных актов, концептуально-доктринальных документов и документов стратегического планирования ОДКБ и государств – членов в сферах обеспечения информационной безопасности, включая вопросы защиты государственных секретов, противодействия преступлениям против информационной безопасности, вопросы развития информационной инфраструктуры, деятельности средств массовой информации в условиях развития информационного общества.

1.2 Цель Рекомендаций

Рекомендации направлены на установление общих подходов государств – членов ОДКБ к правовому обеспечению информационно-коммуникационной безопасности жизнедеятельности общества. Сбалансированность системы обеспечения информационно-коммуникационной безопасности должна быть направлена на стимулирование информационного развития и международного информационного обмена, обеспечение информационных условий экономического и таможенного, научно-технического и культурного сотрудничества, а также на повышение эффективности обеспечения национальной безопасности государств – членов ОДКБ.

В современном обществе информационно-коммуникационная безопасность является важнейшим компонентом национальной безопасности. Данное положение обусловлено рядом обстоятельств:

1) информационная сфера приобрела статус системообразующей, и от нее в значительной степени зависит уровень экономического, социального и политического развития общества и государства;
2) негативные последствия угроз и правонарушений в области информационной безопасности существенно влияют на национальную безопасность государств в политической, экономической, военной и иных сферах;
3) значительный прогресс в развитии и внедрении новейших информационно-коммуникационных технологий и средств коммуникации повлек за собой угрозы и риски, связанные с возможностями использования таких технологий и средств как в гражданской, так и в военной сферах в целях, несовместимых с задачами поддержания международного мира, безопасности и стабильности;
4) интеграция в единые комплексы автоматизированных систем управления производственными и транспортными структурами, административными и финансовыми ресурсами повлекла за собой возникновение нового класса критически важных объектов инфраструктуры – объектов информационно-коммуникационной инфраструктуры (КВОИ);
5) анализ существующих вызовов и угроз на пространстве государств – членов ОДКБ показывает, что в современных условиях возрастает опасность возникновения кризисных ситуаций и совершения противоправных деяний с применением современных информационных и коммуникационных технологий.

С учетом сказанного особую актуальность приобретают вопросы формирования активной согласованной информационной политики государств – членов ОДКБ, развития общего информационного пространства, создания совместного потенциала по противодействию информационным угрозам правам и свободам граждан и интересам государства и общества, защищенности информационных ресурсов и коммуникаций органов ОДКБ, национальных органов власти и управления.

II. Угрозы и состояние организационно-правового обеспечения информационно-коммуникационной безопасности в ОДКБ

Проблема информационно-коммуникационной безопасности носит комплексный характер. Её решение требует системного использования законодательных, организационных, технологических, административных и иных мер обеспечения безопасности.

Общими угрозами информационно-коммуникационной безопасности, в соответствии с доктринальными документами государств – членов ОДКБ, являются:

- отставание в развитии информационной инфраструктуры, формировании информационного пространства, создании аппаратных и программных средств, что негативно отражается на эффективности национальных систем обеспечения информационной безопасности;

- деструктивное информационное воздействие на личность, общество и государство, оказываемое с использованием информационно-коммуникационной инфраструктуры;

- нарушение безопасного, стабильного функционирования критически важных информационных инфраструктур;

- несанкционированный доступ к охраняемой в соответствии с законом информации;

- рост преступности с использованием ИКТ.

Проблема обеспечения информационно-коммуникационной безопасности государств – членов ОДКБ тесно связана с категорией суверенитета и юрисдикции государств, что с необходимостью требует согласования систем организационного и правового обеспечения информационно-коммуникационной безопасности в контексте обеспечения национальной и международной (региональной) безопасности государств – членов ОДКБ.

В настоящее время невыстроенность в правовых актах национального законодательства и межгосударственных соглашениях государств – членов ОДКБ иерархичной системы субъектов (сил) обеспечения информационно-коммуникационной безопасности существенно сказывается на обеспечении безопасности как на национальном, так и на международном (региональном) уровнях.

Содержание, вкладываемое в широко используемое в обороте понятие «*информационная безопасность*», на практике зачастую сужает его до технических аспектов защиты информации, при этом опускаются, прежде всего, социально-гуманитарные аспекты межличностной коммуникации. Нормативное регулирование в таком случае становится, по сути, техническим и направленно преимущественно на стандартизацию технологических процессов, удаляясь от нормативного обеспечения общественных отношений. В силу чего само правовое регулирование процессов обеспечения информационно-коммуникационной безопасности естественно сужается.

