QMMB: 03/22/764/0313-son
16.04.2022-y.

O‘ZBEKISTON RESPUBLIKASINING
QONUNI

О кибербезопасности

Принят Законодательной палатой 25 февраля 2022 года
Одобрен Сенатом 17 марта 2022 года

Глава 1. Общие положения

Статья 1. Цель настоящего Закона

Целью настоящего Закона является регулирование отношений в сфере кибербезопасности.

Статья 2. Законодательство о кибербезопасности

Законодательство о кибербезопасности состоит из настоящего Закона и иных актов законодательства.

Обеспечение кибербезопасности системы оперативно-розыскных мероприятий на сетях телекоммуникации и каналах связи осуществляется в порядке, установленном отдельными актами законодательства.

Если международным договором Республики Узбекистан установлены иные правила, чем те, которые предусмотрены законодательством Республики Узбекистан о кибербезопасности, то применяются правила международного договора.

Статья 3. Основные понятия

В настоящем Законе применяются следующие основные понятия:

объект информатизации – информационные системы различного уровня и назначения, сети телекоммуникаций, технические средства обработки информации, помещения, где установлены и эксплуатируются эти средства;

киберпреступность – совокупность преступлений, осуществляемых в киберпространстве с использованием программного обеспечения и технических средств, с целью завладения информацией, ее изменения, уничтожения или взлома информационных систем и ресурсов;

QMMB: 03/22/764/0313-son
16.04.2022-y.

киберпространство – виртуальная среда, созданная с помощью информационных технологий;

киберугроза – комплекс условий и факторов в киберпространстве, представляющих угрозу интересам личности, общества и государства;

кибербезопасность – состояние защищенности интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве;

инцидент кибербезопасности – событие в киберпространстве, приведшее к сбоям в работе информационных систем и (или) нарушениям доступности информации в них, целостности и ее свободного использования;

объект кибербезопасности – комплекс информационных систем, используемых в деятельности по обеспечению киберзащиты информации и кибербезопасности национальных информационных систем и ресурсов, в том числе объекты критической информационной инфраструктуры;

субъект кибербезопасности – юридическое лицо или индивидуальный предприниматель, имеющий определенные права и обязанности, связанные с владением, пользованием и распоряжением национальными информационными ресурсами и оказанием информационных электронных услуг по их использованию, защитой информации и кибербезопасностью, в том числе субъекты критической информационной инфраструктуры;

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;

кибератака – действие, представляющее угрозу кибербезопасности, умышленно осуществляемое в киберпространстве с использованием аппаратных, аппаратно-программных и программных средств;

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

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), химической, нефтехимической отраслях, металлургии, водопользования и водоснабжения, сельского хозяйства, здравоохранения, жилищно-коммунального обслуживания, банковско-финансовой системы, транспорта, информационно-коммуникационных технологий, экологии и охраны окружающей среды, добычи и переработки

QMMB: 03/22/764/0313-son
16.04.2022-y.

полезных ископаемых стратегического значения, производственной сфере, а также в 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.

Статья 4. Основные принципы обеспечения кибербезопасности

Основные принципы обеспечения кибербезопасности:

законность;

приоритет защиты интересов личности, общества и государства в киберпространстве;

единый подход к регулированию сферы кибербезопасности;

приоритет участия отечественных производителей в создании системы кибербезопасности;

открытость Республики Узбекистан к международному сотрудничеству в обеспечении кибербезопасности.

Статья 5. Принцип законности

В обеспечении кибербезопасности обязательно неукоснительное соблюдение и выполнение требований Конституции Республики Узбекистан, настоящего Закона и других актов законодательства.

Всякое отступление от точного исполнения и соблюдения требований законодательства, какими бы мотивами оно ни было вызвано, является нарушением законности и влечет за собой установленную ответственность.

Статья 6. Принцип приоритета защиты интересов личности, общества и государства в киберпространстве

Защита интересов личности, общества и государства от внешних и внутренних угроз в киберпространстве является приоритетом в обеспечении кибербезопасности государства.

Статья 7. Принцип единого подхода к регулированию сферы кибербезопасности

Единый подход к регулированию сферы кибербезопасности обеспечивается внедрением единой государственной системы киберзащиты информационных систем и ресурсов, направленной

QMMB: 03/22/764/0313-son
16.04.2022-y.

на организацию, осуществление мониторинга и контроля за процессом разработки и внедрения программных и технических средств по обработке и защите данных.

Обеспечение кибербезопасности должно осуществляться на основе единых подходов в формировании системы правового, административного и технического регулирования отношений в этой сфере.

Статья 8. Принцип приоритета участия отечественных производителей в создании системы кибербезопасности

При покупке товаров (работ, услуг), необходимых для обеспечения кибербезопасности органов государственного и хозяйственного управления, органов государственной власти на местах, товары (работы, услуги), произведенные на территории Республики Узбекистан, пользуются приоритетом по отношению к продукции, произведенной за рубежом.

