Приложение
к постановлению ПА ОДКБ
от 19 декабря 2023 года № 16-6.2

МОДЕЛЬНЫЙ ЗАКОН ОДКБ
«О защите информации и кибербезопасности»

Настоящий модельный закон ОДКБ разработан с целью сближения и гармонизации правового регулирования в области обеспечения защиты информации и кибербезопасности в государствах – членах Организации Договора о коллективной безопасности (далее – ОДКБ).

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

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

В настоящем модельном законе используются следующие основные термины и их определения:

защита информации – комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;

информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

информационная сеть – совокупность информационных систем либо комплексов программно-технических средств информационной системы, взаимодействующих посредством сетей электросвязи;

информационная система – совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;

информационные отношения – отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий;

информация ограниченного распространения – информация, доступ к которой ограничен законодательством государства – члена ОДКБ, включая информацию о частной жизни физических лиц и персональные данные, банковскую, врачебную, налоговую и нотариальную тайны, а также тайну голосования, телефонные и иные сообщения, сведения о страховании и усыновлении;

информационный ресурс – организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах;

кибербезопасность – состояние защищенности объектов информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз;

кибератака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

киберинцидент – событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политики безопасности;

объекты информационной инфраструктуры – информационные сети, информационные системы, информационные ресурсы и иные совокупности технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации, принадлежащие государственным органам и иным организациям на праве собственности, хозяйственного ведения, оперативного управления или на ином законном основании, за исключением объектов информатизации, предназначенных для обработки информации, содержащей государственные секреты.

Статья 2. **Предмет регулирования настоящего модельного закона**

1. Настоящий модельный закон регулирует информационные отношения, связанные с обеспечением защиты информации и кибербезопасности в государстве – члене ОДКБ.

2. Действие настоящего модельного закона распространяется на все юридические лица и государственные органы (организации) государства – члена ОДКБ, являющиеся субъектами обеспечения защиты информации и кибербезопасности, в том числе на организации и ведомства, которые подчиняются субъекту обеспечения защиты информации и кибербезопасности или связаны с данным субъектом иными договорными отношениями и которые обеспечивают доступ к информационным системам и ресурсам в пределах данных отношений.

3. Действие настоящего модельного закона не распространяется:

1) на отношения и услуги, связанные с содержанием обрабатываемой (передаваемой, хранящейся) информации в информационных системах;

2) на объекты информатизации и информационные системы, предназначенные для обработки информации, содержащей государственные секреты;

3) на социальные сети, частные электронные информационные ресурсы в сети Интернет (включая блог-платформы, видеохостинги, другие веб-ресурсы), если такие информационные ресурсы не содержат информации, необходимость защиты которой установлена законодательством,

на отношения и услуги, связанные с функционированием таких сетей и ресурсов.

Статья 3. **Правовое регулирование отношений в сфере защиты информации и кибербезопасности**

1. Государственное регулирование и управление в сфере защиты информации и кибербезопасности осуществляются главой государства (правительством) и уполномоченным государственным органом (организацией) государства – члена ОДКБ.

2. Государственное регулирование отношений в сфере защиты информации и кибербезопасности осуществляется путем определения мер по защите информации и кибербезопасности, а также ответственности за нарушение законодательства государства – члена ОДКБ о защите информации и кибербезопасности.

3. Законодательство о защите информации и кибербезопасности основывается на конституции государства – члена ОДКБ и состоит из настоящего модельного закона, иных нормативных правовых актов государства – члена ОДКБ.

4. Если международным договором, ратифицированным государством – членом ОДКБ в установленном порядке, определены иные правила, чем те, которые содержатся в настоящем модельном законе, то государство – член ОДКБ вправе применять правила международного договора.

Глава 2. ЗАЩИТА ИНФОРМАЦИИ

Статья 4. **Цели защиты информации**

Основными целями государственной политики в области защиты информации являются:

1) обеспечение прав субъектов информационных отношений при создании, использовании и эксплуатации информационных систем и информационных сетей, использовании информационных технологий, а также формировании и использовании информационных ресурсов;

2) сохранение и неразглашение информации ограниченного распространения, содержащейся в информационных системах;

3) недопущение неправомерного доступа, уничтожения, модификации, копирования, распространения и (или) предоставления информации, блокирования правомерного доступа к информации, а также иных неправомерных действий.

Статья 5. **Основные принципы защиты информации**

Защита информации основывается на следующих основных принципах:

1) персональная ответственность руководителя организации за организацию работ по защите информации в организации;

2) минимизация обязательных требований по защите информации;

3) обеспечение эффективного контроля за соблюдением законодательства в сфере защиты информации;

4) обеспечение информационной открытости проводимой органом государственного регулирования политики в сфере защиты информации (принцип информационной открытости).

