О внесении на рассмотрение Президента Республики Казахстан предложения о подписании Соглашения о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности

Постановление Правительства Республики Казахстан от 24 ноября 2017 года № 770

Правительство Республики Казахстан **ПОСТАНОВЛЯЕТ:**

внести на рассмотрение Президента Республики Казахстан предложение о подписании Соглашения о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности.

Премьер-Министр
Республики Казахстан *Б. Сагинтаев*

Проект

СОГЛАШЕНИЕ
о сотрудничестве государств-членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности

Государства-члены Организации Договора о коллективной безопасности (далее - ОДКБ), далее именуемые Сторонами,

руководствуясь положениями Договора о коллективной безопасности от 15 мая 1992 года, Устава Организации Договора о коллективной безопасности от 7 октября 2002 года, Стратегии коллективной безопасности Организации Договора о коллективной безопасности на период до 2025 года, утвержденной Решением Совета коллективной безопасности ОДКБ от 14 октября 2016 года, другими решениями Совета коллективной безопасности ОДКБ, направленными на объединение усилий по совершенствованию системы информационной безопасности в интересах Сторон,

выражая обеспокоенность нарастанием угроз в информационном пространстве, способных нанести ущерб национальной и коллективной безопасности государств-членов ОДКБ,

руководствуясь общепризнанными принципами международного права, в целях поддержания мира, международной и региональной безопасности и стабильности,

считая, что обеспечение информационной безопасности является одним из приоритетных направлений обеспечения коллективной безопасности государств – членов ОДКБ,

считая неприемлемым деструктивное информационное воздействие с использованием информационной инфраструктуры, использование информационных

технологий для вмешательства во внутренние дела, провоцирование угроз информационной безопасности,

стремясь воспрепятствовать использованию информационных технологий и ресурсов для дестабилизации обстановки на территории Сторон, в целях нанесения ущерба безопасности критически важным структурам,

признавая, что доверие и безопасность в использовании информационно-коммуникационных технологий относятся к фундаментальным основам информационного общества,

стремясь укрепить правовые и организационные основы сотрудничества Сторон в области обеспечения информационной безопасности,

считая необходимым создание условий для последующей реализации совместных практических мероприятий, направленных на совершенствование системы информационной безопасности,

поддерживая формирование культуры информационной безопасности, основанной на уважении прав и свобод человека, приоритете сохранения политической, социальной и экономической стабильности,

руководствуясь принципами приоритетности государственного суверенитета государств – членов ОДКБ,

подчеркивая, что информационная безопасность каждой из Сторон формирует информационную безопасность ОДКБ и непосредственно влияет на состояние коллективной безопасности ОДКБ в целом,

признавая необходимость соблюдения баланса между основными правами и свободами человека и эффективным противодействием угрозам информационной безопасности,

стремясь обеспечить защищенность интересов Сторон в информационном пространстве,

согласились о нижеследующем:

Статья 1

Целью настоящего Соглашения является развитие взаимодействия Сторон в интересах обеспечения информационной безопасности государств – членов ОДКБ.

Для достижения цели Соглашения Стороны обеспечивают:

- дальнейшее развитие системы информационной безопасности государств – членов ОДКБ на основе межгосударственного сотрудничества и укрепления межведомственного взаимодействия Сторон;

- совершенствование механизмов противодействия угрозам в информационной сфере;

- проведение совместных мероприятий, в том числе практического характера, направленных на укрепление информационной безопасности и противодействие противоправной деятельности в информационном пространстве государств – членов ОДКБ;

- взаимодействие в вопросах обеспечения международной информационной безопасности;

- выработку согласованной позиции по вопросам обеспечения международной информационной безопасности и участие в ее продвижении на международной арене;

- содействие разработке и скорейшему принятию под эгидой ООН универсальных правил, норм и принципов ответственного поведения государств в информационном пространстве;

- взаимную помощь в целях развития технологической основы (базы) обеспечения информационной безопасности Сторон.

