

**Межпарламентская Ассамблея государств – участников  
Содружества Независимых Государств**

**МОДЕЛЬНЫЙ ЗАКОН  
Об информации, информатизации и обеспечении  
информационной безопасности**

**Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ**

**Статья 1. Цели и сфера действия настоящего Закона**

Настоящий Закон регулирует отношения в области создания и использования информационно-коммуникационных технологий в процессе информатизации жизнедеятельности общества, государства, человека, при осуществлении права на поиск, получение, распространение, передачу, использование информации и при обеспечении информационной безопасности.

Сферой действия настоящего Закона является деятельность по сближению национального законодательства и организации информационного взаимодействия субъектов в процессе формирования единого информационного пространства государств – участников Содружества Независимых Государств.

**Статья 2. Основные термины и понятия, используемые в настоящем Законе**

Для целей настоящего Закона используются следующие понятия:

*доступ к информации* – возможность получения информации и ее использования;

*защита информации* – деятельность, направленная на защиту прав субъектов на информацию, предотвращение несанкционированного доступа к ней и (или) утечки защищаемой информации, несанкционированных и (или) непреднамеренных воздействий на нее;

*информатизация* – организационный, социально-экономический и научно-технический процесс создания благоприятных условий для удовлетворения информационных потребностей, реализации прав и свобод субъектов информационной сферы, в основе которого лежит массовое применение информационных систем и технологий во всех видах деятельности физических и юридических лиц;

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

*информационная система* – организационно упорядоченная совокупность средств, реализующих определенные технологические действия посредством информационных процессов, предназначенных для решения конкретных функциональных задач;

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

*информационное пространство межгосударственного взаимодействия* – единое информационное пространство обмена информационными ресурсами, создания и размещения комплексных интегрированных информационных ресурсов по целям межгосударственного сотрудничества;

*информационно-коммуникационные технологии (ИКТ)* – информационные процессы и методы работы с информацией, осуществляемые с применением средств компьютерной техники и телекоммуникаций;

*информационные и телекоммуникационные ресурсы* – объекты информационной инфраструктуры, а также собственно информация, выделяемая по определенному признаку и формирующаяся по целям и потребностям субъекта информационных отношений;

*информационные технологии* – совокупность методов, производственных процессов и программно-технических средств, объединенных в технологический комплекс, обеспечивающий сбор, создание, хранение, накопление, обработку, поиск, вывод, копирование, передачу, распространение и защиту информации;

*информационный объект* – информация, обладающая заданной совокупностью атрибутов (реквизитов), которые позволяют использовать ее в информационных отношениях;

*информация* – сведения или данные о фактах, событиях, явлениях, процессах независимо от способа их представления;

*информация ограниченного доступа* – информация, доступ к которой ограничен законодательством государств либо их международными договорами;

*информация официальная* – информация, исходящая от органов государственной власти и органов местного самоуправления, других государственных и негосударственных органов и организаций, создаваемая, распространяемая и используемая в соответствии с правовым статусом ее источника;

*критически важная информационно-коммуникационная инфраструктура* – совокупность средств и систем формирования, создания, преобразования, передачи, использования и хранения информации, отказ или разрушение которых может оказать существенное отрицательное воздействие на национальную безопасность;

*несанкционированный доступ к информации* – доступ к защищаемой информации с нарушением прав или правил, установленных ее обладателем, владельцем и (или) законодательством государства;

*обеспечение информационной безопасности* – деятельность по разработке и реализации системы мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз в национальном и международном информационно-коммуникационном пространстве;

*персональные данные* – сведения или данные, позволяющие идентифицировать личность;

*сайт* – информационный объект в телекоммуникационной системе Интернета, предназначенный для размещения официальной или авторизованной информации с целью доступа к ней пользователей в телекоммуникационной сети по определенным сетевым адресам;

*сертификация* – форма подтверждения соответствия объектов оценки установленным требованиям;

*уполномоченный орган* – орган государства, наделенный соответствующей компетенцией и полномочиями, осуществляющий координацию деятельности в сфере информационной безопасности.

Иные термины и понятия, используемые в настоящем Законе, применяются в составе и значениях в соответствии с их использованием в национальном законодательстве.

### **Статья 3. Субъекты отношений в сфере действия настоящего Закона**

Субъектами отношений, реализующими права и полномочия в рамках настоящего Закона, являются:

– органы государственной власти и органы местного самоуправления государства;

– уполномоченные органы и организации в области формирования общих для государств – участников СНГ информационных ресурсов, ИКТ; межгосударственных интегрированных информационных систем; удостоверяющих центров электронной подписи; ситуационных и консультативных центров, других структур, обеспечивающих безопасное использование ИКТ;

– граждане и организации при реализации их прав и обязанностей в информационном пространстве социально-экономического, культурного и других областей сотрудничества государств – участников СНГ;

– государственные и общественные экспертные и контрольные органы и организации в области обеспечения информационной безопасности.