Статья 6. **Субъект защиты информации и объект отношений в сфере защиты информации**

1. Субъектом защиты информации является собственник (владелец) информационных систем, в которых обрабатывается информация ограниченного распространения.

2. Иные собственники (владельцы) информационных систем, за исключением указанных в части 1 настоящей статьи, вправе руководствоваться требованиями настоящего модельного закона, если иное не предусмотрено законодательными актами государства – члена ОДКБ.

3. Объектом отношений в сфере защиты информации является информация ограниченного распространения, обрабатываемая в информационной системе (сети).

Статья 7. **Меры по защите информации**

1. К правовым мерам по защите информации относятся действующие законы, указы, нормативные правовые и правовые акты государства – члена ОДКБ, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушение этих правил.

2. К организационным мерам по защите информации относятся обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к информации (материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации, определение правил и процедур выполнения мероприятий по защите информации.

3. К техническим мерам по защите информации относятся меры по использованию средств защиты информации, а также меры по контролю защищенности информации ограниченного распространения, которые должны предусматривать:

1) предотвращение неправомерных доступа, уничтожения, модификации, копирования, предоставления и распространения информации ограниченного распространения;

2) обнаружение и предупреждение угроз информационной безопасности и принятие мер по предупреждению и уменьшению рисков информационной безопасности;

3) недопущение реализации угроз информационной безопасности в отношении информационных систем, а также восстановление

их функционирования в случае такого воздействия;

4) безопасное информационное взаимодействие с иными информационными системами.

4. Требования по защите общедоступной информации могут устанавливаться в целях недопущения ее уничтожения, модификации, блокирования правомерного доступа к ней.

Статья 8. **Функции субъекта защиты информации**

1. Организации – собственники (владельцы) информационных систем, предназначенных для обработки информации ограниченного распространения, в целях обеспечения защиты информации:

1) обеспечивают проведение мероприятий по проектированию и созданию систем защиты информации указанных информационных систем в порядке, предусмотренном законодательством государства – члена ОДКБ в сфере защиты информации;

2) организуют и проводят комплекс организационно-технических мероприятий по аттестации систем защиты информации;

3) осуществляют методическое руководство проведением мероприятий по защите информации организациями, находящимися в их подчинении (входящими в их состав, систему), а также хозяйственными обществами, акции (доли в уставных фондах) которых принадлежат государству – члену ОДКБ либо административно-территориальной единице и переданы в управление указанных организаций.

2. Работы по защите информации в организации проводятся подразделением защиты информации или иным подразделением (должностным лицом), ответственным за обеспечение защиты информации. Работники такого подразделения (должностное лицо) должны иметь высшее образование в области защиты информации либо высшее или профессионально-техническое образование и пройти переподготовку или повышение квалификации по вопросам защиты информации в порядке, установленном законодательством государства – члена ОДКБ.

3. В случае невозможности выполнения работ по защите информации силами подразделения защиты информации или иными подразделениями (должностными лицами), ответственными за обеспечение защиты информации, руководителем организации могут привлекаться организации, имеющие специальные разрешения (лицензии) на деятельность по защите информации и в части соответствующих составляющих данный вид деятельности работ и услуг, в порядке, установленном законодательством государства – члена ОДКБ.

4. Не допускается эксплуатация информационных систем, предназначенных для обработки информации ограниченного распространения, без реализации мер по защите информации.

5. При осуществлении защиты информации используются средства защиты информации, имеющие сертификат соответствия национальной системы подтверждения соответствия государства – члена ОДКБ.

6. Особенности криптографической защиты информации в информационных системах, в которых обрабатываются электронные документы, могут устанавливаться законодательством государства – члена ОДКБ об электронном документе и электронной цифровой подписи.

7. Персональную ответственность за организацию работ по защите информации в организации – собственнике (владельце) информационных систем, предназначенных для обработки информации ограниченного распространения, несет руководитель организации.

Глава 3. КИБЕРБЕЗОПАСНОСТЬ

Статья 9. **Цели кибербезопасности**

Основной целью государственной политики в области кибербезопасности является повышение уровня защиты объектов информационной инфраструктуры государства – члена ОДКБ от внешних и внутренних угроз национальной безопасности в информационной сфере, в том числе:

1) достижение максимальной скоординированности действий государственных органов и иных организаций по обнаружению, предотвращению и минимизации последствий кибератак на объекты информационной инфраструктуры;

2) постоянный поиск потенциальных уязвимостей национального сегмента глобальной компьютерной сети Интернет государства – члена ОДКБ;

3) проведение анализа информации о кибератаках и вызванных ими киберинцидентах, установление причин киберинцидентов;

4) оценка эффективности защиты объектов информационной инфраструктуры от кибератак;

5) прогнозирование ситуации в области обеспечения кибербезопасности объектов информационной инфраструктуры.

