МОДЕЛЬНЫЙ ЗАКОН ОДКБ
«Об информационной безопасности»

Настоящий модельный Закон является правовым ориентиром для регулирования отношений, связанных с определением основных угроз информационной безопасности, направлений и мер ее обеспечения в целях укрепления коллективной безопасности для государств – членов Организации Договора о коллективной безопасности (далее – государства – члены ОДКБ).

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. **Основные термины, используемые в настоящем Законе, и их определения**

1. Для целей настоящего Закона используются следующие основные термины и их определения:

информационное пространство ОДКБ – сфера деятельности и взаимодействия государств – членов ОДКБ, связанная с формированием, созданием, преобразованием, передачей, использованием и хранением информации, оказывающая воздействие на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию;

информационная безопасность ОДКБ – состояние защищенности интересов государства – члена ОДКБ, которое позволяет обеспечить независимость, территориальную целостность, суверенитет, обороноспособность и защиту от информационных угроз каждому из государств – членов ОДКБ;

вызов информационной безопасности – совокупность условий, потенциально способных перерасти в угрозу информационной безопасности государств – членов ОДКБ;

угроза информационной безопасности ОДКБ – совокупность внутренних и внешних факторов, препятствующих достижению стратегической цели ОДКБ;

система обеспечения информационной безопасности ОДКБ – совокупность органов государственной власти, сил и средств обеспечения информационной безопасности государств – членов ОДКБ, обеспечивающих в соответствии с международным правом двусторонними соглашениями и национальными законодательствами защиту жизненно важных коллективных и национальных интересов, суверенитета и территориальной целостности государств – членов ОДКБ в информационной сфере на коллективной основе при формировании объединяющего их безопасного информационного пространства.

2. Используемые в настоящем Законе иные термины в области обеспечения информационной безопасности применяются в том значении, в каком они используются в нормативных правовых документах, принятых к исполнению государствами – членами ОДКБ и регулирующих

информационные отношения между ними, если иное не установлено настоящим Законом.

Статья 2. **Общие принципы информационной безопасности государств – членов ОДКБ**

1. Государства – члены ОДКБ осуществляют сотрудничество в области обеспечения международной информационной безопасности в рамках настоящего Закона, направленное на совершенствование механизмов и мер по предотвращению конфликтов, которые могут возникнуть в том числе как следствие противоправного использования информационно-коммуникационных технологий, а также по преодолению дефицита доверия между сторонами конфликтов.

2. Деятельность государств – членов ОДКБ в рамках настоящего Закона должна быть совместимой с законодательствами государств – членов ОДКБ.

3. Каждое государство – член ОДКБ имеет равные права на защиту информационных ресурсов своего государства от неправомерного использования и несанкционированного вмешательства, в том числе от компьютерных и информационных атак на них. Каждое государство – член ОДКБ не осуществляет по отношению к другому государству – члену ОДКБ подобных действий и оказывает содействие другому государству – члену ОДКБ в реализации указанных прав в информационном пространстве ОДКБ.

4. Государства – члены ОДКБ принимают необходимые коллективные меры по предотвращению применения информационно-коммуникационных технологий для вмешательства во внутренние дела суверенных государств, любых посягательств на территориальную целостность, государственный суверенитет и независимость государств – членов Организации, а также в иных деструктивных целях.

5. Государства – члены ОДКБ, осознавая трансграничный характер современных вызовов и угроз в сфере информационно-коммуникационных технологий, прилагают усилия к координации дальнейших совместных мер в борьбе с использованием информационно-коммуникационных технологий в террористических и других преступных целях.

6. Государства – члены ОДКБ прилагают усилия к тому, чтобы информационные инфраструктуры и ресурсы государств – членов ОДКБ не использовались третьей стороной для нанесения ущерба государствам – членам ОДКБ.

