Приложение
к постановлению ПА ОДКБ
от 19 декабря 2023 года № 16-6.1

МОДЕЛЬНЫЙ ЗАКОН ОДКБ
«О безопасности критической информационной инфраструктуры»

Настоящий модельный закон ОДКБ является правовым ориентиром для формирования системы правового регулирования в области обеспечения безопасности критической информационной инфраструктуры в государствах – членах Организации Договора о коллективной безопасности (далее – ОДКБ).

Статья 1. **Основные понятия, используемые в настоящем модельном законе**

В настоящем модельном законе используются следующие основные понятия:

автоматизированная система управления – комплекс программных и аппаратно-программных средств, предназначенных для управления и контроля за функционированием технологического и (или) производственного оборудования (исполнительных устройств), производственными процессами;

безопасность критической информационной инфраструктуры – состояние защищенности критической информационной инфраструктуры, позволяющее обеспечить ее нормальное функционирование в соответствии с предназначением при проведении в отношении нее компьютерных атак;

информационная инфраструктура – совокупность информационно-телекоммуникационных систем и автоматизированных систем управления конкретными объектами в государственной и частной сферах;

информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационно-телекоммуникационная система – информационная система, предназначенная для обработки, хранения и передачи информации по линиям связи;

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

компьютерная атака – целенаправленное вредоносное информационное воздействие на отдельные элементы или в целом на информационную инфраструктуру в целях нарушения, прекращения ее функционирования, уничтожения входящих в ее состав информации, программных, программно-аппаратных и аппаратных средств или создания угрозы таких последствий;

компьютерный (информационно-технологический) инцидент – нарушение, частичное или полное прекращение функционирования информационной инфраструктуры и (или) нарушение безопасности обрабатываемой таким объектом информации, в том числе вызванные компьютерной атакой;

критическая информационная инфраструктура – информационная инфраструктура, функционирующая в сферах обеспечения деятельности органов государственной власти, органов местного самоуправления, здравоохранения, науки, промышленности, транспорта, связи, финансов, производства энергии, добычи и транспортировки энергоресурсов и полезных ископаемых, экологически и ядерно опасных объектов и производств;

объекты критической информационной инфраструктуры – совокупность информационно-телекоммуникационных систем и автоматизированных систем управления в конкретных органах и организациях, в установленном порядке отнесенных к данной категории;

субъекты критической информационной инфраструктуры – государственные органы, органы местного самоуправления (муниципальные органы), юридические лица, индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные системы или автоматизированные системы управления.

Статья 2. **Государственная политика в области обеспечения безопасности критической информационной инфраструктуры**

1. Государственная политика в области обеспечения безопасности критической информационной инфраструктуры представляет собой совокупность экономических, организационных и правовых мер, направленных на обеспечение устойчивого функционирования критической информационной инфраструктуры, а также взаимодействие между государствами – членами ОДКБ по обеспечению единообразного организационного и технического уровня безопасности критической информационной инфраструктуры.

2. Государственная политика в области обеспечения безопасности критической информационной инфраструктуры осуществляется на основе следующих принципов:

1) законность;

2) уважение и соблюдение прав и свобод человека и гражданина;

3) соответствие мер государственного регулирования в области обеспечения безопасности критической информационной инфраструктуры существующим угрозам;

4) системный подход при реализации мероприятий, направленных на обеспечение безопасности критической информационной инфраструктуры;

5) презумпция угрозы компьютерных атак на объекты критической информационной инфраструктуры.