Статья 10. **Основные принципы обеспечения кибербезопасности**

Основными принципами обеспечения кибербезопасности являются:

1) законность;

2) приоритет защиты интересов личности, общества и государства в киберпространстве;

3) единый подход к регулированию сферы кибербезопасности;

4) приоритет участия производителей государства – члена ОДКБ в создании системы кибербезопасности;

5) открытость государства – члена ОДКБ для международного сотрудничества в обеспечении кибербезопасности.

Статья 11. **Субъекты и объекты кибербезопасности**

1. Субъектами кибербезопасности являются государственные органы (организации) государства – члена ОДКБ, юридические лица или индивидуальные предприниматели, имеющие определенные права и обязанности, которые связаны с владением, пользованием и распоряжением объектами информационной инфраструктуры.

2. Объектами кибербезопасности являются комплексы информационных систем, используемые в деятельности по обеспечению защиты информации и кибербезопасности информационных систем и ресурсов, в том числе объекты информационной инфраструктуры.

Статья 12. **Основные меры по обеспечению кибербезопасности**

1. Государственные органы (организации) государства – члена ОДКБ, юридические лица или индивидуальные предприниматели, имеющие определенные права и обязанности, которые связаны с владением, пользованием и распоряжением объектами информационной инфраструктуры, обеспечивают:

1) предотвращение несанкционированного доступа к объектам информационной инфраструктуры, а также к обрабатываемой на объектах информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации, незамедлительное информирование уполномоченного государственного органа (организации) по вопросам обеспечения кибербезопасности государства – члена ОДКБ;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации, обрабатываемой на объектах информационной инфраструктуры;

4) недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование объекта информационной инфраструктуры;

5) восстановление функционирования объекта информационной инфраструктуры, подвергшегося кибератаке, а также информации, подвергшейся воздействию вследствие несанкционированного доступа к ней;

6) осуществление постоянного контроля за обеспечением защищенности объекта информационной инфраструктуры;

7) применение средств защиты информации, прошедших процедуру подтверждения соответствия в соответствии с законодательством государства – члена ОДКБ;

8) принятие иных правовых, организационных и технических мер с целью обеспечения кибербезопасности объектов информационной инфраструктуры в соответствии с законодательством государства – члена ОДКБ.

2. Государственные органы (организации) государства – члена ОДКБ, юридические лица или индивидуальные предприниматели, имеющие определенные права и обязанности, которые связаны с владением,

пользованием и распоряжением объектами информационной инфраструктуры, обязаны содействовать уполномоченному государственному органу по вопросам обеспечения кибербезопасности государства – члена ОДКБ и сообщать известные им данные о киберугрозах объектам информационной инфраструктуры, кибератаках и (или) обстоятельствах, способствующих предотвращению, выявлению и пресечению таких угроз, противодействию киберпреступности, кибератакам и минимизации их последствий, а также осуществлять иные меры в соответствии с законодательством государства – члена ОДКБ в целях обеспечения кибербезопасности.

3. Граждане, в том числе иностранные граждане, лица без гражданства и объединения граждан вправе принимать меры, указанные в части 2 настоящей статьи.

Статья 13. **Национальная система обеспечения кибербезопасности государства – члена ОДКБ**

1. Для реализации мероприятий по обеспечению кибербезопасности создается национальная система обеспечения кибербезопасности государства – члена ОДКБ, элементами которой являются:

1) уполномоченный государственный орган (организация) по вопросам обеспечения кибербезопасности;

2) центр обеспечения кибербезопасности и реагирования на киберинциденты государства – члена ОДКБ;

3) центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры (далее – центры кибербезопасности);

4) уполномоченный оператор электросвязи по взаимодействию центра обеспечения кибербезопасности и реагирования на киберинциденты государства – члена ОДКБ, центров кибербезопасности (далее – оператор электросвязи);

5) объекты информационной инфраструктуры;

6) сети передачи данных, используемые для взаимодействия элементов национальной системы обеспечения кибербезопасности, указанных в пунктах 2 – 5 настоящей части;

7) иные элементы, необходимые для обеспечения кибербезопасности, предусмотренные законодательством государства – члена ОДКБ.