Статья 2

Для целей настоящего Соглашения используются следующие термины и определения:

"деструктивное информационное воздействие" - использование информационно-коммуникационных технологий в целях нарушения деятельности органов власти, ослабления национальной безопасности, нанесения ущерба информационно-коммуникационным системам, сетям и ресурсам, критически важным и другим структурам, ухудшения межгосударственных отношений, создания внутренней социально-политической напряженности, разрушения традиционных духовных и нравственных ценностей, установления контроля над национальными информационными ресурсами, формирования угрозы возникновения чрезвычайных ситуаций, причинения иного ущерба национальным интересам государств – членов ОДКБ;

"защита информации" - комплекс правовых, организационных и технических мер, направленных на обеспечение целостности, конфиденциальности и доступности информации;

"информационная безопасность" - состояние защищенности личности, общества, государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве;

"информационное пространство" - совокупность информационной инфраструктуры и информации, ею обрабатываемой;

"компьютерная атака"- целенаправленное воздействие программно-техническими средствами на информационно-коммуникационные системы, сети, ресурсы, в том числе на автоматизированные системы управления критически важных структур,

осуществляемое в целях нарушения и/или прекращения их функционирования и/или создания угрозы безопасности обрабатываемой ими информации;

"компьютерный инцидент" - факт нарушения штатного режима функционирования элемента информационной инфраструктуры или информационной инфраструктуры в целом;

"критически важные структуры" -объекты, системы и институты государства, воздействие на которые может иметь последствия, прямо затрагивающие национальную безопасность, включая безопасность личности, общества и государства;

"система информационной безопасности" - комплекс мер правового, политического, военного, организационного, кадрового, финансового, научно-технического и специального характера, нацеленный на обеспечение информационной безопасности;

"угроза информационной безопасности"- фактор (совокупность факторов), создающий (создающая)опасность для личности, общества, государства в информационном пространстве.

Статья 3

В качестве основных угроз информационной безопасности Стороны рассматривают :

осуществление деструктивного информационного воздействия на государства – члены ОДКБ и Организацию в целом;

использование информационно-коммуникационных технологий террористическими и экстремистскими организациями, организованными преступными группами (сообществами);

осуществление противоправной деятельности с использованием информационно-коммуникационных технологий.

Статья 4

Стороны осуществляют сотрудничество в области обеспечения информационной безопасности по следующим основным направлениям:

взаимодействие в разработке и продвижении правовых основ сотрудничества, содействие совершенствованию международной правовой базы;

формирование практических механизмов совместного реагирования на угрозы информационной безопасности;

развитие мер укрепления доверия в сфере обеспечения информационной безопасности;

совершенствование технологической основы обеспечения информационной безопасности;

создание условий для взаимодействия компетентных органов Сторон в целях реализации настоящего Соглашения.

Статья 5

Стороны предпринимают совместные усилия по формированию правовых основ сотрудничества и совершенствованию международной правовой базы в сфере обеспечения информационной безопасности:

разрабатывают проекты международных договоров и иных документов, направленных на реализацию настоящего Соглашения;

совершенствуют национальную нормативную правовую базу Сторон в области обеспечения информационной безопасности;

вырабатывают предложения по гармонизации национального законодательства Сторон, регулирующего обеспечение информационной безопасности;

совершенствуют нормы, регулирующие ответственность за правонарушения в области информационной безопасности;

совершенствуют правовые меры по противодействию противоправной деятельности в информационной сфере.

Статья 6

Стороны содействуют формированию практических механизмов совместного реагирования на угрозы информационной безопасности:

прилагают совместные усилия для выявления, предупреждения и нейтрализации угроз информационной безопасности, ликвидации последствий их проявлений;

обеспечивают планирование и проведение скоординированных мероприятий по обеспечению информационной безопасности;

осуществляют при необходимости взаимодействие в вопросах защиты критически важных структур;

сотрудничают по противодействию деструктивному информационному воздействию;

противодействуют осуществлению противоправной деятельности в информационном пространстве;

осуществляют самостоятельно или при соответствующем обращении меры для предотвращения использования третьей стороной территории и/или информационной инфраструктуры, находящейся под юрисдикцией государства – члена ОДКБ, для оказания деструктивного информационного воздействия, в том числе компьютерных атак, на другое государство – член ОДКБ;

взаимодействуют в интересах определения источника компьютерных атак, проведенных с использованием их территории, противодействия этим атакам и ликвидации последствий;

противодействуют созданию и распространению вредоносного программного обеспечения;

обмениваются опытом по выработке критериев определения информационных ресурсов, используемых в противоправных целях, их выявлению и блокированию;

взаимодействуют в подготовке кадров в области обеспечения информационной безопасности.