Слабая разработанность и отсутствие в настоящее время единого понимания понятийно-категориального аппарата в сфере информационно-коммуникационной безопасности в международных правовых актах и в национальном законодательстве государств – членов ОДКБ, аморфность механизма выработки единых решений в её рамках ставят под сомнение саму возможность успешной гармонизации законодательства.

III. Общие подходы к сближению законодательства государств – членов ОДКБ в сфере информационно-коммуникационной безопасности

Предлагаемый алгоритм сближения законодательства государств-членов ОДКБ в сфере информационно-коммуникационной безопасности должен включать следующую последовательность шагов:

3.1 Определение стратегической цели обеспечения информационно-коммуникационной безопасности ОДКБ

В качестве основной цели постулируется обустройство единого безопасного информационного пространства, как объединенного сегмента информационных пространств государств – членов ОДКБ. Такое информационное пространство поддерживается общегосударственными информационными инфраструктурами, в нём осуществляется оборот информации, необходимой для выполнения уставных задач ОДКБ, и обеспечиваются условия национальной безопасности государств – её членов.

3.2 Определение основных направлений обеспечения информационно-коммуникационной безопасности государств – членов ОДКБ, исходя из уставных задач Организации и складывающейся обстановки в информационно-коммуникационной сфере

Такими направлениям являются:

3.2.1 Общие вопросы организации обеспечения информационной безопасности;

3.2.2 Защита информационных ресурсов;

3.2.3 Противодействие преступлениям в информационной сфере *(в т.ч. информационному терроризму);*

3.2.4 Информационное обеспечение реализации государственной политики;

3.2.5 Защита личности, общества и государства от деструктивного информационного воздействия;

3.2.6 Защита единого информационного пространства;

3.2.7 Обеспечение безопасности информационно-коммуникационной инфраструктуры (*включая обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры — КВОИ*).

3.3 Сближение и гармонизация законодательства государств-членов ОДКБ по каждому из перечисленных выше направлений предполагает унификацию правового обеспечения информационно-коммуникационной безопасности по следующим категориям:

1) ***разработка системы организационных мер обеспечения информационно-коммуникационной безопасности.*** Система указанных мер должна включать:
   - согласование выделенных приоритетных направлений обеспечения информационной безопасности государствами – членами ОДКБ;
   - унификацию понятийно-категориального аппарата в сфере обеспечения информационно-коммуникационной безопасности;
   - синхронизацию механизмов обеспечения информационно-коммуникационной безопасности;
   - организационное обеспечение координации усилий по обеспечению информационно-коммуникационной безопасности в рамках ОДКБ.
2) ***выработка концептуальных подходов правового обеспечения информационно-коммуникационной безопасности.*** Определение стандарта правовой обеспеченности информационно-коммуникационной безопасности государства – члена ОДКБ, достижение которого на национальном уровне будет свидетельствовать о юридической совместимости национальных сегментов информационного пространства и информационной инфраструктуры в целях правового обеспечения безопасности оборота информационных ресурсов. Такой стандарт на национальном уровне должен включать в себя:
   - документ стратегического планирования, определяющий цель и задачи обеспечения информационно-коммуникационной безопасности, а также унифицированный в рамках ОДКБ понятийный аппарат в сфере обеспечения информационно-коммуникационной безопасности;
   - сформированную систему правовых предписаний и запретов, определяющих правила безопасного поведения в информационно-коммуникационной сфере, в том числе, криминализацию деяний, посягающих на национальные интересы;
   - сформированную систему субъектов обеспечения государственной политики в информационной сфере и разработанность организационно-правовых механизмов их деятельности.
3) ***разработка системы практических мер нормативно-правового обеспечения информационно-коммуникационной безопасности на национальном уровне.*** Определение стандарта нормативного обеспечения информационно-коммуникационной безопасности государства – члена ОДКБ, позволяющего обеспечить реализацию на национальном уровне уставных задач по обеспечению

информационно-коммуникационной безопасности в ОДКБ. Такой стандарт должен включать:

- достижение уровня нормативного регулирования всех сформировавшихся на современном этапе групп однородных общественных отношений, (в рамках перечисленных выше в п.п. 3.2.1 – 3.2.6 направлений обеспечения информационно-коммуникационной безопасности для государств-членов ОДКБ). Предполагается, что на современном этапе сближению и гармонизации законодательства государств – членов ОДКБ в сфере информационно-коммуникационной безопасности способствовал бы подход, при котором в рамках каждого из выделенных направлений отношения в сфере информационно-коммуникационной безопасности регулировались специальным законом (в дальнейшем, с принятием государствами – членами ОДКБ Информационных кодексов данная позиция утратит силу);
- конституционную закрепленность информационных отношений, возникающих по поводу обеспечения безопасности базовых прав и интересов взаимодействующих субъектов;
- нормативную регламентацию системы субъектов обеспечения информационно-коммуникационной безопасности;
- готовность государств – членов ОДКБ к наращиванию усилий по подписанию и ратификации основных соглашений в сфере обеспечения информационно-коммуникационной безопасности.