#### **Статья 4. Законодательство в области информации, информатизации и информационной безопасности**

Законодательство государств – участников СНГ по регулированию отношений в области информации, информатизации и информационной безопасности включает:

- модельный закон СНГ «Об информации, информатизации и обеспечении информационной безопасности»;
- национальное законодательство в области информации, информатизации и информационной безопасности государств – участников СНГ;
- нормативные правовые акты в области формирования и использования информации национального потенциала ИКТ в целях обеспечения прав и интересов граждан, деятельности органов государственной власти и органов местного самоуправления, учитывающие процессы формирования единого информационного пространства межгосударственного взаимодействия при обеспечении безопасности государства, общества, человека и гражданина;
- другие законы и подзаконные акты, затрагивающие отношения в информационном пространстве.

#### **Статья 5. Принципы правового регулирования отношений в рамках настоящего Закона**

Принципы правового регулирования отношений в рамках настоящего Закона предусматривают:

- обеспечение свободы поиска, получения, передачи, обработки, распространения, использования и хранения информации, доступ к которой не ограничен законодательством государства;
- свободный доступ к официальной информации органов государственной власти и органов местного самоуправления при обеспечении ее достоверности, целостности, своевременности;
- ограничение доступа к информации и обеспечение ее конфиденциальности, устанавливаемые национальными законами государства;
- поддержание состояния безопасности информационных ресурсов, информационного обеспечения прав пользователей национальными и международными информационными системами;
- обеспечение соблюдения суверенитета государства и реализации норм международного права, норм национального законодательства в организации и реализации потенциала ИКТ в процессе информационного межгосударственного взаимодействия при регулировании отношений информационной безопасности государства, общества, человека и гражданина.

## **Статья 6. Основные принципы государственной политики в области информации, информатизации и обеспечения информационной безопасности**

1. Государственная политика информатизации направлена на повышение качества жизни граждан на основе применения информационных и телекоммуникационных технологий при реализации важнейших направлений жизни общества и выполнении управленческих функций, реализуемых всей системой органов государственной власти и органов местного самоуправления посредством использования продукции, создаваемой отраслью ИКТ. Государственная политика обеспечения информационной безопасности – это деятельность государственных органов по определению содержания (форм, методов, средств, задач, субъектов, функций и др.) мер обеспечения информационной безопасности и последовательности их реализации. Важнейшим объектом информационной безопасности при всех условиях должно являться сознание и психофизиологическое здоровье каждого человека и населения государства в целом.

2. Основные принципы государственной политики в области информации, информатизации и обеспечения информационной безопасности при соблюдении норм статьи 5 настоящего Закона, предусматривают:

- обеспечение прав и законных интересов граждан, институтов общества и государства в информационной среде и пространстве информационного взаимодействия национальных и межгосударственных информационных систем;
- социальную направленность стратегических целей, основных задач и мероприятий, проводимых в сфере информатизации;
- ликвидацию информационного неравенства в обществе, реализацию условий для развития информационного общества;
- обеспечение доступа широких слоев граждан к информационно-коммуникационным сетям, информационным системам и технологиям, к системам открытого доступа к информации;
- открытость политики информатизации и активное привлечение к этой деятельности представителей науки, высшей школы и предпринимателей, работающих в информационной сфере;
- безопасность создаваемых и используемых информационно-коммуникационных сетей, информационных технологий и систем;
- правовую, научную, техническую и экономическую обоснованность разрабатываемых и принимаемых решений;
- комплексность и системность подхода к разработке, созданию и использованию информационно-коммуникационных сетей, информационных технологий и систем;
- системный подход к организационно-правовому обеспечению использования информационных технологий в государственном управлении, перевод реализации функций административных структур на цифровые технологии;

- развитие международного сотрудничества и использование зарубежного опыта в сфере информатизации в целях обеспечения конкурентоспособности создаваемых товаров и услуг на отечественном и мировом рынках;
- развитие законодательства в сфере информации, информатизации и обеспечения информационной безопасности.

## **Глава 2. ИНФОРМАЦИЯ, ИНФОРМАЦИОННЫЕ РЕСУРСЫ, ОСНОВЫ ПРАВОВОГО РЕЖИМА ИНФОРМАЦИОННЫХ РЕСУРСОВ**

### **Статья 7. Информация и информационные ресурсы, виды и учет информационных ресурсов**

1. Информация может являться объектом публичных гражданских и иных правовых отношений.

1.1 Субъект информационных отношений формирует свои информационные ресурсы и распоряжается ими в соответствии со своим правовым статусом, с учетом видов информации и ее категорий по доступу; несет ответственность за ее безопасность и безопасное использование для общества и других субъектов информационных отношений.