Статья 9. Принцип открытости Республики Узбекистан к международному сотрудничеству в обеспечении кибербезопасности

Республика Узбекистан осуществляет международное сотрудничество в области обеспечения кибербезопасности в рамках международных договоров с международными организациями, иностранными государствами и их компетентными ведомствами.

Глава 2. Государственное регулирование сферы кибербезопасности

Статья 10. Единая государственная политика в сфере кибербезопасности

Единую государственную политику в сфере кибербезопасности определяет Президент Республики Узбекистан.

Статья 11. Уполномоченный государственный орган в сфере кибербезопасности

Служба государственной безопасности Республики Узбекистан является уполномоченным государственным органом в сфере кибербезопасности (далее – уполномоченный государственный орган).

К полномочиям уполномоченного государственного органа в сфере кибербезопасности относятся:

разработка нормативно-правовых актов и государственных программ в сфере кибербезопасности;

QMMB: 03/22/764/0313-son
16.04.2022-y.

осуществление контроля за исполнением актов законодательства о кибербезопасности;

проведение оперативно-розыскных мероприятий, доследственных проверок и следственных действий по инцидентам кибербезопасности;

предупреждение, выявление и предотвращение инцидентов кибербезопасности и принятие по ним соответствующих мер, в том числе организационно-технических мер по устранению их последствий;

киберзащита информационных систем и ресурсов при чрезвычайных ситуациях и разработка планов, содержащих меры по другим вопросам в сфере кибербезопасности;

организация работ по обеспечению кибербезопасности, а также работ по предупреждению, выявлению и устранению последствий кибератак на объектах критической информационной инфраструктуры;

организация работ по сертификации аппаратных, аппаратно-программных и программных средств в информационных системах и ресурсах в соответствии с требованиями кибербезопасности;

организация проведения исследований и мониторинга в сфере кибербезопасности;

формирование единого реестра объектов критической информационной инфраструктуры, а также организация и обеспечение его ведения;

принятие решения о включении объектов в единый реестр объектов критической информационной инфраструктуры на основе сведений, представленных субъектами кибербезопасности;

определение требований по обеспечению кибербезопасности объектов критической информационной инфраструктуры;

определение порядка проведения аттестации объектов информатизации и объектов критической информационной инфраструктуры в соответствии с требованиями кибербезопасности;

лицензирование деятельности по разработке, производству и реализации средств криптографической защиты информации;

принятие мер по защите прав и законных интересов пользователей информационных систем и ресурсов;

проведение изучений и проверок информационных систем и ресурсов субъектов кибербезопасности, а также на объектах критической информационной инфраструктуры;

разработка планов по предотвращению попыток кибератак на объекты критической информационной инфраструктуры и их непосредственная реализация;

регулирование деятельности подразделений кибербезопасности, служб и групп независимых экспертов, взаимодействие с правоохранительными органами в сфере противодействия киберугрозам;

информирование органов государственного и хозяйственного управления, органов государственной власти на местах о выявленных в информационных системах и ресурсах уязвимостях, киберугрозах, кибератаках и других подрывных действиях;

QMMB: 03/22/764/0313-son
16.04.2022-y.

привлечение правоохранительных органов и субъектов критической информационной инфраструктуры к совместному расследованию инцидентов кибербезопасности на объектах критической информационной инфраструктуры;

осуществление международного сотрудничества в сфере кибербезопасности и разработка общих подходов по противодействию киберугрозам, объединение усилий в проведении следственных действий и предотвращении киберпреступности, а также принятие мер по недопущению использования киберпространства Республики Узбекистан в террористической, экстремистской и иной незаконной деятельности;

организация работ по внедрению средств выявления, предотвращения и устранения последствий кибератак, а также принятие мер относительно инцидентов кибербезопасности на объектах критической информационной инфраструктуры;

организация работ по выявлению, сбору и анализу данных об имеющихся уязвимостях и возможных угрозах на объектах критической информационной инфраструктуры;

создание классификатора по уровню обеспеченности кибербезопасности в информационных системах и ресурсах;

классификация объектов кибербезопасности по уровню обеспеченности кибербезопасности;

осуществление деятельности по подготовке кадров в сфере кибербезопасности;

определение механизмов проведения экспертизы на соответствие требованиям кибербезопасности;

определение методов оценки и оценка осуществления кибербезопасности объектов кибербезопасности и критической информационной инфраструктуры;

определение критериев категорирования и категорирование объектов критической информационной инфраструктуры;

проведение аттестации сотрудников, задействованных в обеспечении кибербезопасности субъектов кибербезопасности, в порядке, установленном законодательством.

