Приложение
к постановлению МПА СНГ
от 28.11.2014 г. № 41-14

Межпарламентская Ассамблея государств – участников Содружества Независимых Государств

МОДЕЛЬНЫЙ ЗАКОН
О критически важных объектах информационно-коммуникационной инфраструктуры

Настоящий Закон определяет правовые, экономические, социальные и организационные основы безопасного функционирования и обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры, а также регулирует отношения в этой области.

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

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

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

защита критически важного объекта – система мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры, реализуемая работниками соответствующего объекта, его службой безопасности во взаимодействии с сотрудниками государственных органов и иных организаций, иными лицами и направленная на выявление и ликвидацию угроз безопасному функционированию объекта, поддержание функционирования объекта постоянно или в определенный период в случае реализации таких угроз, полное или частичное возмещение вреда, причиненного интересам государства и общества, интересам объекта или эксплуатирующей организации в результате нарушения или прекращения его функционирования;

информационно-коммуникационная инфраструктура – совокупность территориально распределенных государственных и корпоративных информационных систем, сетей связи, средств коммутации и управления информационными потоками, а также организационных структур и нормативно-правовых механизмов регулирования, обеспечивающих их эффективное функционирование;

инцидент безопасности объекта информационно-коммуникационной инфраструктуры – произошедшее в результате реализации угрозы безопасности критически важного объекта информационно-коммуникационной инфраструктуры нарушение или прекращение функционирования такого объекта, а также нарушение законодательства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

критически-важные инфраструктуры – объекты, системы, службы и институты, разрушение или выведение из строя которых может нанести серьезный ущерб социальному, экономическому или политическому порядку или национальной безопасности;

критический элемент критически важного объекта информационно-коммуникационной инфраструктуры – структурный компонент критически важного объекта информационно-коммуникационной инфраструктуры, выход из строя которого с неизбежностью приводит к нарушению или прекращению функционирования объекта в целом;

объект информационно-коммуникационной инфраструктуры – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения функционирования такого объекта, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, а также персонала, который осуществляет их эксплуатацию;

охрана критически важного объекта информационно-коммуникационной инфраструктуры – система мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры, реализуемая работниками соответствующего объекта, его службой безопасности во взаимодействии с сотрудниками государственных органов и иных организаций, иными лицами и направленная на предупреждение угроз безопасному функционированию объекта, на устранение причин их возникновения, на создание условий для безопасного функционирования объекта, ликвидацию или локализацию последствий нарушения или прекращения функционирования объекта;

угроза безопасности критически важного объекта информационно-коммуникационной инфраструктуры – фактор (действие, событие) или совокупность факторов, создающих опасность нарушения или прекращения функционирования критически важного объекта информационно-коммуникационной инфраструктуры;

эксплуатирующая организация – собственник (владелец) критически важного объекта информационно-коммуникационной инфраструктуры, государственный орган или иная организация, в подчинении (составе, системе) которой находится критически важный объект информационно-коммуникационной инфраструктуры.

2. Используемые в настоящем Законе институты, понятия и термины законодательства государства в области информатизации, информационной безопасности, защиты от чрезвычайных ситуаций, других отраслей законодательства применяются в том значении, в каком они используются в этих отраслях законодательства государства, если иное не предусмотрено настоящим Законом.

Статья 2. **Сфера действия настоящего Закона**

1. Настоящим Законом регулируются общественные отношения, складывающиеся:

– в области отнесения объектов информационно-коммуникационной инфраструктуры к критически важным, обеспечения безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры и исключения объектов из числа критически важных;

– при обеспечении безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– при взаимодействии государственных органов и иных организаций в процессе создания и функционирования государственной системы обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

2. Положения настоящего Закона обязательны для исполнения на территории государства органами законодательной, исполнительной и судебной власти государства, а также организациями, наделенными в соответствии с действующим законодательством полномочиями осуществлять от имени государства государственное управление в соответствующей сфере деятельности, региональными органами государственного управления, предприятиями, учреждениями и организациями независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами государства, иностранными гражданами и лицами без гражданства, находящимися на территории государства.

Статья 3. **Безопасность критически важных объектов информационно-коммуникационной инфраструктуры**

1. Безопасность критически важных объектов информационно-коммуникационной инфраструктуры представляет собой урегулированную законодательными актами систему общественных отношений, которая обеспечивает охрану и защиту таких объектов а также их работников от угроз, возникающих в связи с характером их деятельности, а также безопасное функционирование критически важных объектов информационно-коммуникационной инфраструктуры при реализации таких угроз.

2. Безопасность критически важных объектов информационно-коммуникационной инфраструктуры определяется уровнем охраны и защиты таких объектов а также их работников от угроз, возникающих в связи с характером их деятельности, а также уровнем безопасности функционирования этих объектов при наличии таких угроз.

3. Безопасность критически важных объектов информационно-коммуникационной инфраструктуры обеспечивается в соответствии с настоящим Законом, другими актами законодательства, в том числе техническими нормативными правовыми актами.

Статья 4. **Законодательство в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Законодательство в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры основывается на конституции государства и состоит из настоящего Закона, актов законодательства, ре-

гулирующих отношения в области промышленной, радиационной, пожарной, информационной и иной безопасности; законодательства в области предупреждения и ликвидации чрезвычайных ситуаций, использования атомной энергии, обеспечения санитарно-эпидемиологического благополучия населения, законодательства в области безопасности объектов, представляющих повышенную техногенную и экологическую опасность, а также объектов, условно уязвимых в диверсионном отношении. В силу специфики и характера функционирования критически важных объектов информационно-коммуникационной инфраструктуры в законодательство включаются и технические нормативные правовые акты.

2. Если международным договором государства установлены иные правила, чем те, которые содержатся в настоящем Законе, то применяются правила международного договора.

Глава 2. ГОСУДАРСТВЕННАЯ ПОЛИТИКА И ПОЛНОМОЧИЯ ГОСУДАРСТВЕННЫХ ОРГАНОВ В ОБЛАСТИ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Статья 5. **Государственная политика и государственное управление в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Содержанием государственной политики в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры является создание государственными органами государства необходимых правовых, экономических, организационных и других условий, содействующих охране и защите критически важных объектов информационно-коммуникационной инфраструктуры.