1.2 Виды информационных ресурсов классифицируются в установленном государством порядке и могут формироваться по субъектам, создающим и использующим информацию, по целям их применения. Основные массивы информационных ресурсов подлежат учету в реестрах, регистрах и классификаторах, формируемых соответствующими органами исполнительной власти, архивами и библиотеками в электронном виде.

2. Формирование системы информационных ресурсов государства предусматривает создание информационных объектов, относимых к национальному достоянию; ведомственных (отраслевых) информационных ресурсов органов государственной власти и органов местного самоуправления в соответствии с их сферами ведения и полномочий; информационных ресурсов производственных, научных, образовательных, социальных, торговых, финансовых и прочих организаций; информационных ресурсов общественных объединений и организаций и установление их правового режима.

### **Статья 8. Основы правового режима информационных ресурсов**

1. Правовой режим информационных ресурсов устанавливается государством и должен соблюдаться всеми субъектами информационной деятельности и информационных отношений.

2. Правовой режим информационных ресурсов включает:

- соблюдение порядка документирования информации;
- установление права собственности на определенный информационный ресурс;

установление режима доступа и правил обеспечения безопасности этого информационного ресурса (объекта).

3. Документирование информации предусматривает:

– упорядочение номенклатуры информационных объектов, их представления в соответствующей информационной системе в письменном или электронном виде;

– установление порядка учета и легализации факта наличия информации;

– порядок контроля соблюдения правил работы с объектами оцифрованной, электронной, бумажной официальной и другой документированной информации в государственных, корпоративных, межгосударственных информационных системах, в структуре систем международного обмена информацией, включая информационное пространство межгосударственного взаимодействия;

– установление формы собственности и (или) исключительных прав на объекты интеллектуальной собственности, включаемые в структуру информационного ресурса (базы и банки данных, объекты авторских прав).

4. Право собственности на информационный объект реализуется через полномочия владения, распоряжения и пользования. Исключительные права авторов и других законных правообладателей на контент документа, данные или записи, содержащиеся в базах данных и других носителях информации, включаемых в информационную среду и информационное пространство межгосударственного взаимодействия, регулируются в соответствии с законодательством об интеллектуальной собственности. Легальность использования термина «обладатель» должна подтверждаться указанием на законность такого обладания.

5. Установление категории информационного объекта по доступу предполагает порядок создания и использования общедоступной информации и порядок регулирования работы с информацией ограниченного доступа; определение методов и форм обеспечения безопасности информационного ресурса и ответственности за нарушение правил работы с информационным ресурсом; установление видов и форм ответственности за нарушение правового режима информационных ресурсов или использование информационных объектов во вред правам и законным интересам граждан государства.

## **Статья 9. Правовой режим открытой (общедоступной) информации**

1. Правовой режим общедоступной информации предусматривает:

– обеспечение обнаружения и свободного распространения сведений официального характера, включающих: нормативно-правовую информацию, которая создается органами государственной власти в процессе их деятельности по управлению делами общества и государства; статистическую, экологическую, метеорологическую, миграционную информацию; информацию о состоянии социально-экономической и культурной жизни общества, о выборах и референдумах, о состоянии законности и правопорядка, об уровне преступности и другие виды информации, которая предоставляется соответствующими

органами через системы общественного доступа к интернет-среде и СМИ для информирования населения государства и международной общественности;

– соблюдение права каждого субъекта свободно знакомиться с информацией, составляющей общедоступные сведения. Право на ознакомление с общедоступными сведениями и их использование не может быть ограничено. Общедоступная информация в форме открытых данных распространяется в интернет-среде и не требует оформления процедур передачи трансграничного объекта;

– публичное предоставление информации национальными юридическими лицами, а также иностранными юридическими лицами, осуществляющими деятельность на территории государства, осуществляется в случаях и порядке, установленных национальным законодательством;

– порядок поиска и получения открытой и общедоступной информации устанавливается национальным законодательством государства путем разработки единого реестра общедоступной информации.

2. Получение общедоступной информации по запросу пользователя не может быть оформлено как платная услуга.

#### **Статья 10. Информация ограниченного доступа**

1. Информация, которая относится законом к государственным секретам, к конфиденциальной информации в форме коммерческой тайны, к служебной информации ограниченного распространения, к персональным данным, профессиональной тайне, а также к тайне личной жизни, требует соответствующей идентификации и установления порядка санкционированного доступа к ней.

2. Правила использования ограничительных грифов на соответствующих носителях информации ограниченного доступа регулируются национальным законодательством.

### **Глава 3. ИНФОРМАТИЗАЦИЯ, ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**

#### **Статья 11. Государственная политика в сфере информатизации**

1. Государственная политика в сфере информатизации направлена на создание условий для эффективного удовлетворения информационных потребностей личности, общества и государства на основе обеспечения доступа к информации и использования информационных систем и технологий.