4) ***разработка системы практических мер законодательного обеспечения информационно-коммуникационной безопасности на национальном уровне.*** Определение стандарта законодательной обеспеченности информационно-коммуникационной безопасности государств-членов ОДКБ на национальном уровне. Данный стандарт должен определять общие согласованные подходы к развитию и совершенствованию законодательства по следующим направлениям:
   - законодательство об информации;
   - законодательство о конфиденциальной информации и тайнах;
   - законодательство о средствах массовой информации и рекламе;
   - законодательство в сфере интеллектуальной собственности;
   - законодательство о безопасности информационной деятельности;
   - законодательство о связи и телекоммуникациях;

- законодательство о безопасности функционирования информационных и телекоммуникационных систем, сетей связи, средств информатизации обработки информации;
- законодательство о системе органов обеспечения информационной безопасности;
- специальное законодательство о правовом статусе субъектов информационной сферы (таких, например, как организации и органы государственной власти);
- законодательство о юридической ответственности за виновное нарушение норм, регулирующих отношения в области противодействия угрозам информационной безопасности, находящихся в составе нормативных правовых актов различных отраслей национального законодательства.

5) ***формирование системы мер правового обеспечения информационно-коммуникационной безопасности на международном уровне***.

IV. Основные направления обеспечения информационно-коммуникационной безопасности государств-членов ОДКБ

4.1 Общие вопросы организации обеспечения информационно-коммуникационной безопасности

В современной ситуации объективно существует необходимость разработки и нормативного закрепления системы мер и механизмов обеспечения международной информационной безопасности и порядка принятия коллективных мер по противодействию угрозам в информационной сфере. Осуществление противодействие таким угрозам потребует разработки системы показателей и характеристик информационно-коммуникационной безопасности ОДКБ в наиболее важных сферах, разработки механизма их мониторинга.

Понятие «*информационная безопасность*» нашло своё отражение в политических документах ОДКБ (2010 г.) и СНГ (2013 г.) в следующей формулировке: «*состояние защищенности интересов личности, общества и государства от угроз и иных деструктивных воздействий в информационном пространстве*», совпадающей с закреплённой в межправительственном Соглашении в области обеспечения международной информационной безопасности государств – членов Шанхайской организации сотрудничества (ШОС, 2009 г.). В этом Соглашении ШОС нашло своё отражение и понятие «*международная информационная безопасность*» как состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.

В Основах государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года понятие «*международная информационная безопасность*» используется в следующей трактовке: «*состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры*».

ОДКБ – региональная международная организация, её целями являются укрепление мира, международной и региональной безопасности и стабильности.

С прагматических позиций, в целях настоящих Рекомендаций предлагается рассматривать «*информационно-коммуникационную безопасность государств-членов ОДКБ*» как такое состояние информационного пространства ОДКБ, при котором исключены возможности нарушения прав личности, общества и интересов государств-членов Организации Договора о коллективной безопасности в информационной сфере, а также деструктивного и противоправного воздействия на элементы совместной информационной инфраструктуры ОДКБ и национальных критических информационных инфраструктур государств – членов ОДКБ.

Правовой статус субъекта правоотношений в области информационной безопасности – при этом понимается как интегрированная совокупность нормативно закрепленных прав и обязанностей субъекта во всех видах информационных отношений.

На национальном уровне правового обеспечения информационно-коммуникационной безопасности в государствах – членах ОДКБ требуется структурно упорядочить нормативные правовые акты, провести их систематизацию. Необходимо определить структурный необходимый минимум критериев, образующих информационную безопасность (в качестве таковых могут рассматриваться, например: «*защита информационных ресурсов*»; «*противодействие преступлениям в информационной сфере*»; «*противодействие кибертерроризму*»; «*информационное обеспечение реализации государственной политики*»; «*защита информационного пространства*»; «*обеспечение безопасности информационно-коммуникационной инфраструктуры*»; «*обеспечение безопасности КВОИ*»). При этом следует упорядочить юридические термины, используемые в нормативных правовых актах. В целях сближения и единства лексических форм терминология правовых актов, принимаемых в одной сфере, не должна существенно отличаться, следует стремиться к обеспечению преемственности используемого понятийного и терминологического аппарата.