2. Государственное управление в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры осуществляют глава государства, правительство государства и совет безопасности государства в пределах полномочий, установленных законами государства и нормативными правовыми актами главы государства.

Статья 6. **Полномочия главы государства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Глава государства осуществляет в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры следующие полномочия:

– определяет государственную политику в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– осуществляет общее руководство государственными органами по вопросам безопасного функционирования и обеспечения безопасности критиче-

ски важных объектов информационно-коммуникационной инфраструктуры и обеспечивает взаимодействие между ними;

– утверждает государственные программы в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– определяет уполномоченный государственный орган в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– определяет порядок создания и принципы построения государственной системы реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры, а также случаи использования этой системы для решения задач, не связанных с обеспечением безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– принимает решение по привлечению дополнительных сил и средств органов внутренних дел государства, Вооруженных сил государства, других войск и воинских формирований при резком ухудшении политической, социальной, экономической и (или) криминогенной обстановки на территории государства, административно-территориальной единицы или в отдельном населенном пункте в целях обеспечения безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры;

– определяет условия и порядок обязательного страхования критически важных объектов информационно-коммуникационной инфраструктуры;

– осуществляет полномочия в соответствии с конституцией государства, настоящим Законом и иными законодательными актами.

2. Глава государства может делегировать правительству или совету безопасности государства отдельные полномочия в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 7. **Полномочия правительства государства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Правительство государства обеспечивает создание необходимых правовых, экономических, организационных и других условий, содействующих охране и защите критически важных объектов информационно-коммуникационной инфраструктуры.

2. Правительство государства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры:

– обеспечивает реализацию единой государственной политики;

– организует разработку, утверждает и обеспечивает выполнение государственных программ;

– утверждает отраслевые критерии отнесения объектов информационно-коммуникационной инфраструктуры к критически важным;

– определяет порядок категорирования критически важных объектов информационно-коммуникационной инфраструктуры;

– определяет конкретный порядок отнесения объекта информационно-коммуникационной инфраструктуры к критически важному и исключения таких объектов из числа критически важных;

– определяет порядок формирования и ведения государственного реестра критически важных объектов информационно-коммуникационной инфраструктуры;

– утверждает правила обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– осуществляет иные полномочия, предусмотренные настоящим Законом и законодательными актами государства.

Статья 8. **Полномочия совета безопасности государства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Совет безопасности государства проводит государственную политику в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры в пределах предоставленных ему полномочий.

2. Совет безопасности государства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры:

– вносит предложения главе государства по вопросам государственной политики в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– организует устойчивое функционирование государства в любых условиях нарушения или прекращения функционирования критически важных объектов информационно-коммуникационной инфраструктуры;

– осуществляет подготовку документов стратегического планирования в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– вносит предложения главе государства по вопросам разработки и реализации мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– осуществляет иные полномочия, предусмотренные законодательством государства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 9. **Полномочия уполномоченного государственного органа в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Уполномоченный государственный орган в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры определяется главой государства.

2. Уполномоченный государственный орган в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры:

– проводит государственную политику в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– организует и координирует деятельность органов государственного управления, которым в соответствии с законодательством государства предоставлено право осуществлять отдельные функции государственного управления, разрешительные, контрольные и надзорные функции в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры, и согласовывает принимаемые ими нормативные правовые акты по обеспечению безопасности критически важных объектов информационно-коммуникационной инфраструктуры, в том числе технические нормативные правовые акты, утверждаемые (вводимые в действие) ими в пределах своей компетенции;

– издает в пределах своих полномочий нормативные правовые акты по вопросам безопасного функционирования и обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– организует взаимодействие и координацию деятельности государственных органов и иных организаций по вопросам безопасного функционирования и обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– разрабатывает проекты государственных программ и годовых планов деятельности в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– готовит в пределах своих полномочий предложения о расходах на обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры в проект бюджета государства на очередной (финансовый) год;

– разрабатывает и реализует государственную систему реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– определяет порядок деятельности национального центра реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– устанавливает перечень сведений, подлежащих представлению в национальный центр реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры, и порядок их представления;

– определяет порядок доступа к сведениям, содержащимся в государственной системе реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– реализует в пределах своей компетенции меры обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– истребует от уполномоченных субъектов обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры сведения и (или) документы:

по вопросам безопасного функционирования и обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

об угрозах безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

о характере инцидентов безопасности, причинах их возникновения и принятых мерах;

– ведет государственный реестр критически важных объектов информационно-коммуникационной инфраструктуры государства;

– использует имеющиеся у государственных органов, указанных в пункте 1 статьи 10 настоящего Закона, эксплуатирующих организаций критически важных объектов информационно-коммуникационной инфраструктуры силы и средства для решения задач обеспечения безопасности таких объектов;

– в установленном порядке выносит предписания, обязательные для исполнения соответствующими государственными органами, эксплуатирующими и иными организациями, должностными лицами, иными гражданами государства, иностранными гражданами и лицами без гражданства по вопросам безопасного функционирования и обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры, в том числе о приостановлении эксплуатации таких объектов;

– определяет порядок ведения паспорта безопасности критически важного объекта информационно-коммуникационной инфраструктуры;

– организует подготовку кадров для государственных органов и иных организаций в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры, в том числе и на договорной основе, в подчиненных ему учреждениях образования;

– осуществляет иные полномочия, предусмотренные законодательством в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 10. **Полномочия иных государственных органов в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Государственными органами государства, реализующими в пределах своей компетенции меры обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры, являются:

– органы безопасности;

– органы и подразделения по чрезвычайным ситуациям;

– органы внутренних дел;

– органы военного управления;

– органы пограничной службы;

– органы связи и информации;

– региональные органы государственного управления;

– органы охраны окружающей среды.