2. Основными направлениями государственной политики в сфере информатизации являются:

– обеспечение эффективности и безопасности формирования и использования информационного пространства государства, формирование единого информационного пространства взаимодействия государств – участников СНГ;



- формирование, развитие и защита ИКТ, обеспечение их совместимости и взаимодействия в едином информационном пространстве;
- развитие и использование потенциала ИКТ, создание национального программного продукта;
- обеспечение национальной безопасности государства, безопасности граждан и организаций в сфере использования информационно-коммуникационных систем и информационных технологий;
- создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации, участия государства в международном сотрудничестве;
- обеспечение потребностей системы государственного и межгосударственного управления современными программными и коммуникационными средствами и технологиями.

3. В целях осуществления государственной политики в сфере создания и эксплуатации информационных систем и применения ИКТ органы государственной власти и органы местного самоуправления:

- участвуют в разработке и реализации государственных целевых программ в области развития информационного общества;
- формируют и реализуют перспективные и оперативные планы и программы в области совершенствования управления на основе освоения информационных технологий, упорядочения информационных ресурсов в области предоставления услуг населению, выполнения в электронном формате всех доступных информатизации функций и операций в системе их ведения и компетенции;
- участвуют в разработке решений о межгосударственном и межотраслевом информационном взаимодействии в рамках реализации программ сотрудничества государств – участников СНГ и с другими зарубежными партнерами;
- создают специализированные органы по оценке эффективности использования информационных технологий для инноваций в управленческих процессах.

## **Статья 12. Организационно-правовое обеспечение реализации государственной политики в сфере информатизации**

1. Механизмы организационного и правового обеспечения в сфере информатизации определяются в соответствии с государственной политикой как в области развития потенциала ИКТ, так и в области использования этого потенциала в системе государственного управления и обеспечения развития информационного общества с учетом укрепления межгосударственного информационного взаимодействия.

2. Организационное обеспечение информационно-коммуникационной инфраструктуры и развития национальной базы ИКТ реализуется в режиме научно-технического производства как структурная часть (сектор) государственной и мировой экономики.

3. Основными индикаторами успешной деятельности государственных и негосударственных структур в области информатизации являются: показатели освоения мирового и национального рынка, оценка работы по количественным показателям и получаемой прибыли, безопасность ИКТ и их применения для реализации потребностей общества и человека.

### **Статья 13. Формирование и структуризация информационного пространства**

1. Информационное пространство рассматривается как область информационного взаимодействия государств – участников СНГ, коммуникационные связи которых реализуются преимущественно через Интернет и государственные системы СМИ, телекоммуникационные системы, мобильные формы связи, локальные информационные системы межгосударственного и внутригосударственного общения.

2. Закон определяет порядок правового регулирования отношений в области двух взаимодействующих систем: информационной инфраструктуры ИКТ-отрасли и информационной инфраструктуры электронного управления, реализуемого всей совокупностью органов государственной власти и местного самоуправления в национальном информационном пространстве, а также в пространстве межгосударственного информационного взаимодействия государств – участников СНГ.

3. Законодательство государства предусматривает регулирование порядка распространения информации в Интернете с указанием лиц, осуществляющих деятельность по обеспечению функционирования информационно-коммуникационных систем, обеспечивающих прием, передачу, доставку или обработку электронных сообщений пользователей Интернета, а также определяет права и обязанности организатора распространения информации, владельца сайта и (или) страницы сайта.

4. Законодательство государства предусматривает порядок ведения реестра сайтов. В соответствии с настоящим Законом могут быть организованы информационные системы согласования структуры реестров сайтов.

### **Статья 14. Организационно-правовое обеспечение развития информационной инфраструктуры отрасли ИКТ**

1. Организационно-правовое регулирование в области производства и эксплуатации потенциала ИКТ формируется как комплексная и объединяющая государственные, корпоративные и частные производства и средства их обеспечения система, нацеленная на обеспечение конкурентоспособности отрасли информационно-коммуникационных технологий, на повышение качества жизни граждан, на развитие экономической, социально-политической, научно-образовательной и культурной сфер жизни общества.

2. Правительства государств – участников СНГ разрабатывают и принимают перспективные программы и планы развития отрасли ИКТ и контролируют их исполнение.