Статья 3. **Полномочия правительства государства по обеспечению безопасности критической информационной инфраструктуры**

1. Правительство государства устанавливает:

1) основные направления государственной политики в области обеспечения безопасности критической информационной инфраструктуры;

2) национальный государственный орган, ответственный за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры;

3) основные направления и содержание международного сотрудничества в области обеспечения безопасности критической информационной инфраструктуры;

4) основные задачи организаций, в которых функционируют объекты критической информационной инфраструктуры, по обеспечению безопасности таких объектов;

5) порядок и сроки категорирования объектов критической информационной инфраструктуры;

6) показатели критериев значимости объектов критической информационной инфраструктуры;

7) порядок осуществления государственного контроля в области обеспечения безопасности объектов критической информационной инфраструктуры;

8) порядок использования ресурсов государственной сети электросвязи для обеспечения бесперебойного функционирования объектов критической информационной инфраструктуры;

9) порядок подготовки, переподготовки и повышения квалификации кадров объектов критической информационной инфраструктуры и обеспечивает финансирование данной деятельности.

2. В зависимости от конституционной модели определения статуса и полномочий главы государства часть полномочий, указанных в части 1 настоящей статьи, может быть законом возложена на главу государства.

Статья 4. **Полномочия национального государственного органа, ответственного за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры**

Национальный государственный орган, ответственный за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, имеет следующие полномочия:

1) формирование и обеспечение устойчивого функционирования государственной системы обеспечения безопасности критической информационной инфраструктуры, включая государственную систему обнаружения, предупреждения и ликвидации компьютерных атак на критическую информационную инфраструктуру;

2) подготовка и внесение в установленном порядке предложений о совершенствовании нормативного правового регулирования в области обеспечения безопасности критической информационной инфраструктуры главе государства и в правительство государства;

3) определение порядка ведения, содержания и ведение государственного реестра объектов критической информационной инфраструктуры;

4) установление требований по обеспечению безопасности объектов критической информационной инфраструктуры;

5) осуществление координации деятельности органов государственной власти и организаций по вопросам обеспечения безопасности критической информационной инфраструктуры;

6) осуществление государственного контроля в области обеспечения безопасности объектов критической информационной инфраструктуры;

7) определение требований к средствам обеспечения безопасности критической информационной инфраструктуры, требований и технических условий по их установке и эксплуатации;

8) определение порядка проведения научных исследований в области обеспечения безопасности критической информационной инфраструктуры и субъектов, ответственных за осуществление данной деятельности.

Статья 5. **Категорирование объектов критической информационной инфраструктуры**

1. Категорирование объекта критической информационной инфраструктуры представляет собой процедуру, в результате которой:

1) определяется соответствие объекта критической информационной инфраструктуры установленным критериям значимости и их показателям;

2) осуществляется присвоение объекту критической информационной инфраструктуры определенной категории значимости;

3) осуществляются последующие проверки соответствия объекта критической информационной инфраструктуры присвоенной ему категории значимости.

2. Показатели критериев значимости объектов критической информационной инфраструктуры определяются правительством государства исходя из потенциального наступления в результате возникновения компьютерных инцидентов на объектах критической информационной инфраструктуры следующих негативных последствий:

1) причинение вреда жизни и (или) здоровью людей, прекращение или нарушение функционирования объектов обеспечения жизнедеятельности населения;

2) негативное влияние на интересы государства в области его внешней или внутренней политики;

3) ущерб обороне государства или его безопасности в целом или в отдельных отраслях;

4) прекращение или нарушение функционирования транспортной инфраструктуры, сетей связи;

5) прекращение снабжения энергией или топливом субъектов экономической деятельности;

6) ущерб экологии;

7) прекращение доступа граждан и организаций к государственным услугам;

8) ущерб государственному имуществу или имуществу организаций, а также ущерб бюджетам бюджетной системы государства и бюджетам организаций.

3. Исходя из уровня потенциального ущерба устанавливаются следующие категории объектов критической информационной инфраструктуры: первая, вторая и третья, где отнесение к первой категории представляет собой возможность наступления наибольших негативных последствий.

4. Установленная категория объекта критической информационной инфраструктуры может быть изменена или отменена в порядке, предусмотренном для категорирования, по следующим основаниям:

1) на основании мотивированного решения национального государственного органа, ответственного за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры;

2) при изменении вида деятельности объекта критической информационной инфраструктуры, в результате чего при нарушении или прекращении его функционирования более не могут наступать негативные последствия, указанные в части 2 настоящей статьи;

3) при ликвидации органа государственной власти или организации, вследствие чего прекращается функционирование объекта критической информационной инфраструктуры.