2. Государственные органы, указанные в пункте 1 настоящей статьи, при реализации мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры в пределах своей компетенции:

– разрабатывают и реализуют во взаимодействии с другими государственными органами и иными организациями меры обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– предоставляют по требованию уполномоченного государственного органа в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры имеющуюся информацию по вопросам безопасного функционирования и обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– осуществляют государственный контроль и (или) надзор в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– предоставляют уполномоченному государственному органу в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры имеющиеся силы и средства для решения задач обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– по требованию уполномоченного государственного органа в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры оказывают им необходимую помощь в реализации мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

–по требованию уполномоченного государственного органа в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры информируют о других обстоятельствах, имеющих значение для решения задач обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

3. Органы, организации, учреждения и подразделения, подчиненные государственным органам, указанным в пункте 1 настоящей статьи, реализуют полномочия, указанные в пункте 2 настоящей статьи, в пределах своей компетенции.

Глава 3. ОТНЕСЕНИЕ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ К КРИТИЧЕСКИ ВАЖНЫМ

Статья 11. **Критически важные объекты информационно-коммуникационной инфраструктуры**

1. К критически важным объектам информационно-коммуникационной инфраструктуры относятся объекты информационно-коммуникационной инфраструктуры, которые:

– обеспечивают функционирование экологически опасных и (или) социально значимых производств и (или) технологических процессов, нарушение или прекращение штатного режима которых может привести к чрезвычайной ситуации техногенного характера;

– осуществляют функции информационной системы, нарушение или прекращение функционирования которой может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах;

– обеспечивают предоставление значительного объема информационных услуг, частичное или полное нарушение или прекращение оказания которых может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах.

2. Отнесение объектов информационно-коммуникационной инфраструктуры к критически важным и исключение их из числа критически важных осуществляется в соответствии с требованиями настоящего Закона и в порядке, устанавливаемом правительством государства.

Статья 12. **Общие требования отнесения объектов информационно-коммуникационной инфраструктуры к критически важным**

1. Общие требования, предъявляемые к объектам информационно-коммуникационной инфраструктуры для отнесения их к критически важным, определяются функциональным назначением объектов информационно-коммуникационной инфраструктуры и характером взаимодействия их с другими объектами социальной, производственной, транспортной, инженерной и иной инфраструктуры, в том числе отнесенными к критически важным.

2. Основным критерием отнесения объектов информационно-коммуникационной инфраструктуры к критически важным является степень возможных последствий нарушения или прекращения их функционирования:

– утрата управления государством или административно-территориальной единицей;

– потеря управления экономикой государства или административно-территориальной единицы;

– необратимое негативное изменение (или разрушение) государственного управления или экономики государства или административно-территориальной единицы;

– существенное снижение безопасности жизнедеятельности населения, проживающего на территории государства или административно-территориальной единицы, на длительный период.

Статья 13. **Отраслевые критерии отнесения объектов информационно-коммуникационной инфраструктуры к критически важным**

Отраслевые критерии отнесения объектов информационно-коммуникационной инфраструктуры к критически важным разрабатываются органами государственного управления в соответствующей сфере и утверждаются правительством государства.

Статья 14. **Категории критически важных объектов информационно-коммуникационной инфраструктуры**

1. В соответствии с основным критерием, указанным в пункте 2 статьи 12 настоящего Закона, критически важные объекты информационно-коммуникационной инфраструктуры делятся на следующие категории:

– государственные критически важные объекты информационно-коммуникационной инфраструктуры – объекты, нарушение или прекращение функционирование которых влечет за собой тяжкие последствия в масштабе государства в виде:

– утраты управления государством, либо потери управления экономикой государства, либо их необратимого негативного изменения (разрушения);

– существенного снижения уровня безопасности жизнедеятельности населения, проживающего на территории всего государства;

– региональные критически важные объекты информационно-коммуникационной инфраструктуры – объекты, нарушение или прекращение функционирования которых влечет за собой тяжкие последствия для административно-территориальной единицы в виде:

утраты государственного управления административно-территориальной единицей, либо потери управления экономикой данного региона, либо их необратимого негативного изменения (разрушения);

существенного снижения безопасности жизнедеятельности населения, проживающего на территории административно-территориальной единицы.

2. Порядок категорирования критически важных объектов информационно-коммуникационной инфраструктуры и их категории в зависимости от отраслевых критериев определяются правительством государства.

Статья 15. **Порядок отнесения объектов информационно-коммуникационной инфраструктуры к критически важным**

1. Объекты информационно-коммуникационной инфраструктуры относятся к критически важным при соответствии общим требованиям, предусмотренным настоящим Законом, и отраслевым критериям, которые утверждаются правительством государства.

2. Решение об отнесении объекта информационно-коммуникационной инфраструктуры к критически важному или об отказе в отнесении его к крити-

чески важному принимается правительством государства – для государственных критически важных объектов, региональным органом государственного управления – для региональных критически важных объектов.

3. После принятия решения об отнесении объекта информационно-коммуникационной инфраструктуры к критически важному он включается в государственный реестр критически важных объектов информационно-коммуникационной инфраструктуры государства, который ведет уполномоченный государственный орган в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры. Порядок создания и ведения государственного реестра критически важных объектов информационно-коммуникационной инфраструктуры государства определяется правительством государства.

Глава 4. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ФУНКЦИОНИРОВАНИЯ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Статья 16. **Порядок организации безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры**

1. Организация безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры осуществляется после включения таких объектов в государственный реестр критически важных объектов информационно-коммуникационной инфраструктуры государства.

2. Организация безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры включает в себя принятие решения об организации безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры, а также о продолжении функционирования либо о прекращении функционирования таких объектов.

3. Обязательным условием принятия решения об организации безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры является выполнение правил промышленной, радиационной, пожарной, информационной и иной безопасности, а также иных правил, обеспечивающих безопасный ввод в эксплуатацию, безопасную эксплуатацию и безопасный вывод из эксплуатации соответствующих объектов.

4. При организации безопасного функционирования критически важного объекта информационно-коммуникационной инфраструктуры ведется паспорт безопасности критически важного объекта информационно-коммуникационной инфраструктуры. Порядок ведения паспорта безопасности критически важного объекта определяется уполномоченным государственным органом в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 17. **Требования к безопасному функционированию критически важных объектов информационно-коммуникационной инфраструктуры**

1. Безопасное функционирование критически важных объектов информационно-коммуникационной инфраструктуры достигается их эксплуатацией в соответствии с требованиями, установленными законодательством в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры и эксплуатационной документацией.