3. В части правового регулирования инфраструктуры отрасли ИКТ органами исполнительной власти решаются следующие задачи:

- упорядочение производственных, научно-производственных структур; структур сервисного характера (ситуационные, консультативные, сопровождающие, аналитические); органов, выполняющих контрольные функции (сертификация, лицензирование); юридических служб (договоры, конфликты, споры по производству, качеству продукции и рынку) и др.;

- обеспечение правил подготовки, профессиональной переподготовки и повышения квалификации специалистов для сферы ИКТ и всех видов специалистов, задействованных в интернет-среде (программисты, операторы, администраторы информационных систем, разного уровня провайдеры в информационном пространстве и др.), и субъектов, ответственных за безопасность информационной среды, специализированных и локальных информационных систем;

- разработка и внедрение правовых документов, определяющих статус органов, подразделений, должностные обязанности и ответственность специалистов в отраслевых и региональных системах управления;

- установление правил и режима работы сервисных, консультативных и сопровождающих структур по договорам с заказчиками, потребителями продукции ИКТ-сектора экономики;

- разработка и внедрение классификаторов и реестров продукции и сервисов, оказываемых на договорной основе сектором экономики и производства ИКТ пользователям и потребителям услуг;

- анализ состояния рынка продукции ИКТ в национальном и международном обороте.

## **Статья 15. Организационно-правовое регулирование информационной инфраструктуры системы государственного управления**

1. Организационно-правовое регулирование информационной инфраструктуры системы государственного управления решает задачи перевода функциональной деятельности аппарата государственного управления на использование ИКТ в целях электронизации процесса управления. Эта работа осуществляется в следующих направлениях:

- обеспечение перехода на электронный документ в процессе реализации функциональных обязанностей подразделений в системе конкретного органа;

- установление порядка использования электронной подписи;

- обеспечение режима и правил работы с информационными ресурсами, включая служебную и деловую информацию;

- создание информационных систем (баз и банков данных) документированной информации в соответствии со сферой ведения органа исполнительной власти и (или) органа местного самоуправления.

– создание автоматизированных (электронных) систем управления, на базе интеграции которых в отраслевых и региональных системах могут создаваться комплексные электронные системы государственного управления;

– установление согласованных по технологии и целевой ориентации информационно-коммуникационных взаимодействий органов и межведомственного обмена информацией с другими субъектами в управлении делами государства;

– создание информационных, справочных, информационно-консультационных систем с учетом правового режима информационных ресурсов для обеспечения информатизации функций государственного и муниципального управления (систем открытого доступа к информации, «сервисов одного окна» по предоставлению информационных услуг гражданам и организациям);

– создание систем сбора информации и конкретных общественных инициатив населения по совершенствованию работы органов государственной власти и органов местного самоуправления;

– осуществление иных функций по информатизации системы органов государственной власти: законодательных, исполнительных, судебной и других профилей работы по управлению делами государства и общества.

2. Оказание информационных услуг – предоставление открытой информации о деятельности органов государственной власти и органов местного самоуправления, официальной информации (данных) – обеспечивается в порядке функциональной деятельности государственных и муниципальных органов и должно осуществляться на безвозмездной основе.

3. В целях реализации программ по расширению применения в структурах государственного аппарата системы электронного управления создаются механизмы координации и согласования работы всех функциональных структур каждого органа и его контактов в электронной форме с другими органами системы управления, а также формируются подразделения, обеспечивающие экспертную оценку качества работы и получаемых результатов.

## **Статья 16. Взаимодействие органов государственного управления и органов местного самоуправления со структурами, создающими базу ИКТ**

1. Правовое регулирование отношений органов государственного управления и органов местного самоуправления как заказчиков продукции отрасли ИКТ с органами, компаниями, фирмами и другими организациями (исполнителями проектов информатизации государственного и местного управления) нацелено на установление ответственности каждого из участников за определенный компонент информатизации и на определение прав в распоряжении информационными ресурсами, которые находятся в обработке собственника информационной системы.

2. Отношения заказчика создания информационной системы, сайта и (или) заказчика услуг на обработку информации регулируются гражданско-

правовым договором с элементами публичной ответственности с учетом масштаба и среды распространения информации.

3. С учетом определяемых приоритетов планируемых и осуществляемых мероприятий по программам и планам информатизации соответствующими структурами управления формируются показатели (индикаторы) государственных программ с указанием целевых параметров по количеству и качеству достигаемых результатов.

### **Статья 17. Юридическое оформление отношений субъектов в процессе информатизации: договоры, соглашения, регламенты**

1. Органы государственной власти и органы местного самоуправления в процессе информатизации используют следующие механизмы взаимодействия между собой и с другими субъектами:

– взаимодействие органов и их подразделений в структуре одной отрасли управления реализуется на основе положений о них, принимаемых руководством отрасли (ведомством) локальных нормативных актов и регламентов по вопросам информационного взаимодействия в процессе реализации функций этих структур;

– оформление порядка информационного взаимодействия в структуре национальной системы органов государственной власти и органов местного самоуправления осуществляется на основе: законодательства государства; правоприменительных актов вышестоящих в системе управления органов; соглашений органов исполнительной власти между собой (публичных договоров) о порядке и условиях обмена необходимой и достаточной информацией при исполнении функций и операций, связанных с технологиями информатизации;

– отношения органов исполнительной власти с другими, не государственными, организациями по вопросам информатизации оформляются договорами с учетом их предмета как гражданско-правовые (договора подряда, услуг, купли-продажи, выполнения НИР или НИОКР), а также как публично-правовые (в случаях использования форм аутсорсинга и отношений с субъектами облачной обработки информации). Выбор формы договора определяется номенклатурой работ в области разработки, монтажа, пусконаладки и сопровождения объектов, предусмотренных как предмет договорных отношений.

