O‘ZBEKISTON RESPUBLIKASI PREZIDENTINING
QARORI

2023 yil «31» мая №ПП–167

О дополнительных мерах по совершенствованию системы обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан

В соответствии с Законом Республики Узбекистан «О кибербезопасности», Указом Президента Республики Узбекистан от 15 июня 2020 года № УП–6007 «О мерах по внедрению Государственной системы защиты информационных систем и ресурсов Республики Узбекистан» и постановлением от 15 июня 2020 года № ПП–4751 «О дополнительных мерах по дальнейшему совершенствованию системы обеспечения кибербезопасности в Республике Узбекистан» и в целях эффективной организации осуществления единой государственной политики по обеспечению кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан:

1. Утвердить:

Положение о порядке обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан, **согласно приложению № 1**;

Общие требования кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан, **согласно приложению № 2**.

2. Определить, что Служба государственной безопасности Республики Узбекистан (далее – уполномоченный государственный орган) ведет наблюдение за степенью обеспеченности кибербезопасности объектов критической информационной инфраструктуры (далее – КИИ), разрабатывает порядок их оценки и мониторинга, совместно с Инспекцией по контролю в сфере информатизации и телекоммуникаций при Министерстве цифровых технологий Республики Узбекистан принимает участие в осуществлении контроля и мониторинга обеспечения и развития кибербезопасности в порядке, установленном законодательством.

3. Секретно.

4. Применить ежемесячную надбавку, определенную в подпункте «г» пункта 7 Указа Президента Республики Узбекистан от 19 февраля 2018 года № УП–5349 «О мерах по дальнейшему совершенствованию сферы информационных технологий и коммуникаций» также к сотрудникам, ответственным за обеспечение кибербезопасности объектов КИИ и координации их деятельности.

5. Внедрить практику своевременного информирования уполномоченного государственного органа о назначении на должность и освобождении от должности, проведения аттестации работников, ответственных за обеспечение кибербезопасности объектов КИИ, а также проведения аттестации данных работников уполномоченным государственным органом каждые три года.

6. Уполномоченный государственный орган при проведении оперативно-контрольных мероприятий по обеспечению кибербезопасности объектов КИИ на особо важных и категорированных объектах уведомляет и представляет письменную информацию по их результатам в течение 48 часов в аппарат Совета безопасности при Президенте Республики Узбекистан.

7. Службе государственной безопасности Республики Узбекистан (Азизов А.):

в срок **до 1 октября 2023 года** по согласованию с аппаратом Совета безопасности при Президенте Республики Узбекистан сформировать временный Единый государственный реестр объектов КИИ Республики Узбекистан и утвердить временное положение по установлению Порядка классификации объектов КИИ;

в срок **до 1 декабря 2024 года** на основе изучения передового опыта зарубежных государств внести в аппарат Совета безопасности при Президенте Республики Узбекистан предложения о формировании Постоянного Единого государственного реестра объектов КИИ Республики Узбекистан и утверждении Постоянного Положения по установлению Порядка классификации объектов КИИ.

8. Контроль за исполнением настоящего постановления возложить на секретаря Совета безопасности при Президенте Республики Узбекистан Махмудова В.В.

Президент
Республики Узбекистан **Ш. Мирзиёев**

O'ZBEKISTON RESPUBLIKASI PREZIDENTI ADMINISTRATSIYASI
KANSELYARIYA
1

город Ташкент

Приложение № 1
к постановлению Президента Республики Узбекистан
от 31 мая 2023 года № ПП–167

ПОЛОЖЕНИЕ
о порядке обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан

Глава 1. Общие положения

1. Настоящее Положение определяет порядок обеспечения кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан.