Статья 6. **Права и обязанности органов государственной власти, иных государственных органов и организаций, в которых функционируют объекты критической информационной инфраструктуры**

1. Органы государственной власти, иные государственные органы и организации, в которых функционируют объекты критической информационной инфраструктуры, имеют право:

1) получать от национального государственного органа, ответственного за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, информацию, необходимую для реализации задач обеспечения безопасности объектов критической информационной инфраструктуры, в том числе о средствах и методах проведения компьютерных атак, способах их предупреждения и обнаружения;

2) за счет бюджетных ассигнований или за свой собственный счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обеспечения безопасности объектов критической информационной инфраструктуры;

3) разрабатывать и осуществлять инициативные мероприятия по обеспечению безопасности объектов критической информационной инфраструктуры.

2. Органы государственной власти, иные государственные органы и организации, в которых функционируют объекты критической информационной инфраструктуры, обязаны:

1) в сроки, установленные национальным государственным органом, ответственным за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, информировать данный орган о происшедших компьютерных инцидентах и принятых мерах по ликвидации их последствий;

2) оказывать содействие должностным лицам национального государственного органа, ответственного за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов, повышении уровня безопасности объектов критической информационной инфраструктуры;

3) обеспечивать выполнение порядка, технических условий установки и эксплуатации средств, предназначенных для обеспечения безопасности объектов критической информационной инфраструктуры;

4) выполнять предписания должностных лиц национального государственного органа, ответственного за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, выданные в соответствии с их компетенцией;

5) обеспечивать беспрепятственный доступ должностным лицам национального государственного органа, ответственного за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, на объекты критической

информационной инфраструктуры и к информации об их функционировании при осуществлении данными лицами полномочий по государственному контролю.

Статья 7. **Основные задачи и требования по обеспечению безопасности объектов критической информационной инфраструктуры**

1. Основными задачами системы безопасности объекта критической информационной инфраструктуры являются:

1) недопущение вредоносного воздействия на программное обеспечение и технические средства обработки информации, эксплуатируемые на объекте критической информационной инфраструктуры, в результате которого возможно нарушение или прекращение функционирования такого объекта в целом или частично;

2) предотвращение противоправного доступа к информации, обрабатываемой на объекте критической информационной инфраструктуры, ее уничтожения, блокирования, копирования, модификации или распространения, а также иных противоправных действий;

3) оперативное восстановление полноценного функционирования объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет формирования резерва технических средств, а также создания резервных копий программного обеспечения и обрабатываемой информации.

2. Национальным государственным органом, ответственным за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, для каждой категории объектов критической информационной инфраструктуры определяются требования по обеспечению их безопасности.

Органы государственной власти и организации, по согласованию с национальным государственным органом, ответственным за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, вправе устанавливать дополнительные требования к эксплуатируемым у них объектам критической информационной инфраструктуры.

Статья 8. **Оценка уровня обеспечения безопасности критической информационной инфраструктуры**

1. Оценка уровня обеспечения безопасности критической информационной инфраструктуры в государстве в целом осуществляется национальным государственным органом, ответственным за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры.

2. Для осуществления работ по оценке уровня обеспечения безопасности критической информационной инфраструктуры национальному государственному органу, ответственному за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, по его запросам органами государственной власти и организациями предоставляются следующие сведения:

1) получаемые при использовании средств обеспечения безопасности объектов критической информационной инфраструктуры, включенных в государственный реестр таких объектов;

2) о нарушении требований по обеспечению безопасности объектов критической информационной инфраструктуры и принятых мерах по их устранению;

3) иные сведения, необходимые для формирования объективной оценки уровня обеспечения безопасности критической информационной инфраструктуры.