2. Договор на работы, связанные с обработкой информационных ресурсов по заказу их собственника или распорядителя, в соответствии с гражданско-правовым законодательством государства не может предусматривать переход или распространение прав собственника на информационный объект, получаемый от заказчика и предоставляемый ему или соответствующим доверенным лицам в результате выполнения работ по обработке информационных ресурсов.

3. Отношения, связанные с выполнением информационных функций органов государственной власти или органов местного самоуправления, их части или комплекса операций, затрагивающих интересы и права третьих лиц (физи-

ческих или юридических лиц), должны оформляться публичным договором в одной из двух возможных форм:

– форма делегирования функции и соответствующих полномочий (в случае предоставления публичных услуг не самим органом, а другой государственной организацией, реализующей, например, функции «одного окна» или государственного многофункционального центра не в структуре органа исполнительной власти);

– форма смешанного (публично-гражданского) договора на выполнение информационных работ, предусмотренных статусом органа исполнительной власти, исполнителем, не входящим по своему правовому статусу в систему органов государственной власти или органов местного самоуправления. Форма такого договора разрабатывается по согласованию уполномоченных органов государств – участников СНГ.

4. С учетом пунктов 2, 3 настоящей статьи осуществляется регулирование отношений в процессе формирования межгосударственных информационных систем в национальных структурах управления, а также в процессе формирования и использования интегрированных регионально распределенных информационных систем в информационном пространстве СНГ.

#### **Глава 4. ОСНОВЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ОТВЕТСТВЕННОСТИ ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАТИЗАЦИИ**

##### **Статья 18. Организационно-правовое обеспечение политики в области информационной безопасности**

1. Политика в области обеспечения информационной безопасности, проводимая государствами – участниками СНГ, определяется стратегиями и концепциями формирования и развития информационного общества и обеспечения информационной безопасности национального потенциала ИКТ. Такая политика реализуется в рамках конкретных форм международного сотрудничества и взаимодействия при освоении и использовании информационного пространства, при поддержании состояния безопасности общественных отношений в области создания и использования ИКТ, информационных и телекоммуникационных ресурсов, при защите интересов личности, общества и государства с максимальным учетом воздействия факторов проявления внутренних и внешних угроз.

2. Обеспечение информационной безопасности рассматривается как деятельность государственных органов и организаций по поддержанию состояния устойчивого функционирования информационной и коммуникационной инфраструктуры, защищенности информационных ресурсов, индивидуального и общественного сознания, стабильного безопасного информационного функцио-

нирования и развития всех социальных и государственных институтов и механизмов в едином информационном пространстве.

3. Обеспечение информационной безопасности включает систему мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз.

4. Организационно-правовое регулирование обеспечения информационной безопасности рассматривается как важнейший институт информационного права и законодательства. Развитие и совершенствование правового регулирования обеспечения информационной безопасности в рамках СНГ осуществляется путем принятия модельных законов и гармонизации законодательства государств – участников СНГ в сфере информационной безопасности.

### **Статья 19. Направления, цели и задачи обеспечения информационной безопасности**

1. Направления обеспечения информационной безопасности охватывают программные решения в области развития информационного общества и обеспечения национальной безопасности государства. Они реализуются через перспективные программы и планы развития информационного общества и интегрируют проблемы безопасности информационного пространства.

2. Целями обеспечения информационной безопасности являются:

- обеспечение реализации конституционных прав и свобод граждан в информационной сфере с учетом соблюдения установленных государством гарантий доступа к информации и форм ее использования;

- создание условий для безопасного поступательного развития информационного общества и применения потенциала ИКТ в процессах информатизации;

- информационное обеспечение всех направлений национальной безопасности и поддержание суверенитета государства;

- противодействие распространению вредной для общества и человека информации;

- безопасность формирования и использования систем международного информационного пространства в рамках региональных и других форм международного информационного сотрудничества.

3. В целях обеспечения информационной безопасности государство решает задачи создания отрасли производства средств информатизации, обеспечения безопасности программного обеспечения всех форм информатизации и связи, обеспечения контроля качества используемого национального и импортного информационного продукта.