2. В настоящем Положении используются следующие основные понятия:

киберзащита – комплекс правовых, организационных, финансово-экономических, инженерно-технических мер, а также мер криптографической и технической защиты данных, направленных на предотвращение инцидентов кибербезопасности, выявление кибератак и защиту от них, устранение последствий кибератак, восстановление стабильности и надежности деятельности телекоммуникационных сетей, информационных систем и ресурсов;

критическая информационная инфраструктура – комплекс автоматизированных систем управления, информационных систем и ресурсов сетей и технологических процессов, имеющих важное стратегическое и социально-экономическое значение;

кибератака на объект критической информационной инфраструктуры – умышленное действие, представляющее угрозу кибербезопасности путем использования в киберпространстве аппаратных, аппаратно-программных и программных средств на объектах критической информационной инфраструктуры;

инцидент кибербезопасности на объекте критической информационной инфраструктуры – инцидент, при эксплуатации объекта критической информационной инфраструктуры в киберпространстве приведший к сбоям в работе информационных систем и (или) нарушениям доступности, целостности и свободного использования информации;

объекты критической информационной инфраструктуры – системы информатизации, применяемые в сфере государственного управления и оказания государственных услуг, обороны, обеспечения государственной безопасности, правопорядка, топливно-энергетического комплекса (атомной энергетики), в химической, нефтехимической отраслях, металлургии, водопользования и водоснабжения, сельского хозяйства, здравоохранения, жилищно-коммунального обслуживания, банковско-финансовой системы, сферах транспорта, информационно-коммуникационных технологий, экологии и охраны окружающей среды, добычи и переработки полезных ископаемых стратегического значения, производственной сфере и других отраслях экономики и социальной сфере;

субъекты критической информационной инфраструктуры – государственные органы и организации, а также юридические лица, владеющие объектами критической информационной инфраструктуры на правах собственности, аренды или на других законных основаниях, в том числе юридические лица и (или) индивидуальные предприниматели, обеспечивающие эксплуатацию и взаимодействие объектов критической информационной инфраструктуры;

кибербезопасность (объектов) критической информационной инфраструктуры – состояние защищенности, обеспечивающее устойчивое функционирование объекта критической информационной инфраструктуры и защиту от нарушения, которое может привести к возникновению инцидента кибербезопасности на объекте критической информационной инфраструктуры.

3. Обеспечение кибербезопасности объектов критической информационной инфраструктуры (далее – КИИ) основывается на принципах законности, непрерывности и комплексности киберзащиты, приоритетности выявления, предотвращения, оперативного реагирования и устранения последствий кибератаки.

4. Основными направлениями обеспечения кибербезопасности объектов КИИ являются:

осуществление государственной политики в области кибербезопасности объектов КИИ;

организационно-правовое регулирование деятельности по обеспечению кибербезопасности объектов КИИ;

установление требований в области обеспечения кибербезопасности объектов КИИ, организация их технической безопасности на всех этапах жизненного цикла – создание, эксплуатация, использование и модернизация;

оценка защищенности объектов КИИ, проведение мероприятий по выявлению угроз и уязвимостей кибербезопасности;

предупреждение кибератак, их предотвращение, принятие оперативных мер и устранение их последствий, обеспечение оперативного взаимодействия субъектов КИИ при расследовании инцидентов кибербезопасности;

организационное, материально-техническое и кадровое обеспечение кибербезопасности объектов КИИ;

пресечение попыток или прямых кибератак на объекты КИИ, разработка и подготовка к применению планов восстановления их стабильной работы в случае кибератак;

проведение научно-исследовательских и опытно-конструкторских работ по обеспечению кибербезопасности объектов КИИ.

5. Участниками государственной системы обеспечения кибербезопасности объектов КИИ являются:

уполномоченный государственный орган в области кибербезопасности в Республике Узбекистан – Служба государственной безопасности Республики Узбекистан (далее – уполномоченный государственный орган);

рабочий орган уполномоченного государственного органа (далее – рабочий орган);

Инспекция по контролю в сфере информатизации и телекоммуникаций при Министерстве цифровых технологий Республики Узбекистан (далее – «Узкомназорат»);

субъекты КИИ.

Обеспечение кибербезопасности объектов КИИ Республики Узбекистан осуществляется в соответствии с прилагаемой организационной схемой.

6. Отношения в сфере обеспечения кибербезопасности объектов КИИ регулируются Конституцией и законами Республики Узбекистан, указами, постановлениями и распоряжениями Президента Республики Узбекистан, постановлениями и распоряжениями Кабинета Министров, а также настоящим Положением и иными актами законодательства.