2. Безопасное функционирование критически важных объектов информационно-коммуникационной инфраструктуры предусматривает руководство финансово-экономической, организационной деятельностью соответствующих объектов, а также деятельностью по обеспечению эффективной, надежной и безопасной эксплуатации таких объектов.

3. Не допускается функционирование критически важных объектов информационно-коммуникационной инфраструктуры без реализации на этих объектах комплекса мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

4. Эксплуатирующая организация обязана обеспечить безопасное функционирование критически важного объекта информационно-коммуникационной инфраструктуры. В случае непринятия мер по обеспечению безопасного функционирования критически важного объекта информационно-коммуникационной инфраструктуры эксплуатирующая организация и ее должностные лица несут ответственность в соответствии с настоящим Законом и другими законодательными актами.

5. Представители общественных и иных организаций имеют право доступа на территорию критически важного объекта информационно-коммуникационной инфраструктуры в порядке, установленном законодательством государства.

6. Для обеспечения безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры осуществляется их внутренний и внешний контроль.

Статья 18. **Внутренний контроль безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры**

1. Внутренний контроль безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры осуществляется эксплуатирующей организацией в целях определения соответствия функциональных характеристик таких объектов требованиям, установленным законодательством в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры и эксплуатационной документацией.

2. Внутренний контроль критически важных объектов информационно-коммуникационной инфраструктуры осуществляется не реже одного раза в год.

3. Результаты внутреннего контроля критически важных объектов информационно-коммуникационной инфраструктуры оформляются актом, со-

ставляемым в двух экземплярах, один из которых в течение семи дней направляется в уполномоченный государственный орган в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 19. **Внешний контроль безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры**

1. Внешний контроль безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры осуществляется уполномоченным государственным органом в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры в целях определения соответствия функциональных характеристик таких объектов требованиям, установленным законодательством в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

2. Для осуществления внешнего контроля уполномоченный государственный орган в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры может привлекать государственные органы, определенные в пункте 1 статьи 10 настоящего Закона, и другие государственные органы.

3. Внешний контроль осуществляется не реже одного раза в пять лет либо в случае:

– принятия уполномоченным государственным органом в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры решения о проведении внешнего контроля по результатам внутреннего контроля;

– принятия эксплуатирующей организацией в установленном порядке решения об изменении функций критически важного объекта информационно-коммуникационной инфраструктуры;

– изменения местонахождения критически важного объекта информационно-коммуникационной инфраструктуры;

– возникновения инцидента безопасности.

4. Результаты внешнего контроля оформляются актом, составляемым в двух экземплярах, один из которых в течение семи дней направляется эксплуатирующей организации.

Глава 5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Статья 20. **Задачи обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры является важнейшей составной ча-

стью обеспечения национальной безопасности государства и представляет собой правомерную деятельность работников такого объекта, его службы безопасности во взаимодействии с сотрудниками государственных органов и иных организаций, иными лицами по охране и защите критически важного объекта информационно-коммуникационной инфраструктуры.

2. Общими задачами обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры являются:

– поддержание стабильного государственного управления государством субъектом федерации или административно-территориальной единицей;

– поддержание устойчивого уровня экономики государства, субъекта федерации или административно-территориальной единицы;

– поддержание должного уровня жизнедеятельности населения, проживающего на территории государства, субъекта федерации или административно-территориальной единицы;

– создание и соблюдение условий для безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры.

3. Специальными задачами обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры являются:

– выявление и ликвидация угроз безопасному функционированию критически важных объектов информационно-коммуникационной инфраструктуры;

– поддержание функционирования критически важного объекта или его критического элемента постоянно или в определенный период в случае реализации угроз его безопасности;

– полное или частичное возмещение вреда, причиненного интересам государства и общества, интересам объекта в результате нарушения или прекращения его функционирования.

Статья 21. **Основные принципы обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры основывается на следующих общих принципах:

– законность;

– соблюдение и защита прав и свобод человека и гражданина;

– гуманизм;

– уважение и соблюдение принципов международного права.

2. Специальными принципами обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры являются:

– непрерывность реализации мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– системность и комплексное использование мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– необходимая достаточность и максимально возможное использование сил и средств при определении объема и содержания мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– реализация мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры с учетом социальных, экономических, природных и иных характеристик и особенностей такого объекта, а также степени реальности угроз его безопасности.

Статья 22. **Система обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Систему обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры составляют объекты, субъекты и меры обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

2. Целью системы обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры является обеспечение должного функционирования таких объектов, в том числе в случае реализации угроз их безопасности.

Статья 23. **Организация и поддержание системы обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Организация и поддержание системы обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры включают в себя управление такой системой, а также комплекс мероприятий, составляющих ее содержание.

2. Управление системой обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры предусматривает совокупность организованных действий руководства такого объекта и его службы безопасности, обеспечивающую согласованность функционирования всех его подразделений и работников в целях охраны и защиты объекта от внутренних и внешних угроз. Управление системой обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры направлено на организацию непрерывного процесса поддержания заданного уровня функционирования объекта и должно обеспечивать своевременное, полное выполнение всеми работниками объекта предусмотренных мероприятий, составляющих содержание системы обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры, в том числе в случае возникновения инцидентов безопасности.

3. Основными мероприятиями, составляющими содержание системы обеспечения безопасности критически важных объектов информационно-ком-

муникационной инфраструктуры, являются подготовка и реализация планов различного уровня:

– ежегодных планов мероприятий по обеспечению безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– типовых планов обеспечения повышенной готовности критически важных объектов информационно-коммуникационной инфраструктуры к деятельности в условиях реализации угроз;

– типовых планов действий персонала критически важных объектов информационно-коммуникационной инфраструктуры при возникновении инцидентов безопасности;

– типовых планов обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры в особых условиях.

4. Реализация мероприятий, составляющих содержание системы обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры, осуществляется в рамках повседневного режима функционирования таких объектов, режима повышенной готовности их функционирования и режима чрезвычайной ситуации их функционирования. Повседневный режим функционирования критически важных объектов информационно-коммуникационной инфраструктуры действует на соответствующем объекте, когда отсутствуют угрозы его безопасности. Режим повышенной готовности функционирования критически важных объектов информационно-коммуникационной инфраструктуры вводится в случае возникновения вероятности реализации угроз безопасности объекта. Режим чрезвычайной ситуации функционирования критически важных объектов информационно-коммуникационной инфраструктуры вводится тогда, когда в результате реализации угроз безопасности объекта возникает инцидент безопасности.