Статья 3. **Основные направления обеспечения информационной безопасности**

1. Стратегической целью обеспечения информационной безопасности государств – членов ОДКБ является защита их жизненно важных интересов от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов

агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств – членов ОДКБ и представляющих угрозу международному миру, безопасности и стратегической стабильности, формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

2. Достижение стратегической цели обеспечения информационной безопасности государств – членов ОДКБ осуществляется путем разработки и системной реализации комплекса взаимосвязанных политических, дипломатических, оборонных, экономических, информационных и иных мер, направленных на упреждение или снижение угроз информационной безопасности.

3. Основными направлениями реализации межгосударственной политики государств – членов ОДКБ в области международной информационной безопасности по совершенствованию межгосударственного взаимодействия, направленного на противодействие угрозе использования информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств – членов ОДКБ, являются:

1) развитие сотрудничества государств – членов ОДКБ с другими государствами, международными, международными неправительственными организациями и организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, в целях выработки правового механизма международного обмена информацией о таких инцидентах и повышения эффективности взаимодействия уполномоченных органов;

2) содействие созданию на глобальном, региональном, многостороннем и двустороннем уровнях эффективного механизма межгосударственного взаимодействия, направленного на предотвращение компьютерных атак на информационные ресурсы государств – членов ОДКБ, в том числе на критическую информационную инфраструктуру;

3) содействие выработке на глобальном, региональном, многостороннем и двустороннем уровнях порядка обмена информацией о передовых практиках обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы государств – членов ОДКБ, в том числе на критическую информационную инфраструктуру, а также совместного реагирования на компьютерные инциденты;

4) совершенствование взаимодействия между национальными уполномоченными органами по расследованию компьютерных инцидентов государств – членов ОДКБ, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также совместного реагирования на компьютерные инциденты.

4. Основными сферами реализации указанных направлений обеспечения коллективной информационной безопасности являются сферы:

1) обороны;

2) защиты конституционного строя и государственной безопасности;

3) информационных технологий и связи;

4) стратегической стабильности и равноправного стратегического партнерства.

Глава 2. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ОБОРОНЫ

Статья 4. **Основные угрозы информационной безопасности в сфере обороны**

Основными угрозами информационной безопасности в сфере обороны являются:

1) создание иностранными государствами военно-политических блоков, военной инфраструктуры, сил и средств, направленных на активное информационное противоборство с государством – членом ОДКБ в военной сфере;

2) попытки иностранных государств получить неправовым путем достоверную конфиденциальную информацию о состоянии обеспечения национальной информационной безопасности в государствах – членах ОДКБ;

3) возможность применения иностранными государствами в любое время средств активного деструктивного информационного воздействия на военную информационную инфраструктуру, включая средства связи, средства управления оружием и военной техникой, для подавления или ослабления возможностей обороны государств – членов ОДКБ в целом или по отдельности;

4) попытки иностранных государств использования информационных ресурсов и технологий в целях совершения киберпреступлений, которые отрицательно сказываются на информационной безопасности и стабильности государств – членов ОДКБ.

Статья 5. **Основные направления обеспечения информационной безопасности в сфере обороны**

Основными направлениями обеспечения информационной безопасности в сфере обороны являются:

1) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;

2) построение системы обеспечения информационной безопасности коллективных и национальных Вооруженных сил с применением единых принципов вооружения, основанных на передовых достижениях науки и техники;

3) поддержание сил и средств информационной безопасности в области обороны на уровне, обеспечивающем отражение любых угроз.