Глава 2. Задачи уполномоченного государственного органа и «Узкомназорат» в области обеспечения кибербезопасности объектов критической информационной инфраструктуры

7. Уполномоченный государственный орган:

вырабатывает решения по созданию системы кибербезопасности объектов КИИ, а также обеспечению бесперебойной работы и развитию технической инфраструктуры;

вносит предложения в аппарат Совета безопасности при Президенте Республики Узбекистан по совершенствованию нормативно-правового регулирования в области обеспечения кибербезопасности (объектов) КИИ;

координирует деятельность по выявлению, предупреждению, оперативному реагированию, устранению последствий кибератак и обеспечению кибербезопасности объектов КИИ;

формирует и ведет единый государственный реестр объектов КИИ (далее – реестр);

осуществляет надзор за соблюдением законодательства в области кибербезопасности объектов КИИ, обрабатывающих сведения, которые составляют государственную тайну;

организует и осуществляет систему аттестации объектов КИИ в соответствии с законодательством;

регулирует организацию и проведение изучений и проверок совместно с рабочим органом и «Узкомназорат» по определению состояния обеспечения кибербезопасности объектов КИИ;

определяет порядок обмена информацией об инцидентах кибербезопасности в рамках взаимодействия с субъектами КИИ, правоохранительными органами, уполномоченным государственным органом, а также субъектами КИИ и уполномоченными органами иностранных государств, международными негосударственными организациями, осуществляющими деятельность в сфере реагирования на инциденты кибербезопасности;

устанавливает и координирует реализацию требований к применению мер по выявлению, предотвращению кибератак и устранению их последствий, реагированию на инциденты кибербезопасности на объектах КИИ;

выявляет, собирает и анализирует информацию о возможных угрозах кибербезопасности объектов КИИ и об их уязвимостях;

совместно с субъектами КИИ разрабатывает планы по предотвращению попыток или прямых кибератак на объекты КИИ, а также по восстановлению стабильной работы объектов в случае инцидента кибербезопасности, проводит по ним плановые учения.

8. Уполномоченный государственный орган в пределах своих полномочий участвует в международных мероприятиях в области обеспечения кибербезопасности КИИ и осуществляет обмен информацией об угрозах кибербезопасности и инцидентах кибербезопасности в соответствии с международными договорами.

9. «Узкомназорат»:

осуществляет надзор за соблюдением законодательства в области кибербезопасности объектов КИИ, обрабатывающих информацию, не содержащую государственную тайну;

совместно с рабочим органом проверяет, изучает и контролирует выполнение субъектами КИИ требований нормативных документов в сфере технического регулирования в области обеспечения кибербезопасности объектов КИИ;

участвует в разработке предложений и рекомендаций по совершенствованию нормативно-правовой базы в области обеспечения кибербезопасности объектов КИИ;

в пределах своих полномочий дает указания субъектам КИИ по устранению выявленных слабых сторон и недостатков в обеспечении кибербезопасности объектов КИИ;

участвует в деятельности межведомственных консультативно-совещательных органов, международных семинарах, научно-технических конференциях, симпозиумах, встречах и выставках по вопросам обеспечения кибербезопасности объектов КИИ.

Глава 3. Задачи рабочего органа в области обеспечения кибербезопасности объектов критической информационной инфраструктуры

10. В соответствии с решениями уполномоченного государственного органа на рабочий орган возлагаются задачи по созданию системы кибербезопасности объектов КИИ, а также по обеспечению ее бесперебойного функционирования и развитию технической инфраструктуры.

Рабочий орган:

в централизованном порядке собирает и анализирует информацию о современных угрозах кибербезопасности с целью выработки рекомендаций и предложений по оперативному принятию эффективных организационных и программно-технических решений в предотвращении кибератак на объекты КИИ;

оказывает содействие защите от возможных кибератак и обеспечению бесперебойного функционирования объектов КИИ;

внедряет средства выявления, предотвращения и устранения последствий кибератак на объекты КИИ;

взаимодействует с правоохранительными органами по реагированию на инциденты кибербезопасности и киберугрозы на объектах КИИ;

координирует деятельность подразделений кибербезопасности субъектов КИИ и оказывает содействие в расследовании инцидентов кибербезопасности на объектах КИИ;

обеспечивает методологическое содействие деятельности субъектов КИИ по защите объектов КИИ от кибератак и принятию мер против инцидентов кибербезопасности;

проводит аудит, аттестацию и экспертизу объектов КИИ на соответствие техническим поручениям и требованиям кибербезопасности;