5. Система мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры реализуется на общем уровне работниками подразделений таких объектов, сотрудниками правоохранительных и контролирующих органов, иными уполномоченными лицами, а также на специальном уровне работниками служб безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 24. **Объекты обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры направлено на защиту интересов государства и общества, а также интересов эксплуатирующих организаций и критически важных объектов информационно-коммуникационной инфраструктуры.

2. При обеспечении безопасности критически важных объектов информационно-коммуникационной инфраструктуры должен достигаться баланс интересов государства и общества, интересов эксплуатирующих организаций и критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 25. **Субъекты обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Субъектами, уполномоченными обеспечивать безопасность критически важных объектов информационно-коммуникационной инфраструктуры, являются:

– работники критически важных объектов информационно-коммуникационной инфраструктуры, в том числе работники их служб безопасности;

– работники эксплуатирующих организаций;

– сотрудники государственных органов, указанных в пункте 1 статьи 10 настоящего Закона, сотрудники правоохранительных и контролирующих государственных органов, военнослужащие внутренних войск министерства внутренних дел государства;

– работники организаций, осуществляющих проектирование, монтаж, наладку и техническое обслуживание средств и систем охраны, иные лица, в установленном законодательством порядке уполномоченные осуществлять охрану и защиту критически важных объектов информационно-коммуникационной инфраструктуры.

2. При обеспечении безопасности критически важных объектов информационно-коммуникационной инфраструктуры уполномоченные субъекты в пределах своей компетенции обязаны:

– соблюдать положения настоящего Закона, иных нормативных правовых актов в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– обеспечивать безопасное функционирование критически важных объектов информационно-коммуникационной инфраструктуры и их критических элементов;

– предупреждать, выявлять, пресекать и локализовывать угрозы безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– реализовывать меры безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– выполнять распоряжения и предписания уполномоченного государственного органа в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры и его должностных лиц, отдаваемые в соответствии с их полномочиями;

– представлять в национальный центр реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры сведения об угрозах безопасности критически важных объектов информационно-коммуникационной инфраструктуры и о характере инцидентов безопасности, причинах их возникновения, принятых мерах и результатах их расследования;

– осуществлять мероприятия по локализации и ликвидации последствий инцидентов безопасности на критически важных объектах информационно-коммуникационной инфраструктуры, оказывать содействие государственным органам в расследовании таких инцидентов;

– осуществлять профилактические мероприятия по устранению причин и условий реализации угроз безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– вести паспорт безопасности критически важного объекта информационно-коммуникационной инфраструктуры.

3. При обеспечении безопасности критически важных объектов информационно-коммуникационной инфраструктуры уполномоченные субъекты в пределах своей компетенции имеют право:

– создавать подразделения по охране и защите критически важных объектов информационно-коммуникационной инфраструктуры и (или) их отдельных элементов;

– самостоятельно определять формы и методы охраны и защиты критически важных объектов информационно-коммуникационной инфраструктуры и (или) их отдельных элементов;

– приостанавливать эксплуатацию критически важных объектов информационно-коммуникационной инфраструктуры или их критических элементов самостоятельно либо по предписанию уполномоченного государственного органа в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры или его должностных лиц в случае инцидента безопасности, а также в случае обнаружения вновь открывшихся обстоятельств, влияющих на безопасное функционирование критически важных объектов информационно-коммуникационной инфраструктуры.

4. Субъекты обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры осуществляют свои полномочия исключительно в пределах компетенции, установленной законодательными актами государства, во взаимодействии с другими государственными органами.

Статья 26. **Служба безопасности критически важного объекта информационно-коммуникационной инфраструктуры**

1. Службой безопасности критически важного объекта информационно-коммуникационной инфраструктуры является его структурное подразделение (специально выделенные работники), основная функция которого заключается в реализации мер обеспечения безопасности критически важного объекта информационно-коммуникационной инфраструктуры. Служба безопасности критически важного объекта информационно-коммуникационной инфраструктуры подчиняется непосредственно руководителю такого объекта.

2. Основными функциями службы безопасности критически важного объекта информационно-коммуникационной инфраструктуры являются:

– предупреждение, выявление, пресечение и локализация угроз безопасности критически важных объектов информационно-коммуникационной инфраструктуры;

– организация и обеспечение пропускного и внутриобъектового режима в зданиях и помещениях критически важного объекта информационно-коммуникационной инфраструктуры, порядка несения охраны;

– контроль соблюдения требований режима безопасности работниками критически важного объекта информационно-коммуникационной инфраструктуры, сотрудниками взаимодействующих государственных органов и иных организаций, посетителями;

– разработка системы мер обеспечения безопасности критически важного объекта информационно-коммуникационной инфраструктуры, организация их исполнения на общем уровне и непосредственная реализация их на специальном уровне;

– информирование руководства критически важного объекта информационно-коммуникационной инфраструктуры по вопросам обеспечения его безопасности для принятия необходимых управленческих решений.

3. Основными задачами службы безопасности критически важного объекта информационно-коммуникационной инфраструктуры являются:

– разработка и реализация политики информационной безопасности;

– выявление существующих и прогнозирование потенциальных угроз безопасности критически важного объекта информационно-коммуникационной инфраструктуры;

– информационное обеспечение принятия управленческих решений руководством критически важного объекта информационно-коммуникационной инфраструктуры;

– разработка и реализация мер по предупреждению и ликвидации угроз безопасности критически важного объекта информационно-коммуникационной инфраструктуры, а также по локализации последствий их осуществления;

– реализация инженерно-технических, аппаратно-программных и специальных мер обеспечения безопасности критически важного объекта информационно-коммуникационной инфраструктуры;

– формирование собственных сил и средств, необходимых для обеспечения безопасности критически важного объекта информационно-коммуникационной инфраструктуры, и их подготовка;

– создание условий для реализации правовых и организационных мер обеспечения безопасности критически важного объекта информационно-коммуникационной инфраструктуры;

– реализация аварийно-спасательных и иных мер по ликвидации последствий инцидентов безопасности критически важного объекта информационно-коммуникационной инфраструктуры;

– организация взаимодействия с правоохранительными и контролирующими органами для привлечения лиц, виновных в нарушении безопасности критически важного объекта информационно-коммуникационной инфраструктуры, к установленным видам ответственности.