Сближение и гармонизацию законодательства государств-членов ОДКБ представляется рациональным осуществлять «сверху-вниз»: от

международного акта — к национальным, поскольку сегодня отсутствует эталонная национальная правовая система, правовые регуляторы которой можно было бы взять за основу. Реализация такой задачи потребует создания эффективного механизма для совершенствования нормативно-правовой базы и устранения пробелов в национальном законодательстве.

Новизна, сложность и слабая определенность возникающих задач требуют совершенствования системы органов обеспечения информационной безопасности. Вероятно, в рамках ОДКБ будет полезным создание:

1) центра информационной безопасности государств – членов ОДКБ;
2) ситуационного центра Организации Договора о коллективной безопасности по мониторингу социальных сетей и открытых источников информации — с целью прогноза развития обстановки в зоне ответственности ОДКБ и прилегающих регионах;
3) информационно-аналитического центра ОДКБ.

Рациональным представляется создание на базе рабочих групп по информационной безопасности и информационной политике при Комитете Секретарей Советов безопасности (КССБ) постоянного рабочего органа — организационной структуры из представителей компетентных государственных органов, отвечающих за обеспечение информационной безопасности.

Самостоятельный интерес представляет проработка и формализация вопросов взаимодействия с другими международными структурами в сфере обеспечения информационной безопасности.

Заслуживают внимания проработка вопросов подготовки международного правового акта о взаимодействии государств – членов ОДКБ в информационной сфере и разработка Концепции сотрудничества государств – членов ОДКБ по противодействию современным угрозам в информационной сфере. Представляется, что в таких документах должны найти свое отражение вопросы развития системы субъектов по международной информационной безопасности и подготовки принятия единого стандарта для государств – членов ОДКБ по правовому обеспечению вопросов информационной безопасности.

4.2 Защита информационных ресурсов

С позиций защиты информационных ресурсов для государств – членов ОДКБ не перестают быть актуальными такие угрозы как несанкционированный доступ к охраняемой в соответствии с законом информации и деятельность иностранных разведок по похищению государственных секретов.

Актуальными сегодня задачами являются разработка общих критериев совместимости способов хранения и использования общих информационных ресурсов государств – членов ОДКБ, а также создание системы обеспечения безопасности электронного документооборота. Правоприменительная

практика требуется согласованного толкования таких понятий как «*неправомерное использование информационных ресурсов*», «*несанкционированное вмешательство в информационные ресурсы*», «*конфиденциальная и секретная информация*» и др.

Защита информационных ресурсов на национальном уровне требует:

а) создания эффективной системы правового обеспечения защиты информационных ресурсов государственного значения всех видов;

б) приведения национального законодательства государств – членов ОДКБ к единому стандарту нормативной урегулированности отношений в сфере обеспечения информационно-коммуникационной безопасности;

в) ратификации основных соглашений в рамках ОДКБ в данной сфере.

В рамках Организации Договора о коллективной безопасности необходимо разработать скоординированную систему защиты информации разных видов, предусмотреть адекватное скоординированное государственное регулирование в данной сфере. Это потребует также создания развитой нормативной правовой базы для функционирования межгосударственной системы защиты информации от технических разведок и от ее утечки по техническим каналам.

Система организационных мер должна включать:

1) разработку согласованных методик оценки содержания информационных ресурсов;
2) определение статуса информации и информационных ресурсов, используемых в рамках деятельности ОДКБ, регламентацию оснований и порядка доступа к ним;
3) формирование надежного, основанного на современных технических средствах механизма обмена информацией в интересах политического, экономического и военного сотрудничества государств – членов ОДКБ, включая сохранность информации при ее передаче по национальным телекоммуникационным каналам и сетям связи;
4) осуществление системы контроля за созданием, использованием и защитой систем и средств сбора, обработки, хранения и передачи охраняемой в соответствии с законом информации;
5) совершенствование механизмов защиты секретной информации в рамках ОДКБ;
6) развитие системы противодействия иностранным техническим разведкам.

В целях совершенствования системы защиты информационных ресурсов в рамках ОДКБ представляется целесообразной разработка и принятие межгосударственного Соглашения о принципах и механизмах осуществления информационного обмена. Отдельного внимания требует разработка проекта Соглашения о сотрудничестве по организации

межгосударственного обмена информацией в сфере обеспечения информационной безопасности.