2. Порядок создания национальной системы обеспечения кибербезопасности определяется правительством государства – члена ОДКБ.

Статья 14. **Полномочия уполномоченного государственного органа (организации)**

Уполномоченный государственный орган (организация) по вопросам обеспечения кибербезопасности государства – члена ОДКБ осуществляет координацию деятельности других государственных органов и иных организаций по созданию и функционированию национальной системы

обеспечения кибербезопасности, а также:

1) определяет требования по кибербезопасности объектов информационной инфраструктуры;

2) устанавливает состав технических параметров киберинцидента, вырабатывает рекомендации по выявлению, предупреждению и исследованию кибератак, киберинцидентов, доводит их до сведения центров кибербезопасности;

3) определяет типовую структуру центров кибербезопасности и иные требования к ним, согласовывает назначение на должность руководителей таких центров, продление с ними трудового договора (контракта);

4) организует информационное взаимодействие элементов национальной системы обеспечения кибербезопасности, определяет порядок такого взаимодействия;

5) осуществляет сбор, обработку, накопление, систематизацию, хранение и поддержание в актуальном состоянии информации об элементах национальной системы обеспечения кибербезопасности;

6) информирует государственные органы и иные организации об угрозах в отношении принадлежащих им объектов информационной инфраструктуры и о необходимых мерах по нейтрализации данных угроз;

7) выступает заказчиком государственных научно-технических и иных программ и проектов, организует проведение научно-исследовательских, опытно-конструкторских и иных работ в области обеспечения кибербезопасности;

8) принимает участие в выполнении иных мероприятий по созданию и развитию национальной системы обеспечения кибербезопасности государства – члена ОДКБ;

9) выносит обязательные для исполнения предписания государственным органам и иным организациям об устранении выявленных нарушений норм настоящего модельного закона и иных актов законодательства государства – члена ОДКБ, а также требований по кибербезопасности объектов информационной инфраструктуры этих государственных органов (организаций). Порядок вынесения и исполнения указанных предписаний определяется правительством государства – члена ОДКБ.

Статья 15. **Полномочия центра обеспечения кибербезопасности и реагирования на киберинциденты государства – члена ОДКБ**

1. Центр обеспечения кибербезопасности и реагирования на киберинциденты государства – члена ОДКБ может являться структурным подразделением уполномоченного государственного органа (организации) по вопросам обеспечения кибербезопасности государства – члена ОДКБ.

2. Центр обеспечения кибербезопасности и реагирования на киберинциденты государства – члена ОДКБ:

1) взаимодействует с центрами кибербезопасности, формирует и ведет базу данных о киберинцидентах;

2) координирует и реализует мероприятия по выявлению, предупреждению и исследованию кибератак и вызванных ими киберинцидентов на объектах информационной инфраструктуры, реагированию на такие киберинциденты;

3) осуществляет автоматизированные сбор, обработку, накопление, систематизацию и хранение данных о кибербезопасности объектов информационной инфраструктуры;

4) оказывает методическую и практическую помощь субъектам кибербезопасности в вопросах обеспечения кибербезопасности принадлежащих им объектов информационной инфраструктуры;

5) проводит учения по действиям при возникновении киберинцидентов на объектах информационной инфраструктуры, разрабатывает программы и методики проведения этих учений, сценарии реагирования на кибератаки;

6) организует проведение аналитических и научных исследований в области обеспечения кибербезопасности, при необходимости распространяет результаты таких исследований, в том числе в средствах массовой информации.

Статья 16. **Полномочия центров кибербезопасности**

1. Центры кибербезопасности:

1) осуществляют автоматизированные сбор, обработку, накопление, систематизацию и хранение данных о кибербезопасности объектов информационной инфраструктуры, реагирование на киберинциденты;

2) проводят оценку степени защищенности объектов информационной инфраструктуры, мероприятия по установлению причин киберинцидентов, вызванных кибератаками на объекты информационной инфраструктуры;

3) осуществляют сбор, обработку, анализ и обобщение информации о состоянии кибербезопасности на объектах информационной инфраструктуры;

4) информируют центр обеспечения кибербезопасности и реагирования на киберинциденты государства – члена ОДКБ о выявленных киберинцидентах не позднее одного часа с момента их выявления, а также представляют сведения, в том числе о результатах реагирования и ликвидации последствий киберинцидента, в порядке, объеме и сроки, определяемые уполномоченным государственным органом (организацией);

5) обеспечивают функционирование в своем составе команд реагирования на киберинциденты.

2. Центры кибербезопасности организуют повышение квалификации руководящих работников и специалистов, в обязанности которых входит

обеспечение кибербезопасности, в порядке и сроки, определяемые уполномоченным государственным органом государства – члена ОДКБ.