4. Государство создает инфраструктуру управления процессами информатизации с учетом их отраслевого, регионального и местного значения и форми-

рует структуры, ответственные за состояние информационно-коммуникационной инфраструктуры страны.

5. Координацию деятельности системы обеспечения информационной безопасности и оценку состояния обеспечения безопасности по всем направлениям развития информационного общества, включая направления международного сотрудничества и взаимодействия в информационном пространстве межгосударственного взаимодействия, осуществляет уполномоченный государственный орган по обеспечению информационной безопасности.

## **Статья 20. Методы организационно-правового регулирования обеспечения информационной безопасности**

Методы организационно-правового регулирования обеспечения информационной безопасности включают:

- методы и правовые средства охраны и защиты информационных ресурсов с учетом их категорий по доступу и видам информации;
- защиту прав и законных информационных интересов граждан, организаций и органов государственной власти в информационном пространстве государства с учетом соблюдения установленных государством гарантий доступа к информации;
- защиту от распространения по каналам массовых коммуникаций (включая социальные сети Интернета, СМИ, рекламу) информации, способной причинить вред обществу и человеку;
- методы и правовые средства охраны и защиты информационных систем с учетом их статуса и режима использования;
- специальные методы обеспечения безопасности объектов критически важной информационно-коммуникационной инфраструктуры;
- методы предотвращения несанкционированного доступа к информационным ресурсам, а также специальные меры (и порядок их реализации) по ликвидации возможных деструктивных последствий осуществления противоправных деяний, предусмотренные законодательством государства;
- создание, нормативное обеспечение и координация деятельности соответствующих национальных и межгосударственных органов и организаций в области информационного взаимодействия и реализации политики в сфере информационной безопасности.

## **Статья 21. Обеспечение безопасности информационно-коммуникационной инфраструктуры**

Информационно-коммуникационную инфраструктуру образует совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации. Обеспечение безопасности информационно-коммуникационной инфраструктуры осуществляется посредством осуществления комплекса мер:



- применение методов, средств и мер организационной, правовой и технической охраны и защиты;
- лицензирование отдельных видов деятельности по созданию и обслуживанию элементов и объектов информационно-коммуникационной инфраструктуры;
- установление требований к надежности и безопасности аппаратных и программных средств и их сертификация, проверка соответствия указанным требованиям;
- установление предписаний на обязательное использование определенных средств и элементов информационно-коммуникационной инфраструктуры;
- установление ограничения оборота отдельных видов аппаратных и программных средств, используемых на объектах информационно-коммуникационной инфраструктуры;
- установление специальных требований к необходимому уровню квалификации лиц, осуществляющих отдельные виды деятельности на объектах информационно-коммуникационной инфраструктуры;
- выделение объектов критически важной информационно-коммуникационной инфраструктуры, установление и нормативное закрепление дополнительных требований к обеспечению их безопасности;
- установление государственного контроля качества осуществления мер обеспечения безопасности информационно-коммуникационной инфраструктуры.

## **Статья 22. Обеспечение информационной безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Критически важную информационно-коммуникационную инфраструктуру образует совокупность территориально распределенных государственных и корпоративных информационных систем, сетей связи, средств коммутации и управления информационными потоками, являющихся жизненно важными для государства, отказ или разрушение которых может оказать существенное отрицательное воздействие на национальную безопасность, а также организационных структур, обеспечивающих их эффективное функционирование.

2. В соответствии со стратегиями, программами, планами развития информационного общества и стратегией национальной безопасности государства соответствующие органы государственной власти определяют состав и порядок формирования перечней критически важных объектов информационно-коммуникационной инфраструктуры, требующих адекватных методов обеспечения безопасности, а также технологических, материальных, финансовых и кадровых ресурсов, необходимых для обеспечения требуемого состояния указанных объектов.

3. В целях обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры государство устанавливает

порядок их функционирования и осуществляет контроль за их состоянием и целевым использованием.

### **Статья 23. Защита информационных ресурсов, меры ограничения доступа**

1. Право на информацию – право свободно искать, получать, передавать, производить и распространять информацию любым законным способом – гарантируется национальным конституционным и информационным законодательством и международными правовыми нормами. Ограничения на реализацию этого права человека и гражданина и порядок доступа и работы с охраняемой информацией ограниченного использования устанавливаются законом.

2. Доступ к охраняемым информационным ресурсам и информационно-коммуникационным системам может ограничиваться как организационно-правовыми, так и организационно-техническими мерами.

2.1 Организационно-правовыми мерами ограничения доступа к информационно-коммуникационным системам и возможности последующей передачи информации из них является установление специального режима допуска на объекты (территорию и в помещения), где может реализовываться доступ к охраняемой информации; разграничение уровней доступа к информационным ресурсам по кругу лиц и характеру информации.