4. Организационную структуру службы безопасности критически важного объекта информационно-коммуникационной инфраструктуры могут составлять:

– подразделение (уполномоченные работники) режима и охраны;

– подразделение (уполномоченные работники) работы с документами, содержащими сведения, которые относятся к государственной, служебной, коммерческой тайне или к другой охраняемой информации;

– подразделение (уполномоченные работники) информационной безопасности;

– инженерно-техническое подразделение (уполномоченные работники);

– информационно-аналитическое подразделение (уполномоченные работники).

5. Организационная структура, численность и состав службы безопасности критически важного объекта информационно-коммуникационной инфраструктуры определяются исходя из реальных финансовых возможностей объекта, масштабов его уставной деятельности, степени конфиденциальности информации, циркулирующей на объекте.

Статья 27. **Угрозы безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Угрозами безопасности критически важных объектов информационно-коммуникационной инфраструктуры являются природные, техногенные и социальные угрозы. Угрозы могут быть внешними и внутренними.

2. Природные угрозы составляют опасные метеорологические и гидрологические явления, опасная сейсмическая активность, опасные уровни воды, раннее появление льда и образование ледостава, пожары, иные природные явления, могущие привести к нарушению или прекращению функционирования критически важных объектов информационно-коммуникационной инфраструктуры или их критических элементов.

3. Техногенные угрозы составляют аварии, отказы или повреждения критических элементов критически важных объектов информационно-коммуникационной инфраструктуры или технических устройств на иных объектах, обеспечивающих безопасное функционирование критически важных объектов информационно-коммуникационной инфраструктуры; нарушения производственных процессов на критически важных объектах информационно-коммуникационной инфраструктуры, которые могут вызвать инциденты безопасности, иные техногенные инциденты, могущие привести к нарушению или прекращению функционирования критически важных объектов информационно-коммуникационной инфраструктуры.

4. Социальные угрозы представляют экстремистские, террористические или диверсионные проявления (акты), компьютерные атаки, а также иные противоправные действия в отношении критически важных объектов информационно-коммуникационной инфраструктуры, их критических элементов и (или) их работников; недостаточные производственная дисциплина и профессиональная подготовка работников критически важных объектов информационно-коммуникационной инфраструктуры; иные социальные проявления, могущие привести к нарушению или прекращению функционирования критически важных объектов информационно-коммуникационной инфраструктуры.

5. Внешними угрозами являются природные угрозы, а также техногенные и социальные угрозы, не связанные с деятельностью критически важных объектов информационно-коммуникационной инфраструктуры или их работников.

6. Внутренними угрозами являются техногенные и социальные угрозы, связанные с деятельностью критически важных объектов информационно-коммуникационной инфраструктуры или их работников.

7. Уполномоченные субъекты обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры определяют угрозы безопасности критически важных объектов информационно-коммуникационной инфраструктуры в зависимости от месторасположения, производственного цикла таких объектов и иных факторов, влияющих на их безопасное функционирование.

Статья 28. **Система мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Систему мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры составляют правовые, организационные, инженерно-технические, аппаратно-программные, специальные и иные меры.

2. Применение системы мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры является достаточным, если исключает нарушение или прекращение функционирования критически важного объекта информационно-коммуникационной инфраструктуры.

3. Содержание мер безопасности для конкретного критически важного объекта информационно-коммуникационной инфраструктуры определяется эксплуатирующей организацией и (или) руководством такого объекта в соответствии с настоящим Законом, иными актами законодательства, в том числе техническими нормативными правовыми актами.

4. К правовым мерам обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры относятся положения настоящего Закона, требования иных актов законодательства, в том числе технических нормативных правовых актов, в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры, а также действия уполномоченных субъектов обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры по их реализации.

5. К организационным мерам обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры относятся действия уполномоченных субъектов обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры, направленные на организацию и поддержание системы обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

6. К инженерно-техническим мерам обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры относятся действия уполномоченных субъектов обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры, направленные на поддержание функционирования таких объектов (их компонентов) в определенный период в случае выхода из строя их критических и иных элементов, а также на создание и поддержание систем физической охраны этих объектов.

7. К аппаратно-программным мерам обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры относятся действия уполномоченных субъектов обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры, направленные на защиту информационных активов таких объектов, обрабатываемых и (или) хранящихся в различных информационных системах либо в отдельных комплексах программно-технических средств.

8. К специальным мерам обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры относятся действия уполномоченных субъектов обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры, направленные на предупреждение, выявление, пресечение и локализацию угроз безопасности критически важных объектов информационно-коммуникационной инфраструктуры, осуществление информационно-аналитической деятельности и физическую охрану работников такого объекта.

9. К иным мерам обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры относятся любые меры, создающие условия для реализации правовых, организационных, инженерно-технических, аппаратно-программных и специальных мер обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 29. **Обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры в особых условиях**

1. К особым условиям в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры относится введение на территории государства или административно-территориальной единицы чрезвычайного или военного положения, а также резкое ухудшение политической, социальной, экономической, террористической и (или) криминогенной обстановки на территории государства, административно-территориальной единицы или в отдельном населенном пункте.

2. При введении на территории государства военного положения обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры возлагается на советы обороны, Вооруженные силы государства, другие войска и воинские формирования. Уполномоченные субъекты обеспечения безопасности критически важных объектов информационно-

коммуникационной инфраструктуры поступают в оперативное управление советов обороны.

3. При введении на территории государства или в отдельной административно-территориальной единице чрезвычайного положения обеспечение безопасности критически важных объектов информационно-коммуникационной инфраструктуры может дополнительно осуществляться силами и средствами органов внутренних дел государства, Вооруженных сил государства, других войск и воинских формирований. Уполномоченные субъекты обеспечения безопасности критически важных объектов информационно-коммуникационной инфраструктуры поступают в оперативное управление коменданта территории, на которой введено чрезвычайное положение.