4.3 Противодействие преступным проявлениям в информационной сфере

Рациональным решением представляется приведение национального законодательства государств – членов ОДКБ к единому стандарту нормативной урегулированности информационных отношений. На национальном уровне в государствах – членах ОДКБ необходимы совершенствование и гармонизация уголовного законодательства, требуют уточнения составы преступлений против информационной безопасности, а также составы противоправных деяний.

Примерный перечень наиболее опасных и могущих стать наиболее опасными правонарушений в области информационной безопасности, затрагивающих как национальные интересы государств – членов ОДКБ, так и правонарушений, посягающих на законные информационные права и интересы самой Организации, приведён в Приложении. Такой перечень требует детальной проработки и обоснования, как самих наименований, так и состава охватываемых им правонарушений.

4.3.1 Основные приоритетные направления развития правовой сферы:

- подготовка и принятие концептуального документа о межгосударственном взаимодействии по противодействию преступлениям в сфере современных информационных технологий;
- закрепление в нормативных актах системы правоохранительных субъектов и механизмов их взаимодействия;
- синхронное согласованное совершенствование норм, регулирующих ответственность за правонарушения в области обеспечения информационной безопасности во всех государствах – членах ОДКБ;
- развитие и совершенствование правового обеспечения оперативно-розыскной деятельности по предупреждению, выявлению и пресечению правонарушений в сфере компьютерной информации. Разработка учебно-методических и научных материалов по проблемам противодействия информационной преступности в государствах – членах ОДКБ;
- унификация механизмов выявления расследования правонарушений в информационной сфере и процедур привлечения виновных к уголовной, административной и иным видам ответственности.

В целях эффективного противодействия современным криминальным вызовам и угрозам представляется необходимым:

1) создание эффективного правового механизма, позволяющего организовывать взаимодействие субъектов оперативно-розыскной деятельности при расследовании преступлений против информационной безопасности;

2) разработка основополагающих концептуальных документов о взаимодействии в вопросах ограничения функционирования информационных ресурсов, используемых для осуществления противоправной деятельности;
3) разработка руководящих нормативных документов по вопросам межгосударственного взаимодействия при обмене оперативными данными о ресурсах сети Интернет, используемых (могущих использоваться) в террористических и иных противоправных целях.

4.3.2 Требует постоянного внимания совершенствование системы органов обеспечения информационной безопасности.

Необходимо закрепление в межгосударственных нормативных актах системы действующих правоохранительных субъектов и механизмов их взаимодействия. На национальном уровне необходимо определение уполномоченного органа по борьбе с преступностью в информационной сфере, а в рамках ОДКБ — создание международного центра реагирования на компьютерные инциденты.

Система организационных мер с необходимостью должна включать:
1) взаимодействие компетентных правоохранительных органов государств по предупреждению и пресечению преступлений в информационной сфере;
2) координацию на уровне структур ОДКБ деятельности правоохранительных органов государств – членов ОДКБ по предотвращению компьютерных преступлений;
3) создание защищенной системы интегрированных банков данных оперативно-розыскного, справочного и статистического характера;
4) развитие систем и методик выявления фактов преступлений против информационно-коммуникационной безопасности и осуществление межгосударственного обмена ими;
5) привлечение общественности к обеспечению законности и правопорядка в информационной сфере, создание механизмов общественного контроля и содействия правоохранительным органам;
6) предотвращение создания и использования средств нарушения нормального функционирования международных и национальных информационных и телекоммуникационных систем и сетей связи.

4.4 Информационное обеспечение реализации государственной политики

С учетом динамики возникновения и характера современных вызовов и угроз становится все более острой настоятельная необходимость всесторонней углубленной научной проработки принципиальных целей, задач и направлений развития сотрудничества государств – членов ОДКБ по

противодействию современным угрозам в информационной сфере. Детальной проработки и нормативного закрепления требует, например, такая категории как «*информационный суверенитет государства*» — правовой статус, обеспечивающий способность государства самостоятельно осуществлять свои функции в информационной сфере в целях соблюдения прав и свобод граждан, обеспечения национальной безопасности.

На национальном уровне в государствах – членах ОДКБ требуют своего решения задачи совершенствования государственной системы обеспечения информационной безопасности, уточнение функций и усиление полномочий государственных органов. Отдельного внимания требует развитие и совершенствование подготовки специалистов в области обеспечения информационной безопасности государственной политики.

Представляется, что заслуживают особого внимания постановка вопросов о разработке в рамках ОДКБ межгосударственной политики обеспечения информационной безопасности и о построении единой системы обеспечения информационной безопасности государств – членов ОДКБ. В этой связи требуют постановки и решения задачи создания системы рабочих органов по координации и согласованию информационной политики, выявлению реальных и прогнозированию потенциальных угроз информационным интересам личности, общества и государства, своевременного согласованного реагирования на проявляющиеся информационные вызовы и угрозы.