сертифицирует телекоммуникационное оборудование, аппаратные, программно-аппаратные средства по защите информации, используемые на объектах КИИ, на соответствие требованиям нормативных документов в области технического регулирования;

обеспечивает переподготовку и повышение квалификации специалистов субъектов КИИ, ответственных за обеспечение кибербезопасности;

оказывает содействие в разработке и реализации политики информационной безопасности на объектах КИИ;

совместно с уполномоченным государственным органом изучает и проверяет состояние кибербезопасности на объектах КИИ;

участвует в международных мероприятиях по вопросам обеспечения кибербезопасности объектов КИИ и организует научно-технические конференции, симпозиумы, совещания, выставки, в том числе готовит информационно-аналитические материалы.

Глава 4. Права и обязанности субъектов критической информационной инфраструктуры

11. Субъекты КИИ имеют следующие права:

получение от уполномоченного государственного органа информации по обеспечению кибербезопасности объектов КИИ, в том числе о киберугрозах данным, обрабатываемым такими объектами, и уязвимостях в программном обеспечении, устройствах и технологиях, используемых на таких объектах;

создание собственных подразделений кибербезопасности, разработка и реализация мероприятий по обеспечению кибербезопасности объектов КИИ.

12. Субъекты КИИ обязаны:

соблюдать требования нормативно-правовых актов в области кибербезопасности объектов КИИ и нормативных документов в области технического регулирования;

незамедлительно уведомлять уполномоченный государственный орган и рабочий орган об инцидентах кибербезопасности в установленном порядке;

оказывать содействие уполномоченному государственному органу и рабочему органу в обнаружении и предотвращении кибератак, устранении их последствий, выявлении причин и условий возникновения инцидентов кибербезопасности;

уведомлять уполномоченный государственный орган о случаях неправомерного вмешательства государственных органов в процесс обеспечения кибербезопасности объектов КИИ;

по согласованию с уполномоченным государственным органом устанавливать и поддерживать за свой счет средства, предназначенные для обнаружения и предотвращения кибератак, устранения их последствий, реагирования на инциденты кибербезопасности;

обеспечивать полноценную работу средств, предназначенных для обнаружения и предотвращения кибератак, устранения их последствий на объектах КИИ в соответствии с установленными требованиями;

реагировать на инциденты кибербезопасности в порядке, утвержденном уполномоченным государственным органом, принимать меры по устранению последствий кибератак, совершенных на объекты КИИ, участвовать в расследовании инцидентов кибербезопасности;

обеспечивать установленном законодательством порядке доступ на объекты КИИ должностным лицам уполномоченного государственного органа, рабочего органа и «Узкомназорат» в процессе осуществления ими полномочий, предусмотренных настоящим Положением;

по согласованию с уполномоченным государственным органом и рабочим органом предотвращать возможные киберугрозы на объектах КИИ и разрабатывать планы по восстановлению стабильного функционирования объектов КИИ в случае кибератак;

участвовать в плановых учениях, организуемых уполномоченным государственным органом и рабочим органом.

13. Субъекты КИИ могут иметь иные права и нести иные обязанности в соответствии с законодательством.

Глава 5. Система кибербезопасности объектов критической информационной инфраструктуры

14. Субъекты КИИ создают систему кибербезопасности объектов КИИ и обеспечивают ее функционирование.

15. Основными задачами системы кибербезопасности объектов КИИ являются:

предотвращение неправомерного использования, удаления, изменения, блокирования (ограничения), копирования, предоставления и распространения информации, обрабатываемой на объектах КИИ, а также иных неправомерных действий;

недопущение воздействия на аппаратные, программные и программно-аппаратные средства обработки информации, способного вызвать нарушение и (или) остановку работы объектов КИИ;

восстановление работы объектов КИИ путем резервирования телекоммуникационных сетей, информационных ресурсов и системы жизнедеятельности.

Глава 6. Заключительные положения

16. Координация и контроль над внедрением государственной системы обеспечения кибербезопасности объектов КИИ и ее бесперебойной работой осуществляется аппаратом Совета безопасности при Президенте Республики Узбекистан.

17. Лица, виновные в нарушении требований настоящего Положения, несут ответственность в соответствии с законодательством Республики Узбекистан.