4. При резком ухудшении политической, социальной, экономической, террористической и (или) криминогенной обстановки на территории государства, административно-территориальной единицы или в отдельном населенном пункте по решению главы государства допускается привлечение дополнительных сил и средств органов внутренних дел государства, Вооруженных сил государства, других войск и воинских формирований в целях обеспечения безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры.

5. В целях обеспечения безопасного функционирования критически важных объектов информационно-коммуникационной инфраструктуры уполномоченные субъекты обеспечения безопасности таких объектов по согласованию с уполномоченным государственным органом в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры разрабатывают типовые планы обеспечения безопасности таких объектов.

Глава 6. ГОСУДАРСТВЕННАЯ СИСТЕМА РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Статья 30. **Национальный центр реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Для снижения уровня угроз безопасности критически важных объектов информационно-коммуникационной инфраструктуры в рамках государственной системы реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры создается национальный центр реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры. В состав национального центра реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры входит национальный центр реагирования на компьютерные инциденты.

2. Порядок деятельности национального центра реагирования на инциденты безопасности критически важных объектов информационно-коммуника-

ционной инфраструктуры определяется уполномоченным государственным органом в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 31. **Реагирование на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. В случае возникновения инцидента безопасности критически важных объектов информационно-коммуникационной инфраструктуры вводится режим чрезвычайной ситуации и реализуется типовой план действий работников такого объекта при возникновении инцидентов безопасности.

2. В рамках режима чрезвычайной ситуации работники критически важного объекта информационно-коммуникационной инфраструктуры реализуют соответствующие меры безопасности критически важных объектов информационно-коммуникационной инфраструктуры, направленные на ликвидацию инцидентов безопасности и поддержание функционирования объекта.

3. Служба безопасности критически важного объекта информационно-коммуникационной инфраструктуры осуществляет действия по пресечению и локализации угроз безопасности такого объекта и привлекает для этого в случае необходимости сотрудников государственных органов и иных организаций в соответствии с их компетенцией.

4. Для установления причин и условий возникновения инцидентов безопасности, выработки мер по недопущению их повторного возникновения проводится расследование инцидентов безопасности в соответствии с положениями настоящего Закона, требованиями актов законодательства государства, в том числе технических нормативных правовых актов, устанавливающих правила промышленной, радиационной, пожарной, информационной и иной безопасности.

Статья 32. **Представление информации в государственную систему реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. О возникновении инцидента безопасности критически важных объектов информационно-коммуникационной инфраструктуры, его последствиях, принятых мерах и результатах расследования незамедлительно информируется национальный центр реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

2. Конкретный перечень сведений, подлежащих представлению в национальный центр реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры, и порядок их представления устанавливаются уполномоченным государственным органом в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

3. Сведения, содержащиеся в государственной системе реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры, относятся к информации ограниченного распро-

странения. Порядок доступа к сведениям, содержащимся в государственной системе реагирования на инциденты безопасности критически важных объектов информационно-коммуникационной инфраструктуры, определяется уполномоченным государственным органом в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Глава 7. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ. ВОЗМЕЩЕНИЕ ВРЕДА, ПРИЧИНЕННОГО НАРУШЕНИЕМ ИЛИ ПРЕКРАЩЕНИЕМ ФУНКЦИОНИРОВАНИЯ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Статья 33. **Ответственность за нарушение законодательства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Нарушение законодательства государства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры влечет за собой уголовную, административную, гражданско-правовую и иную ответственность в соответствии с настоящим Законом и законодательными актами государства.

2. Привлечение виновных лиц к ответственности за нарушение законодательства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры не освобождает их от возмещения вреда, причиненного критически важному объекту информационно-коммуникационной инфраструктуры, и выполнения мероприятий по обеспечению его безопасности.

Статья 34. **Ответственность эксплуатирующей организации за нарушение законодательства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Эксплуатирующая организация обязана возместить вред, причиненный жизни и здоровью физических лиц, их имуществу, окружающей среде, а также имуществу юридических лиц при создании, реконструкции, эксплуатации, консервации и ликвидации критически важных объектов информационно-коммуникационной инфраструктуры в полном объеме, если не докажет, что вред возник вследствие непреодолимой силы или умысла потерпевшего. Эксплуатирующая организация может быть освобождена судом от ответственности за причинение вреда полностью или частично только по основаниям, предусмотренным гражданским кодексом государства.

2. Обязанность возмещения вреда, причиненного жизни или здоровью физических лиц, их имуществу, а также имуществу юридических лиц при создании, реконструкции, эксплуатации, консервации и ликвидации критически

важных объектов информационно-коммуникационной инфраструктуры, возлагается на эксплуатирующую организацию в соответствии с законодательством государства.

3. Обязанность возмещения вреда, причиненного при создании, реконструкции, эксплуатации, консервации и ликвидации критически важных объектов информационно-коммуникационной инфраструктуры, может быть возложена законодательными актами государства на иное физическое или юридическое лицо.

4. Возмещение затрат, связанных с проведением работ по предотвращению или минимизации последствий вредного воздействия на окружающую среду и ликвидации чрезвычайных ситуаций, вызванных созданием, реконструкцией, эксплуатацией, консервацией и ликвидацией критически важных объектов информационно-коммуникационной инфраструктуры, производится физическими или юридическими лицами, ответственными за причинение вреда, а при возникновении или опасности возникновения чрезвычайных ситуаций природного характера – в соответствии с законодательством государства.

Статья 35. **Страхование ответственности за причинение вреда в случае нарушения или прекращения функционирования критически важных объектов информационно-коммуникационной инфраструктуры**

1. Условия и порядок обязательного страхования критически важных объектов информационно-коммуникационной инфраструктуры определяются главой государства.

2. Эксплуатирующая организация обязана на условиях и в порядке, установленных законодательством государства в области страхования, за свой счет страховать в качестве страхователя имущественные интересы, связанные с обязанностью возместить вред, причиненный потерпевшим, путем заключения договора обязательного страхования со страховщиком в течение всего срока эксплуатации критически важных объектов информационно-коммуникационной инфраструктуры.