Информационное обеспечение государственной политики требует создания эффективной системы распространения объективной и достоверной информации. В этой связи актуальна задача создания эффективно действующего органа по распространению объективной и достоверной информации о деятельности ОДКБ, повышение её положительного имиджа у национальной и международной общественности.

Настоятельно необходима разработка и осуществление комплекса мер по нейтрализации возможных негативных последствий от имеющих место «*вбросов*» недостоверной информации об отдельных государствах – членах и ОДКБ в целом. Это требует создания системы выявления реальных и прогнозирования потенциальных угроз информационным интересам личности, общества и государства и реагирования на информационные вызовы и угрозы.

Перспективной представляется задача приведения национального законодательства государств – членов ОДКБ к единому стандарту нормативной урегулированности отношений в сфере информационной безопасности. В перспективе развития сотрудничества и укрепления Организации договора о коллективной безопасности актуальной будет разработка и принятие международного правового акта, регулирующего общественные отношения в области противодействия угрозам

национальным интересам государств – членов ОДКБ в информационной сфере.

4.5 Защита единого информационного пространства

Разработка правовых основ создания единого информационного пространства, требований и правовых механизмов по обеспечению его безопасности, требует научной проработки и правовой легализации, прежде всего, таких базовых категорий как:

- «*деструктивное информационное воздействие*» — под которым предлагается понимать осуществление информационного влияния на политические и социально-экономические процессы происходящие в государствах – членах ОДКБ, на государственные органы этих государств, а также на физических и юридических лиц этих государств в целях ослабления обороноспособности государств – членов ОДКБ, нарушения общественной безопасности, принятия заведомо невыгодных решений, заключения заведомо невыгодных международных договоров, ухудшения отношений с другими государствами, создания социально-политической напряженности внутри государств – членов ОДКБ, формирования угрозы возникновения чрезвычайных ситуаций, разрушения традиционных духовных и нравственных ценностей, создания препятствий для нормальной деятельности государственных органов, а также причинения иного ущерба национальной безопасности государств – членов ОДКБ;

- «*информационное оружие*» — понимаемое как совокупность средств, методов и технологий, обеспечивающих возможность силового воздействия на информационную сферу противника с целью разрушения его информационной инфраструктуры, систем управления государством, снижения обороноспособности и применяемых в целях ведения информационной войны;

- «*информационное противоборство*» — рассматриваемое как соперничество социальных систем в информационной сфере по поводу влияния на те, или иные сферы социальных отношений и установления контроля над источниками стратегических ресурсов, в результате которого одни участники соперничества получают преимущества, необходимые им для дальнейшего развития, а другие их утрачивают.

Представляется, что в настоящее время к наиболее актуальным угрозам и правонарушениям в информационной сфере следует отнести, в первую очередь, распространение информации с признаками разжигания национальной и религиозной розни, пропаганды терроризма и экстремизма и деструктивное информационное воздействие на личность, общество и государство. Как следствие, требуют своего решения следующие первоочередные задачи:

- создание правового механизма контроля и ограничения доступа к Интернет-ресурсам, представляющим угрозу безопасности для государств – членов ОДКБ;

- разработка инструментария оценки содержания информационного контента и критериев отнесения его к материалам террористического, экстремистского или иного противоправного характера;

- противодействие и нейтрализация информационных потоков, формирующих негативное отношение и недостоверное представление о государствах – членах ОДКБ.

Необходима разработка комплекса мер активного практического информационного противоборства с позиций и в интересах государств – членов ОДКБ. В этой связи первоочередными задачами в рамках совершенствования национального законодательства представляются:

1) закрепление в национальных законодательствах запрета на использование информационных технологий в ущерб безопасности личности, общества и государства;
2) криминализация деяний, посягающих на национальные интересы государств – членов ОДКБ в информационном пространстве;
3) совершенствование механизмов управления и контроля национальных доменов сети Интернет и закрепление основных принципов государственной политики обеспечения информационной безопасности открытых телекоммуникационных сетей (ОТКС) в законодательном акте;
4) приведение национального законодательства государств – членов ОДКБ к единому стандарту нормативной урегулированности отношений.