Глава 3. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ЗАЩИТЫ КОНСТИТУЦИОННОГО СТРОЯ И ГОСУДАРСТВЕННОЙ/НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Статья 6. **Основные угрозы обеспечению информационной безопасности в сфере защиты конституционного строя и государственной/национальной безопасности**

Основными угрозами обеспечению информационной безопасности в сфере защиты конституционного строя и государственной/национальной безопасности являются:

1) информационное воздействие, направленное на дестабилизацию внутриполитической и социальной ситуации в государстве – члене ОДКБ, подрыв его национального суверенитета и территориальной целостности;

2) использование средств массовой информации, Интернета и сетей мобильной связи для размывания традиционных духовно-нравственных ценностей, пропаганды терроризма и экстремизма, в том числе на религиозной основе;

3) использование средств массовой информации и других информационных ресурсов для разжигания в государстве – члене ОДКБ ненависти и вражды между различными социальными, этническими и религиозными группами граждан;

4) использование средств массовой информации и других информационных ресурсов для навязывания обществу ложных или умышленно искаженных фактов, направленных на подрыв авторитета легитимной власти;

5) попытки осуществлять деструктивное идеологическое и психологическое воздействие на население государства – члена ОДКБ через информационные сети и медиаресурсы;

6) использование информационных и коммуникационных технологий в целях оказания деструктивного воздействия на общественно-политическую и социально-экономическую обстановку, а также попытки манипулирования общественным сознанием в государстве – члене ОДКБ;

7) использование информационно-коммуникационных технологий в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

8) использование информационно-коммуникационных технологий в экстремистских целях, а также для вмешательства во внутренние дела суверенных государств;

9) применение иностранными государствами технологий комбинированных форм воздействия на государство – член ОДКБ с целью разрушения государственности, дестабилизации внутриполитической ситуации или смены политического режима.

Статья 7. **Основные направления обеспечения информационной безопасности в сфере защиты конституционного строя и государственной/национальной безопасности**

Основными направлениями обеспечения информационной безопасности в сфере защиты конституционного строя и государственной/национальной безопасности являются:

1) построение эффективной системы, направленной на обеспечение информационной безопасности в случае возникновения активного деструктивного информационного воздействия одного или нескольких иностранных государств, имеющего целью дестабилизацию внутриполитической и социальной ситуации в государстве – члене ОДКБ;

2) построение системы пресечения распространения в информационно-телекоммуникационной сети Интернет сведений, имеющих целью размывание традиционных духовно-нравственных ценностей, пропаганду терроризма и экстремизма, в том числе на религиозной основе, с применением единообразных критериев противоправности.

Глава 4. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СВЯЗИ

Статья 8. **Основные угрозы обеспечению информационной безопасности в сфере информационных технологий и связи**

Основными угрозами обеспечению информационной безопасности в сфере информационных технологий и связи являются:

1) дезорганизация функционирования опорных сетей связи путем компьютерных атак на их системы управления;

2) дезорганизация функционирования сетей мобильной связи;

3) попытки дезорганизации функционирования доступа к информационно-телекоммуникационной сети Интернет в рамках функционирования национальных сегментов этой сети;

4) блокирование и уничтожение информации в государственных и иных базах данных критически важных объектов информатизации;

5) блокирование доступа или дезорганизация работы официальных сайтов органов государственной власти;

6) использование информационно-коммуникационных технологий для получения противоправного доступа к информационным ресурсам государств – членов ОДКБ и реализация умышленной утечки сведений, составляющих государственную тайну, и иных сведений конфиденциального характера;

7) попытки получения противоправного доступа к информации, содержащей персональные данные, защищаемой организациями и гражданами от распространения;

8) использование технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно-коммуникационных технологий, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, а также для усиления их технологической зависимости от доминирующих в сфере информатизации государств и информационного неравенства;

9) стремление закрепить монопольное положение в информационно-телекоммуникационной сети Интернет и контролировать все информационные ресурсы без законных на то оснований и вопреки нормам международного права, введение цензуры и блокировки альтернативных интернет-платформ.

Статья 9. **Основные направления обеспечения коллективной информационной безопасности в сфере информационных технологий и связи**

Основными направлениями обеспечения коллективной информационной безопасности в сфере информационных технологий и связи являются:

1) взаимодействие государств – членов ОДКБ с международными организациями в сфере борьбы с киберпреступностью;

2) противодействие государств – членов ОДКБ распространению материалов террористического и экстремистского характера в информационно-телекоммуникационной сети Интернет;

3) разработка и проведение государствами – членами ОДКБ совместных мер по борьбе с кибертерроризмом, совершенствование нормативно-правовой базы в данной сфере.