3. До начала функционирования центры кибербезопасности подлежат аттестации. Порядок проведения аттестации определяется уполномоченным государственным органом государства – члена ОДКБ.

Статья 17. **Полномочия оператора электросвязи**

Оператор электросвязи обеспечивает оказание государственным органам (организациям), юридическим лицам или индивидуальным предпринимателям, имеющим определенные права и обязанности, связанные с владением, пользованием и распоряжением объектами информационной инфраструктуры, услуг электросвязи, необходимых для организации информационного взаимодействия этих органов (организаций), юридических лиц или индивидуальных предпринимателей с центром обеспечения кибербезопасности и реагирования на киберинциденты государства – члена ОДКБ и центрами кибербезопасности.

Глава 4. ПОДДЕРЖКА И РАЗВИТИЕ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ

Статья 18. **Государственная поддержка субъектов кибербезопасности**

Государственной поддержкой субъектов кибербезопасности могут являться:

1) предоставление субъектам кибербезопасности льгот и преференций в соответствии с законодательством государства – члена ОДКБ, ограничение прибыли для организаций, предоставляющих услуги субъектам кибербезопасности;

2) создание условий для привлечения средств хозяйствующих субъектов в целях финансирования сферы кибербезопасности;

3) разработка и реализация государственных программ в сфере кибербезопасности, нацеленных на обеспечение гарантированного внедрения продуктов и передовых технологий, основанных на научно-технических достижениях организаций государства – члена ОДКБ;

4) оказание содействия в подготовке и переподготовке кадров в сфере кибербезопасности, а также повышении их квалификации.

Статья 19. **Поддержка научно-технической и инновационной деятельности в сфере кибербезопасности**

Поддержка научно-технической и инновационной деятельности в сфере кибербезопасности осуществляется органами государственного управления и хозяйствующими субъектами государства – члена ОДКБ посредством:

1) размещения заказа на выполнение научно-исследовательских, опытно-конструкторских и технологических работ в рамках государственного заказа;

2) выделения субсидий субъектам кибербезопасности для финансирования научно-исследовательских, опытно-конструкторских и технологических работ, проводимых в процессе реализации инвестиционных проектов, в том числе для исследования возможности использования технологии искусственного интеллекта в целях обеспечения кибербезопасности;

3) стимулирования спроса на инновационную продукцию, в том числе оптимизации закупаемых для государственных нужд товаров (работ, услуг);

4) оказания финансовой помощи организациям, реализующим проекты по повышению уровня кибербезопасности, в том числе занимающимся инновационной деятельностью в сфере услуг с использованием передовых технологий;

5) создания условий для осуществления научной, научно-технической и инновационной деятельности в сфере кибербезопасности и обеспечения кибербезопасности объектов информационной инфраструктуры;

6) предоставления приоритета продукции производства государства – члена ОДКБ при реализации государственных программ, связанных с обеспечением кибербезопасности.

Статья 20. **Развитие и поддержка кадрового потенциала в сфере обеспечения кибербезопасности**

1. Развитие и поддержка кадрового потенциала органов государственного управления и хозяйствующих субъектов государства – члена ОДКБ в сфере обеспечения кибербезопасности может осуществляться посредством:

1) предоставления финансовой, информационно-консультационной помощи организациям, осуществляющим деятельность по подготовке, переподготовке и повышению квалификации кадров в сфере обеспечения кибербезопасности;

2) оказания учебно-методической и научно-педагогической помощи в сфере обеспечения кибербезопасности.

2. Работники, ответственные за обеспечение кибербезопасности, на постоянной основе должны повышать свою квалификацию в соответствии со стандартами и требованиями государства – члена ОДКБ.

Глава 5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Статья 21. **Международное сотрудничество в сфере защиты информации и кибербезопасности**

1. Уполномоченный государственный орган (организация) в пределах своих полномочий осуществляет международное сотрудничество в сфере защиты информации и кибербезопасности.

2. Международное сотрудничество в сфере защиты информации и кибербезопасности осуществляется в соответствии с настоящим модельным законом и международными договорами государства – члена ОДКБ.

3. Международное сотрудничество включает в себя сотрудничество уполномоченного органа (организации) государства – члена ОДКБ с международными организациями и иностранными государствами.

Статья 22. **Ответственность за нарушение законодательства о защите информации и кибербезопасности**

Лица, виновные в нарушении законодательства о защите информации и кибербезопасности, несут ответственность в порядке, определяемом в соответствии с законодательством государства – члена ОДКБ.