В организационном плане требуют первоочередного решения следующие задачи:

1) выделение из национальной инфраструктуры сегментов, интегрируемых в единую информационную структуру ОДКБ;
2) интеграция национальных информационных пространств в единое информационное пространство ОДКБ;
3) обеспечение безопасности ОТКС, совершенствование механизмов управления и контроля национальных доменов сети Интернет;
4) разработка и осуществление мер по нейтрализации, локализации и противодействию информационному и информационно-психологическому воздействию со стороны иностранных государств.

4.6 Обеспечение безопасности информационно-коммуникационной инфраструктуры

Первостепенной задачей является анализ состояния общей критически важной информационно-коммуникационной инфраструктуры государств –

членов ОДКБ. В этой связи требуют легализации и правового закрепления толкования таких понятий как: «*общая (единая) информационная инфраструктура государств – членов ОДКБ*»; «*критически важные объекты информационно-коммуникационной инфраструктуры ОДКБ*»; «*обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры ОДКБ*».

В качестве наиболее актуальных и опасных угроз с позиций информационно-коммуникационной инфраструктуры следует рассматривать, в первую очередь:

- использование коммуникационных технологий для дестабилизации общественно-политической ситуации;
- снижение надежности и устойчивости функционирования информационно-коммуникационной инфраструктуры;
- нарушение безопасного, стабильного функционирования объектов критически важных информационных инфраструктур.

Концептуальным организационным решением должно стать лицензирование деятельности, регистрация и стандартизация работ и услуг, сертификация товаров в области обеспечения информационной безопасности.

К числу первоочередных задач следует отнести:

1) создание единой системы обеспечения безопасности информационной инфраструктуры и информационных технологий;
2) разработку системы государственных стандартов по информационной безопасности;
3) установление правовых механизмов обязательной сертификации информационных систем и средств, предназначенных для обработки охраняемой в соответствии с законом информации;
4) разработку и стандартизацию в государствах – членах ОДКБ национальных технических и программных средств, используемых для работы с информационными ресурсами и обеспечения их безопасности, замена ими импортных аналогов.

Решение перечисленных выше задач потребует:

1) разработки критериев и методов оценки эффективности средств обеспечения информационно-коммуникационной безопасности;
2) создания системы сертификации средств защиты информации, стандартизации способов и средств защиты информации;
3) совершенствования системы сертификации телекоммуникационного оборудования и программного обеспечения по требованиям информационной безопасности;
4) создания системы государственного контроля за обеспечением безопасности КВОИ;
5) разработки системы мониторинга состояния информационной безопасности КВОИ;

6) разработки системы мер по защите информационных систем, обеспечивающих управление КВОИ;
7) совершенствования системы информирования населения об угрозах возникновения чрезвычайных ситуаций.

В этой связи важнейшими задачами, требующими своего решения на национальном уровне, являются:

- приведение национального законодательства государств – членов ОДКБ к единому стандарту нормативной урегулированности информационных отношений;
- формирование правового регулирования использования критически важной инфраструктуры, определение ее правового статуса и принадлежности;
- усиление ответственности на действия, создающие угрозу или приводящие к нарушению функционирования КВОИ.

На межгосударственном уровне важнейшими задачами, требующими своего решения, должны стать разработка нормативных документов о взаимодействии в вопросах защиты критически важных объектов коммуникаций и инфраструктуры и нормативное закрепление вопросов создания общей критически важной информационно-коммуникационной инфраструктуры в рамках ОДКБ.

V. Некоторые первоочередные мероприятия

В государствах – членах ОДКБ необходима организация регулярной работы по системному совершенствованию национальной нормативно-правовой базы, устранению пробелов в законодательстве, препятствующих организации эффективного взаимодействия и противодействию угрозам национальных интересов государств – членов ОДКБ в информационной сфере.

В целях повышения уровня обеспечения информационно-коммуникационной безопасности государств – членов ОДКБ представляется необходимым организовать работу по структурному упорядочению нормативных правовых актов, закрепляющих нормы правового обеспечения информационно-коммуникационной безопасности. Необходимы систематизация, выстраивание иерархии и, по возможности, кодификация таких нормативных правовых актов.

На международном и национальном уровнях представляется необходимым организовать системную работу по анализу и проработке понятийного аппарата. Упорядочение юридических терминов, используемых в нормативных правовых актах, закрепляющих нормы правового обеспечения информационно-коммуникационной безопасности, создаст возможность при осуществлении законотворческой деятельности и правоприменительной практики в информационной сфере учитывать дефиниции, уже закрепленные в законодательстве.

В практическом плане на базе унификации терминов и определений в сфере информационной безопасности целесообразно форсировать работу по созданию толкового словаря — Глоссария терминов информационного законодательства государств – членов ОДКБ.