Глава 5. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ – ЧЛЕНОВ ОДКБ В СФЕРЕ СТРАТЕГИЧЕСКОЙ СТАБИЛЬНОСТИ И РАВНОПРАВНОГО СТРАТЕГИЧЕСКОГО ПАРТНЕРСТВА

Статья 10. **Основные направления обеспечения информационной безопасности государств – членов ОДКБ в сфере стратегической стабильности и равноправного стратегического партнерства**

Основными направлениями обеспечения информационной безопасности государств – членов ОДКБ в сфере стратегической стабильности и равноправного стратегического партнерства являются:

1) защита общих интересов и суверенитета государств – членов ОДКБ в международном информационном пространстве посредством осуществления согласования позиций, направленных на реализацию коллективных и национальных интересов государств – членов ОДКБ в информационной сфере;

2) участие государств – членов ОДКБ в формировании системы международной информационной безопасности, обеспечивающей эффективное противодействие использованию информационных технологий в военно-политических целях, противоречащих международному праву, а также в террористических, экстремистских, криминальных и иных противоправных целях;

3) создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве;

4) продвижение в рамках деятельности международных организаций согласованной коллективной позиции государств – членов ОДКБ, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере.

Глава 6. КОЛЛЕКТИВНАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Статья 11. **Правовое и организационное обеспечение безопасности критической информационной инфраструктуры**

Государство – член ОДКБ принимает меры к формированию и гармонизации с другими государствами – членами ОДКБ законодательства в области защиты критической информационной инфраструктуры.

Статья 12. **Содержание деятельности государств – членов ОДКБ по обеспечению информационной безопасности**

Деятельность государств – членов ОДКБ по обеспечению информационной безопасности включает в себя следующие основные направления:

1) прогнозирование, выявление, анализ и оценка угроз информационной безопасности;

2) определение основных направлений государственной политики и стратегическое планирование в области обеспечения информационной безопасности;

3) правовое регулирование в области обеспечения информационной безопасности;

4) разработка и применение комплекса оперативных и долговременных мер по выявлению, предупреждению и устранению угроз информационной безопасности, локализации и нейтрализации последствий их проявления;

5) разработка, производство и внедрение современных технологий защиты информации, а также техники двойного и гражданского назначения в целях обеспечения информационной безопасности;

6) организация научной деятельности в области обеспечения информационной безопасности;

7) финансирование расходов на обеспечение информационной безопасности, контроль за целевым расходованием выделенных средств;

8) международное сотрудничество в целях обеспечения коллективной информационной безопасности государств – членов ОДКБ;

9) взаимодействие государств – членов ОДКБ в сфере противодействия иностранным техническим разведкам и преступлениям в информационной сфере, включая обмен информацией о зарубежных деструктивных центрах в области информационной безопасности, а также об отдельных гражданах, участвующих в их деятельности;

10) гармонизация национальных нормативных документов государств – членов ОДКБ в области технической защиты информации и систем информационных технологий в части, не противоречащей законодательству государств – членов ОДКБ;

11) составление единого списка физических лиц, организаций, видов и составов киберинцидентов, с помощью которых осуществляются кибератаки на информационно-телекоммуникационные системы государств – членов ОДКБ, в целях предупреждения и заблаговременного пресечения злоумышленных действий указанных физических лиц и организаций;

12) реализация совместных образовательных программ, направленных на приобретение новых навыков и компетенций для обеспечения информационной безопасности, текущая подготовка, дополнительное образование и переподготовка государственного профессионального персонала и специалистов по защите критических информационных инфраструктур.

Статья 13. **Вступление в силу настоящего Закона**

Настоящий Закон вступает в силу после его официального опубликования.