Статья 7

Стороны, развивая меры укрепления доверия в области обеспечения информационной безопасности:

обеспечивают обмен информацией и взаимное оповещение об угрозах информационной безопасности и их источниках, компьютерных инцидентах, принимаемых мерах реагирования, в том числе ликвидации последствий;

в соответствии с национальным законодательством представляют запрашиваемую информацию, необходимую для расследования противоправных деяний в сфере действия Соглашения;

обмениваются опытом по предотвращению, правовому разбирательству и ликвидации последствий противоправных деяний с использованием информационных технологий, противодействия угрозам информационной безопасности;

содействуют обмену информацией о признаках, фактах, методах и средствах использования сетей связи общего пользования в террористических и иных противоправных целях;

осуществляют в соответствии с национальным законодательством обмен результатами научно-исследовательских работ, информационно-аналитическими и справочными материалами, нормативными правовыми актами в области обеспечения информационной безопасности;

стимулируют научно-технические разработки в области обеспечения информационной безопасности.

Статья 8

Стороны принимают согласованные меры по совершенствованию технологической основы обеспечения информационной безопасности:

поддерживают создание совместных, а также совместимых систем обеспечения информационной безопасности;

содействуют гармонизации технических требований к обеспечению информационной безопасности;

содействуют Сторонам в вопросах, касающихся оснащения программно-техническими средствами обеспечения информационной безопасности и их модернизации.

Статья 9

Практическое взаимодействие компетентных органов Сторон в целях реализации данного Соглашения осуществляется в соответствии с принятыми в рамках ОДКБ международными правовыми актами.

Статья 10

Стороны обеспечивают защиту информации, передаваемой или создаваемой в ходе сотрудничества в рамках настоящего Соглашения, доступ и распространение которой ограничены в соответствии с законодательством Сторон.

Защита такой информации осуществляется в соответствии с законодательством и (или) соответствующими взаимными обязательствами Сторон в рамках иных многосторонних соглашений, принятых в ОДКБ, нормативными правовыми актами получающей Стороны.

Получаемая информация не раскрывается, не передается третьей стороне без письменного согласия передающей Стороны, являющейся источником этой информации.

Порядок обмена, условия и меры по защите сведений, составляющих государственную тайну (секреты) Сторон в ходе реализации настоящего Соглашения, определяются Соглашением о взаимном обеспечении сохранности секретной информации в рамках Организации Договора о коллективной безопасности от 18 июня 2004 года.

Статья 11

Положения настоящего Соглашения не затрагивают прав и обязательств каждой из Сторон, вытекающих из других международных договоров, участниками которых они являются.

Статья 12

Настоящее Соглашение действует в течение срока действия Договора о коллективной безопасности от 15 мая 1992 года, если Стороны не примут иного решения.

Статья 13

В настоящее Соглашение по взаимному согласию Сторон могут вноситься изменения и дополнения, являющиеся его неотъемлемой частью, которые оформляются отдельными протоколами, вступающими в силу в порядке, предусмотренном статьей 16 настоящего Соглашения.

Статья 14

Спорные вопросы, связанные с толкованием и применением настоящего Соглашения, разрешаются путем консультаций и переговоров между Сторонами.

Во время таких консультаций и переговоров Стороны продолжают выполнять свои обязательства в соответствии с положениями настоящего Соглашения.

Статья 15

Стороны самостоятельно несут расходы по участию их представителей и экспертов в соответствующих мероприятиях по исполнению настоящего Соглашения.

В отношении прочих расходов, связанных с исполнением настоящего Соглашения, Стороны в каждом отдельном случае могут согласовывать иной порядок финансирования в соответствии с законодательством Сторон.

Статья 16

Настоящее Соглашение вступает в силу с даты получения депозитарием четвертого письменного уведомления о выполнении подписавшими его Сторонами внутригосударственных процедур, необходимых для вступления его в силу.

Для Сторон, выполнивших необходимые внутригосударственные процедуры позднее, настоящее Соглашение вступает в силу с даты сдачи депозитарию соответствующего письменного уведомления.

Статья 17

Каждая Сторона может выйти из настоящего Соглашения, направив письменное уведомление об этом депозитарию не позднее, чем за 6 месяцев до выхода, урегулировав все обязательства, возникшие за время действия настоящего Соглашения.

Генеральный секретарь Организации Договора о коллективной безопасности уведомляет Стороны о выходе Стороны из Соглашения и прекращении его действия для этой Стороны.

Совершено в городе _____ "__"_____ 201__ года в одном подлинном экземпляре на русском языке. Подлинный экземпляр настоящего Соглашения хранится в Секретариате Организации Договора о коллективной безопасности, который направит каждому государству, подписавшему настоящее Соглашение, его заверенную копию.

За Республику Армения

За Республику Беларусь

За Республику Казахстан

За Кыргызскую Республику

За Российскую Федерацию

За Республику Таджикистан