Приложение № 2
к постановлению Президента Республики Узбекистан
от 31 мая 2023 года № ПП–167

ОБЩИЕ ТРЕБОВАНИЯ
по обеспечению кибербезопасности объектов критической информационной инфраструктуры Республики Узбекистан

Глава 1. Основные положения

1. Настоящие Требования определяют общие требования по обеспечению кибербезопасности объектов критической информационной инфраструктуры (далее – КИИ) Республики Узбекистан.

2. Субъект КИИ обеспечивает кибербезопасность принадлежащего ему объекта КИИ в соответствии с Законом Республики Узбекистан «О кибербезопасности», настоящими Требованиями и иными актами законодательства.

Глава 2. Основные требования по обеспечению кибербезопасности объектов КИИ

3. К объектам КИИ предъявляются следующие требования обеспечения кибербезопасности:

создание системы эффективного обеспечения кибербезопасности объекта КИИ;

предотвращение несанкционированного использования информации в информационной системе, ее уничтожения, модификации, блокирования (ограничения), копирования, предоставления и распространения, а также иных действий, приводящих к нарушению и (или) прекращению деятельности объектов КИИ;

соответствие параметров системы обеспечения кибербезопасности требованиям технических регламентов, внедрение мероприятий по обеспечению кибербезопасности и бесперебойной работы объекта КИИ;

наличие возможности быстрого восстановления системы киберзащиты в случае инцидента кибербезопасности;

эффективно налаженная система мониторинга, аудита и анализа кибератак, выявления, принятия мер и устранение их последствий;

наличие документов по кибербезопасности и кибербезопасности объекта КИИ и его эксплуатации.

4. Руководитель объекта КИИ является ответственным за обеспечение его кибербезопасности. В установленном порядке руководителем объекта КИИ назначаются специалисты или структурное подразделение, ответственные за обеспечение функционирования системы защиты, обеспечивающей кибербезопасность на объекте.

5. Руководитель объекта КИИ утверждает политику обеспечения информационной безопасности объекта, положения, инструкции, требования, порядок применения средств защиты, организации и контроля над работой системы защиты, обеспечивающей кибербезопасность, а также принимает меры по их постоянному совершенствованию.

6. У объекта КИИ должны быть следующие документы:

документы, подтверждающие назначение руководителем кибербезопасности объекта КИИ ответственных за обеспечение работы системы киберзащиты на объекте специалистов и/или наличие структурного подразделения киберзащиты;

документы, подтверждающие утверждение и постоянное совершенствование политики информационной безопасности кибербезопасности и объекта КИИ, положений, инструкций, требований, порядка применения средств защиты, организации и контроля работы системы киберзащиты;

мониторинг состояния кибербезопасности и важных показателей информационных систем, а также документы, подтверждающие анализ угроз информационной безопасности и возможных способов (сценариев) и моделей их реализации, ее слабых сторон, принятие мер по предупреждению и устранению последствий инцидентов кибербезопасности;

документы, подтверждающие опытную эксплуатацию системы и подсистем киберзащиты, приемо-сдаточные испытания и практику испытаний системы киберзащиты;

документы, подтверждающие повышение знаний и практических навыков сотрудников по обеспечению информационной безопасности и кибербезопасности;

утвержденные рабочие или эксплуатационные документы по обеспечению кибербезопасности объекта КИИ;

документы, подтверждающие проведение плановых и внеплановых проверок состояния системы защиты в соответствии с нормативными документами в области технического регулирования в сфере информационной и кибербезопасности;

документы, подтверждающие соблюдение правил, регламентирующих процесс ввоза и вывоза, хранения, передачи и списания всех носителей информации на территорию объекта;

документы, подтверждающие выполнение мероприятий по обеспечению кибербезопасности, определенных годовыми планами.

7. Все аппаратные, программно-аппаратные и программные средства, обеспечивающие кибербезопасность объектов КИИ, должны иметь необходимые сертификаты соответствия и соответствовать законодательству по кибербезопасности.

8. Помимо требований по обеспечению кибербезопасности объектов КИИ дополнительно предусматриваются:

планирование, разработка, совершенствование и введение мероприятий по обеспечению кибербезопасности объектов КИИ;

принятие организационных, правовых и технических мер по обеспечению кибербезопасности объектов КИИ;

определение показателей и характеристик аппаратных, программно-аппаратных и программных средств, используемых для обеспечения кибербезопасности объектов КИИ.