Представляет интерес разработка проекта Стратегии информационной безопасности для государств – членов ОДКБ. Разработка подобного документа видится рациональной с использованием подходов стратегического планирования, что придаст правовым мерам обеспечения информационной безопасности в рамках ОДКБ должную целенаправленность. Представляется, что концептуально такой документ должен быть нацелен на реализацию обеспечения устойчивого развития информационных отношений в государствах – членах ОДКБ с учетом динамики процессов развития информационного общества, на обеспечение прогнозирования, создание препятствий для реализации и надежную защиту от угроз жизненно важным интересам личности, общества и государства в информационной сфере. Это с неизбежностью потребует обеспечения системного дополнения национального законодательства государств – членов ОДКБ в части разработки стандартов и общих требований соответствия. Самостоятельную задачу представляет определение структурно необходимого минимума (стандарта) критериев, образующих информационно-коммуникационную безопасность.

В прагматическом аспекте видится полезной разработка проекта Соглашения о сотрудничестве государств – членов ОДКБ по организации межгосударственного обмена информацией в сфере обеспечения информационной безопасности.

Приложение
к разделу 4.3

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ
наиболее опасных и могущих стать наиболее опасными правонарушений в области информационной безопасности, затрагивающих как национальные интересы государств-членов ОДКБ (1.1-1.16)**, так и правонарушений, посягающих на законные информационные права и интересы самой Организации Договора о коллективной безопасности** (2.1-2.5)**.**

1.1 - распространение информации, направленное на возбуждение расовой, национальной, религиозной вражды или розни, на унижение национальной чести и достоинства;

1.2 - распространение информации, запрещённой к распространению, в том числе порнографических материалов, материалов, пропагандирующих культ насилия и жестокости;

1.3 - призывы к организации или проведению массовых беспорядков, к незаконным действиям по организации или проведению массовых мероприятий;

1.4 - изготовление и (или) распространение, а равно хранение с целью распространения экстремистских материалов;

1.5 - распространение в средствах массовой информации, а также в компьютерных сетях сведений, которые могут быть использованы для причинения вреда здоровью или нарушения общественной безопасности, в том числе информации о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ, их прекурсоров и аналогов, а также взрывчатых веществ и огнестрельного оружия;

1.6 - угроза совершением акта терроризма;

1.7 - заведомо ложное сообщение, в том числе об опасности;

1.8- разглашение коммерческой, банковской, следственной и иной охраняемой законом тайны;

1.9 - похищение либо собирание незаконным способом сведений, составляющих коммерческую или банковскую тайну;

1.10 - незаконное ограничение свободы массовой информации;

1.11 - несообщение информации об опасности для жизни людей;

1.12 - нарушения порядка распространения продукции средств массовой информации, религиозной информации, информации о нацистской символике или атрибутике;

1.13 - сокрытие либо умышленное искажение сведений, обязательных для публичного распространения, в том числе о загрязнении окружающей среды;

1.14 - нарушение требований законодательства по ограничению доступа пользователей интернет-услуг к информации, запрещенной к распространению в соответствии с законодательными актами;

1.15 - изменение, уничтожение, или блокирование информации, хранящейся в компьютерной системе, сети или на машинных носителях;

1.16 - разработка, использование либо распространение вредоносных компьютерных программ.

2.1 - распространение в любой форме взглядов, идей или призывов с целью вызвать напряжённость в отношениях либо агрессию одной страны в отношении другой;

2.2 - разглашение сведений, составляющих секретную информацию в ОДКБ и служебную информацию ограниченного распространения;

2.3 - выдача иностранному государству, иностранной организации или их представителю государственных секретов государств – членов ОДКБ или иной информации ограниченного распространения в ОДКБ;

2.4 - передача, похищение, собирание или хранение с целью передачи иностранному государству, иностранной организации или их представителю сведений, составляющих государственные секреты государств – членов ОДКБ и иной информации ограниченного распространения в ОДКБ;

2.5 - призывы к действиям, направленным в ущерб внешней безопасности государств – членов ОДКБ, их суверенитету, территориальной неприкосновенности, национальной безопасности и обороноспособности.

Следует также принимать во внимание общественную опасность и других деяний, направленных на дискредитацию государств – членов ОДКБ, таких, например, как распространение заведомо ложных, позорящих руководство государств – членов ОДКБ измышлений, нацеленных на унижение чести и достоинства руководителей государств – членов ОДКБ.

Приводимый здесь перечень правонарушений может служить в качестве иллюстрации. В целом представляется, что подобный перечень требует детальной проработки и обоснования, как самих наименований, так и состава охватываемых им правонарушений.