3. Для реализации задач по оценке уровня обеспечения безопасности объектов критической информационной инфраструктуры национальный государственный орган, ответственный за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, вправе осуществлять установку в сетях электросвязи, независимо от их принадлежности, технических средств, предназначенных для обнаружения признаков компьютерных атак.

Статья 9. **Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы**

1. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы является основной подсистемой государственной системы обеспечения безопасности критической информационной инфраструктуры.

2. Государственная система обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы представляет собой единый территориально распределенный организационный комплекс, распространяющий свою деятельность на всю территорию государства, а также на дипломатические и консульские учреждения, осуществляющие деятельность за пределами государства.

3. Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы образуют:

1) подразделения и должностные лица национального государственного органа, ответственного за функционирование

государственной системы обеспечения безопасности критической информационной инфраструктуры;

2) организации, создаваемые национальным государственным органом, ответственным за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, предназначенные для координации деятельности в данной области государственной деятельности, в том числе для координации деятельности органов государственной власти и организаций, в которых функционируют объекты критической информационной инфраструктуры, включенные в государственный реестр;

3) структурные подразделения и должностные лица органов государственной власти и организаций, в которых функционируют объекты критической информационной инфраструктуры, включенные в государственный реестр.

4. К основным средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, относятся программные, программно-аппаратные, технические и иные средства, предназначенные для поиска признаков и обнаружения компьютерных атак, их ликвидации и для обмена информацией, необходимой органам государственной власти и организациям, в которых функционируют объекты критической информационной инфраструктуры, при обнаружении, предупреждении и ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации.

5. Предоставление из государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы сведений, составляющих государственную тайну, а также конфиденциальной информации осуществляется в соответствии с законодательством государства.

Статья 10. **Государственный контроль в области обеспечения безопасности критической информационной инфраструктуры**

1. Государственной контроль в области обеспечения безопасности критической информационной инфраструктуры осуществляется в целях проверки соблюдения субъектами критической информационной инфраструктуры требований, установленных нормативными правовыми актами государства в области обеспечения безопасности критической информационной инфраструктуры.

2. Государственный контроль проводится путем осуществления национальным государственным органом, ответственным за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, плановых и внеплановых проверок.

3. Периодичность плановых проверок деятельности объектов критической информационной инфраструктуры устанавливается правительством государства.

4. Решение о проведении внеплановой проверки принимается национальным государственным органом, ответственным за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, по следующим основаниям:

1) необходимость оценки качества и полноты выполнения предписания об устранении выявленного нарушения требований по обеспечению безопасности объектов критической информационной инфраструктуры;

2) возникновение компьютерного инцидента, повлекшего за собой негативные последствия для безопасного функционирования объекта критической информационной инфраструктуры;

3) указание главы государства или председателя правительства государства о проведении внеплановой проверки функционирования объекта критической информационной инфраструктуры;

4) мотивированное требование прокуратуры об устранении нарушений законодательства.

5. По итогам проверки в случае выявления нарушения требований, установленных нормативными правовыми актами государства в области обеспечения безопасности критической информационной инфраструктуры, национальный государственный орган, ответственный за функционирование государственной системы обеспечения безопасности критической информационной инфраструктуры, выдает органу государственной власти или организации, в которых функционирует объект критической информационной инфраструктуры, предписание об устранении выявленного нарушения с указанием сроков его устранения.

6. Временное приостановление функционирования объекта критической информационной инфраструктуры для устранения выявленных нарушений не допускается.

7. В случае выявления компьютерного инцидента принимаются необходимые меры по его локализации в целях уменьшения негативного воздействия на объекты критической информационной инфраструктуры.

Статья 11. **Ответственность за нарушение законодательства в области обеспечения безопасности критической информационной инфраструктуры**

Нарушение требований настоящего модельного закона и принятых в соответствии с ним иных нормативных правовых актов влечет за собой юридическую ответственность в соответствии с законодательством государства.