3. Размер страховой выплаты, причитающейся потерпевшему в счет возмещения вреда, причиненного имуществу, определяется в соответствии с правилами обязательного страхования с учетом реального ущерба, причиненного повреждением имущества. Размер страховой выплаты, причитающейся потерпевшему в счет возмещения вреда, причиненного в связи с нарушением условий жизнедеятельности, определяется исходя из понесенных потерпевшим расходов, связанных с переездом к месту временного поселения и обратно, проживанием в месте временного поселения, приобретением жизненно важных материальных средств. Указанные расходы при отсутствии документов, подтверждающих размер расходов, учитываются при определении размера страховой выплаты по нормативам, устанавливаемым правилами обязательного страхования.

4. Страховая сумма по договору обязательного страхования и размеры страховых выплат по договору обязательного страхования определяются в соответствии с законодательством государства в области страхования.

5. При наступлении страхового случая потерпевший вправе предъявить непосредственно страховщику требование о возмещении причиненного вреда. Соответствующее заявление потерпевшего направляется страховщику вместе с документами, подтверждающими причинение вреда и его размер. Перечень указанных документов определяется законодательством государства в области страхования. При этом потерпевший обязан сообщить страховщику в соответствии с правилами обязательного страхования свои персональные данные, необходимые для осуществления страховой выплаты.

6. В случае смерти потерпевшего страховая выплата осуществляется независимо от выплат, причитающихся по другим видам страхования.

7. Порядок установления факта нарушения условий жизнедеятельности и критерии, по которым устанавливается указанный факт, определяются законодательством государства в области страхования. Документы, подтверждающие факт нарушения условий жизнедеятельности на определенной территории, выдаются по требованию потерпевших региональными органами государственного управления, наделенными полномочиями по решению вопросов организации и осуществления мероприятий по гражданской обороне, защите населения и территории от чрезвычайных ситуаций в границах такой территории.

8. По договору обязательного страхования страховщик не возмещает:

– вред, причиненный имуществу страхователя;

– расходы потерпевшего, связанные с неисполнением или ненадлежащим исполнением своих гражданско-правовых обязательств;

– вред, причиненный имуществу потерпевшего, умышленные действия которого явились причиной инцидента безопасности;

– убытки, являющиеся упущенной выгодой, в том числе связанные с утратой товарной стоимости имущества, а также моральный вред.

9. Страховщик освобождается от обязанности осуществить страховую выплату, если вред потерпевшим причинен в результате инцидента безопасности критически важных объектов информационно-коммуникационной инфраструктуры, произошедшего вследствие воздействия ядерного взрыва, радиации или радиоактивного загрязнения, военных действий, гражданской войны, а также в результате диверсий и террористических актов.

10. Страховая выплата осуществляется путем наличного или безналичного расчета – по выбору потерпевшего. Днем исполнения страховщиком обязанности по осуществлению страховой выплаты считается день поступления денежных средств на банковский счет потерпевшего или день выплаты денежных средств из кассы страховщика.

Статья 36. **Возмещение вреда, причиненного нарушением законодательства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Физические, а также юридические лица независимо от их организационно-правовых форм и форм собственности обязаны возместить вред, причиненный жизни, здоровью или имуществу третьих лиц и окружающей среде

вследствие нарушения ими законодательства в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

2. Возмещение вреда осуществляется в соответствии с законодательством государства.

Глава 8. ИСКЛЮЧЕНИЕ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ ИЗ ЧИСЛА КРИТИЧЕСКИ ВАЖНЫХ

Статья 37. **Основания для исключения объектов информационно-коммуникационной инфраструктуры из числа критически важных**

Основаниями для исключения объекта информационно-коммуникационной инфраструктуры из числа критически важных являются:

– несоответствие объекта информационно-коммуникационной инфраструктуры общим и (или) отраслевым критериям отнесения его к критически важным;

– прекращение функционирования объекта, отнесенного к критически важным объектам информационно-коммуникационной инфраструктуры.

Статья 38. **Порядок исключения объектов информационно-коммуникационной инфраструктуры из числа критически важных**

1. Решение об исключении объекта информационно-коммуникационной инфраструктуры из числа критически важных принимается правительством государства – для государственных критически важных объектов, региональным органом государственного управления – для региональных критически важных объектов. Конкретный порядок исключения объекта информационно-коммуникационной инфраструктуры из числа критически важных определяется правительством государства.

2. После принятия решения об исключении объекта информационно-коммуникационной инфраструктуры из числа критически важных уполномоченный государственный орган в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры исключает его из государственного реестра критически важных объектов информационно-коммуникационной инфраструктуры.

3. При установлении обстоятельств, не позволяющих исключить объект информационно-коммуникационной инфраструктуры из числа критически важных, в отношении такого объекта принимается решение об условиях возможности его дальнейшего функционирования с учетом этих обстоятельств по согласованию с уполномоченным государственным органом в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры.

Глава 9. ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ И НАДЗОР В ОБЛАСТИ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ ИНФРАСТРУКТУРЫ

Статья 39. **Организация государственного контроля и надзора в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Государственный контроль в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры организуется в соответствии с законодательством в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры в целях соблюдения требований указанного законодательства, защиты прав и интересов юридических и физических лиц, эксплуатирующих организаций и государства.

2. Государственный контроль в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры организуется на принципах самостоятельности и независимости от подконтрольных объектов.

Статья 40. **Осуществление государственного контроля и надзора в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры**

1. Государственный контроль и надзор за безопасным функционированием критически важных объектов информационно-коммуникационной инфраструктуры осуществляют уполномоченные государственные органы в области промышленной, радиационной, пожарной, информационной и иной безопасности, а также в соответствии с законодательством, уполномоченные органы в области предупреждения и ликвидации чрезвычайных ситуаций, в области использования атомной энергии, санитарно-эпидемиологического благополучия населения, а также в области безопасности объектов, представляющих повышенную техногенную и экологическую опасность.

2. Государственный контроль за обеспечением безопасности критически важных объектов информационно-коммуникационной инфраструктуры осуществляет уполномоченный государственный орган в области безопасности критически важных объектов информационно-коммуникационной инфраструктуры и иные уполномоченные на то государственные органы в соответствии с законодательством государства.

Принят на сорок первом
пленарном заседании
Межпарламентской Ассамблеи
государств – участников СНГ
(постановление № 41-14 от 28 ноября 2014 года)