Выполнение законных требований (указаний) уполномоченного государственного органа является обязательным.

Статья 12. Права уполномоченного государственного органа

Уполномоченный государственный орган при осуществлении полномочий в сфере кибербезопасности имеет право:

получать в аренду технические, программные и аппаратно-программные средства, предназначенные для выявления кибератак, предотвращения и устранения их последствий, а также принятия мер относительно инцидентов кибербезопасности;

QMMB: 03/22/764/0313-son
16.04.2022-y.

безвозмездно пользоваться техническими установками и услугами для принятия безотлагательных мер по устранению кибератак;

посещать государственные органы и иные организации, знакомиться с необходимыми документами и материалами, а также запрашивать и получать от государственных органов и иных организаций, граждан сведения и другие необходимые документы и материалы, проводить их идентификацию и использовать в следственных действиях по инцидентам кибербезопасности;

создавать рабочий орган по обеспечению кибербезопасности, а также передавать ему часть своих полномочий;

вносить субъектам кибербезопасности обязательные для исполнения предписания и указания об устранении причин и условий, способствовавших совершению правонарушений, представляющих угрозу кибербезопасности;

в целях осуществления функции государственного контроля и проверки обеспечения состояния кибербезопасности на беспрепятственный доступ и подключение в установленном порядке к информационным системам и ресурсам государственных органов и организаций, объектов критической информационной инфраструктуры, а также изучение данных в части внедрения и эксплуатации средств обеспечения кибербезопасности информационных систем и ресурсов этих объектов;

на доступ к системам мониторинга или объектам критической информационной инфраструктуры для осуществления организационно-технических мероприятий при проведении мониторинговых работ по обеспечению кибербезопасности;

входить беспрепятственно, при необходимости с повреждением запирающих устройств и других предметов, в жилые помещения и иные объекты физических и юридических лиц, осматривать их при преследовании лиц, подозреваемых в совершении преступлений в сфере информационных технологий, либо при наличии достаточных оснований полагать, что там совершается или совершено такое преступление, или находится лицо, скрывшееся от правоохранительных органов, либо если промедление может поставить под угрозу жизнь и здоровье граждан, с последующим сообщением об этом прокурору в течение двадцати четырех часов, а также с возмещением причиненного вреда в порядке, установленном законодательством.

Статья 13. Обязанности уполномоченного государственного органа

Уполномоченный государственный орган при осуществлении возложенных полномочий в сфере кибербезопасности обязан:

принимать все необходимые меры по предупреждению, выявлению и предотвращению киберпреступлений;

QMMB: 03/22/764/0313-son
16.04.2022-y.

участвовать в подготовке и реализации государственных программ в сфере кибербезопасности;

осуществлять научно-исследовательскую и организационно-методичесую деятельность по проблемам в сфере кибербезопасности;

регистрировать обращения и сведения о киберпреступлениях и правонарушениях, представляющих угрозу кибербезопасности, своевременно принимать по ним меры в порядке, установленном законодательством;

принимать меры по предупреждению правонарушений, представляющих угрозу кибербезопасности, выявлению и устранению причин и условий, способствовавших их совершению;

уведомлять в письменной форме прокурора в течение двадцати четырех часов обо всех случаях проникновения сотрудниками уполномоченного государственного органа в жилые помещения и иные объекты физических и юридических лиц вопреки воле собственников и их представителей или в их отсутствие.

На уполномоченный государственный орган могут быть возложены и другие обязанности в соответствии с законодательством.

Глава 3. Права и обязанности государственных органов и организаций в обеспечении кибербезопасности. Резервное копирование данных

Статья 14. Права и обязанности государственных органов и организаций в обеспечении кибербезопасности

Государственные органы и организации имеют право:

получать от уполномоченного государственного органа в целях обеспечения кибербезопасности информацию о киберугрозах, уязвимостях программного обеспечения, оборудования и технологий;

получать от уполномоченного государственного органа информацию и консультации о средствах и методах защиты от кибератак, способах их выявления и предотвращения;

разрабатывать и реализовывать меры по обеспечению кибербезопасности.

Государственные органы и организации обязаны:

обеспечивать кибербезопасность в находящихся в их ведении информационных системах и ресурсах, стабильность работы сетей, а также выполнять свои обязательства по кибербезопасности, предупреждать уполномоченный государственный орган о кибератаках;

принимать меры по предотвращению случаев хищения и фальсификации данных, хранящихся в их информационных системах и ресурсах;

QMMB: 03/22/764/0313-son
16.04.2022-y.

использовать сертифицированные аппаратные, аппаратно-программные и программные средства для киберзащиты своих информационных систем и ресурсов;

согласовывать с уполномоченным государственным органом разрабатываемые нормативно-правовые акты в сфере кибербезопасности и нормативные документы в области технического регулирования.