9. Органы государственной власти и управления, объединения, предприятия, учреждения и организации по согласованию с уполномоченным государственным органом и его рабочим органом могут устанавливать дополнительные требования к разработке политики информационной безопасности, при ее реализации, средствам обеспечения кибербезопасности объектов КИИ, исходя из особенностей деятельности объектов.

Глава 3. Требования к средствам обеспечения безопасности конфиденциальной и секретной информации, обрабатываемой в автоматизированных и информационных системах объекта КИИ

10. Система защиты кибербезопасности должна обеспечить:

недопущение несанкционированного использования, уничтожения, изменения, блокирования (ограничения), копирования, представления, распространения и иных подобных действий с данными, обрабатываемыми средствами КИИ;

предотвращение информационного воздействия на аппаратные, программно-аппаратные и программные средства, способного привести к неисправности и/или остановке деятельности объекта КИИ;

обеспечение полноценного функционирования объекта КИИ в условиях угроз кибербезопасности информации, не составляющей государственные секреты и охраняемой законодательством (далее – конфиденциальная информация);

обеспечить возможность восстановления работы объекта КИИ.

11. В автоматизированных и информационных системах подлежат защите:

все обрабатываемые данные;

аппаратные, программно-аппаратные и программные средства, в том числе компьютерные запоминающие устройства, рабочие станции, сервера, телекоммуникационное оборудование, линии связи, средства обработки графической, видео- и речевой информации;

программное обеспечение программно-аппаратных средств;

архитектура и конфигурация информационных систем.

12. В сетях телекоммуникаций подлежат защите:

данные, передаваемые по линиям связи;

телекоммуникационное оборудование, в том числе программное обеспечение, система управления;

встроенное защитное оборудование;

целостность архитектуры и конфигурации телекоммуникационной сети.

13. В автоматизированных системах управления подлежат защите:

информация о параметрах и состоянии контролируемого объекта или процесса, включая входные и выходные данные, управленческие данные, контрольно-измерительные и другие важные данные;

программное и аппаратное обеспечение, включая рабочие станции, промышленные сервера, телекоммуникационное оборудование, линии связи, программируемые логические контроллеры, производственное, технологическое оборудование;

программное обеспечение программно-аппаратных средств;

встроенное защитное оборудование;

архитектура автоматизированной системы управления и конфигурация.

14. Одним из обязательных критериев реализации мер безопасности является учет угроз кибербезопасности всем объектам и субъектам доступа на аппаратном, системном, программном и сетевом уровнях, в том числе в виртуализированной среде.

15. В зависимости от угроз кибербезопасности в устройствах обработки конфиденциальной и секретной информации на объектах КИИ должны быть реализованы следующие меры:

идентификация и аутентификация на каждом этапе получения доступа к элементам подсистемы или других систем;

управление доступом к файлам, системам и устройствам;

ограничение программной среды для пользователя, не имеющего полномочий на управление информационной инфраструктурой;

защита средств, несущих конфиденциальную и секретную информацию;

проведение аудита кибербезопасности систем, программ, в том числе программных и программно-аппаратных ресурсов;

защита объекта КИИ информационных активов от вредоносного программного обеспечения;

обнаружение, предотвращение и устранение последствий кибератак;

обеспечение целостности всех данных, передаваемых устройствами, вне зависимости от назначения применения;

обеспечение доступа и защиту данных для пользователей системы в зависимости от позиции пользователя в деятельности объекта КИИ;

обеспечение безопасности технических средств защиты информации;

управление конфигурацией;

своевременное управление обновлениями программного обеспечения;

своевременное реагирование на инциденты кибербезопасности;

выполнение необходимых действий в чрезвычайных ситуациях;

хранение резервной копии критичных данных, целостность, конфиденциальность и доступность которых связаны с работой и безопасностью объекта КИИ;

состояние кибербезопасности, несанкционированный доступ постоянный мониторинг и анализ попыток изменения информации;

внедрение механизмов быстрого восстановления данных;

аттестация объекта на соответствие требованиям кибербезопасности.

Глава 4. Заключение

16. Лица, виновные в нарушении указанных требований, несут ответственность в соответствии с актами законодательства.