2.2. К организационно-техническим мерам ограничения доступа к информационно-коммуникационным системам и возможности передачи информации из них относятся меры физической, аппаратной и программной защиты информационно-коммуникационным систем, использование криптографических средств защиты информации, а также систем контроля доступа и протоколирования фактов доступа к информационно-коммуникационной системе.

3. Использование технических мер ограничения доступа к информационно-коммуникационным системам не должно причинять вред или создавать угрозу причинения вреда здоровью и имуществу граждан.

### **Статья 24. Обеспечение безопасности информационной среды**

1. Официальная и иная открытая информация, исходящая от идентифицируемых субъектов, требует условий распространения и использования, которые исключают опасность нарушения ее доступности и целостности, способного повлечь за собой угрозу нанесения вреда пользователям этой информацией.

2. Правила классификации, определение видов и категорий информационных ресурсов, используемых в процессе функционирования информационных систем национального и межгосударственного значения, правила обеспечения безопасности их использования должны предусматривать:

– закрепление прав на информационные ресурсы и определение правового статуса субъектов относительно форм работы с информационными ресурсами;

- защиту информационных ресурсов в соответствии со статьей 23 настоящего Закона и нормами национального законодательства государств – участников СНГ по вопросам правового режима, категорий и видов информационных ресурсов, правил работы с информацией;
- обеспечение соблюдения установленного порядка доступа и работы с открытой и общедоступной информацией;
- определение категорий информации ограниченного доступа, соблюдение норм законодательства о защите государственной и иных охраняемых законом тайн и других категорий информации ограниченного доступа;
- установление правил работы с персональными данными в органах государственной власти, управления и в организациях независимо от их формы собственности и правового статуса;
- протоколирование и учет противоправных деяний в отношении информации и прав субъектов на информацию, анализ эффективности применения мер ответственности к правонарушителям установленного порядка и правил работы с информацией.

## **Статья 25. Защита от распространения вредной и использования деструктивной информации**

1. Запрещается распространение информации, нарушающей права и законные интересы граждан и организаций, и информации, оказывающей деструктивное воздействие на индивидуальное, групповое или общественное сознание, подрывающей национальную безопасность.

1.1 Информацией, распространение которой нарушает права и законные интересы граждан и организаций, являются: заведомо ложная, позорящая, унижающая честь и достоинство личности информация; сведения, дискредитирующие деловую репутацию хозяйствующего субъекта; ложные сведения о товарах и услугах; заведомо ложное сообщение, в том числе об опасности; информация, содержащая угрозы причинения вреда правам и интересам лица, в том числе угрозу убийства или причинения другого вреда здоровью, угрозу уничтожения имущества; иная информация при отсутствии возможности отказаться от ее получения.

1.2 К информации, оказывающей деструктивное воздействие на индивидуальное, групповое или общественное сознание, подрывающей национальную безопасность, следует относить: информацию экстремистского, порнографического характера; информацию, пропагандирующую культ насилия и жестокости, содержащую призывы к насильственному свержению конституционного строя, организации или проведению массовых беспорядков; информацию, пропагандирующую войны, социальную, национальную, религиозную и расовую вражду или рознь; информацию, включающую угрозу совершения акта терроризма; сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ, их прекурсоров и аналогов, а также взрывчатых веществ и огнестрельного оружия.

2. Официальная и иная открытая информация, исходящая от идентифицируемых субъектов в информационном пространстве, требует условий распространения и использования, исключающих опасность ее искажения и нанесения вреда объектам и субъектам – пользователям такой информации, информационных и телекоммуникационных ресурсов.

3. Запрещается несанкционированное обладателем распространение информации, которая может нарушать его права и законные интересы.

4. Порядок функционирования источников информирования населения, определяемый национальным законодательством и органами саморегулирования средств массовой информации и коммуникаций, должен предусматривать соблюдение требования аутентификации публикуемой и распространяемой информации.

### **Статья 26. Виды и формы юридической ответственности за правонарушения в области информационных отношений**

1. Юридическая ответственность за правонарушения в области информационных отношений устанавливается нормами уголовного, административного, гражданского и трудового законодательства.

2. Для рассмотрения конфликтов и нарушений договорных отношений в области информационного взаимодействия и информационной безопасности государства – участники СНГ могут создавать третейский или арбитражный суд. Прецеденты, связанные с нарушением международного права в области защиты прав человека, могут рассматриваться соответствующими международными судами.

3. Защита прав субъектов информационных отношений при нарушении законодательства в области интеллектуальной собственности при их использовании в информационно-коммуникационном пространстве Интернета и взаимодействие субъектов государств – участников СНГ осуществляются в соответствии с национальными законами об интеллектуальной собственности.

Принят на сорок первом  
пленарном заседании  
Межпарламентской Ассамблеи  
государств – участников СНГ  
(постановление № 41-15 от 28 ноября 2014 года)