Статья 15. Резервное копирование данных

Обеспечение хранения данных информационных систем и ресурсов государственных органов и организаций, а также объектов критической информационной инфраструктуры осуществляется в соответствии с внутренней политикой информационной безопасности путем создания резервной копии данных, срок хранения которой не должен быть менее трех последних месяцев.

Глава 4. Обеспечение кибербезопасности

Статья 16. Права и обязанности субъектов кибербезопасности

Субъекты кибербезопасности имеют право:

получать от уполномоченного государственного органа сведения о киберугрозах, уязвимостях программного обеспечения, оборудовании и технологиях в целях обеспечения своей кибербезопасности;

получать сведения и консультации уполномоченного государственного органа о средствах и методах защиты от кибератак, а также методах их выявления и предотвращения;

разрабатывать и реализовывать меры по обеспечению своей кибербезопасности.

Субъекты кибербезопасности обязаны:

предотвращать незаконное распространение, хищение, утерю, нарушение целостности, блокировку и фальсификацию данных в информационных системах и ресурсах, а также иные виды несанкционированного доступа (входа) к информационным системам и ресурсам, принимать своевременные соответствующие меры при выявлении таких случаев;

в целях минимизации негативных последствий при нарушении порядка доступа в информационные системы и ресурсы и в случае их изменения или удаления в результате несанкционированного доступа к ним принимать меры по их оперативному восстановлению;

уведомлять уполномоченный государственный орган о произошедших инцидентах кибербезопасности и киберпреступлениях, принимать меры по недопущению утери соответствующих цифровых следов для полного раскрытия данных инцидентов, а также обеспечивать

QMMB: 03/22/764/0313-son
16.04.2022-y.

постоянное хранение сведений, необходимых для анализа инцидентов кибербезопасности и расследования киберпреступлений;

осуществлять взаимный обмен с уполномоченным государственным органом данными в сфере охраны и проведения мониторинга безопасной работы объектов кибербезопасности;

соблюдать требования кибербезопасности, определенные уполномоченным государственным органом, в обеспечении киберзащиты информационных систем и ресурсов;

обеспечивать функционирование механизмов принятия мер в отношении инцидентов кибербезопасности и работу подразделений по обеспечению кибербезопасности, а в случае их отсутствия – пользоваться услугами аутсорсинга с разрешения уполномоченного государственного органа в установленном порядке;

предоставлять уполномоченному государственному органу право доступа в мониторинговые системы и (или) объекты кибербезопасности для осуществления организационно-технических мероприятий мониторинга обеспечения кибербезопасности.

Статья 17. Классификация объектов кибербезопасности

Классификация объектов кибербезопасности состоит из комплекса организационных мероприятий, направленных на определение уровня организационно-технической сложности типа объектов кибербезопасности.

Категории объектов кибербезопасности, подлежащие классификации, определяются в соответствии с законодательством.

Статья 18. Экспертиза на соответствие требованиям кибербезопасности

Экспертиза на соответствие требованиям кибербезопасности осуществляется в обязательном порядке или по инициативе субъектов кибербезопасности.

Экспертизе на соответствие требованиям кибербезопасности в обязательном порядке подлежат:

информационные ресурсы государственных органов;

информационные системы государственных органов;

информационные системы, включенные в категорию объектов критической информационной инфраструктуры.

Порядок проведения экспертизы на соответствие требованиям кибербезопасности определяется уполномоченным государственным органом.

QMMB: 03/22/764/0313-son
16.04.2022-y.

Статья 19. Сертификация аппаратных, аппаратно-программных и программных средств, применяемых для обеспечения кибербезопасности информационных систем и ресурсов

Аппаратные, аппаратно-программные и программные средства, применяемые для обеспечения кибербезопасности информационных систем и ресурсов государственных органов и организаций, а также объектов критической информационной инфраструктуры, подлежат сертификации в обязательном порядке.

Порядок сертификации аппаратных, аппаратно-программных и программных средств, применяемых для обеспечения кибербезопасности информационных систем и ресурсов, устанавливается уполномоченным государственным органом.

Статья 20. Аттестация объектов информатизации и объектов критической информационной инфраструктуры

Аттестацией объектов информатизации и объектов критической информационной инфраструктуры является комплекс организационно-технических мероприятий, направленных на определение соответствия фактического состояния защищенности объектов информатизации требованиям государственных стандартов и нормативно-правовых актов в сфере кибербезопасности.

Категории объектов информатизации и объектов критической информационной инфраструктуры, подлежащих аттестации, определяются в соответствии с законодательством.

Порядок проведения аттестации объектов информатизации и объектов критической информационной инфраструктуры на соответствие требованиям кибербезопасности определяется уполномоченным государственным органом.

Статья 21. Оценка уровня обеспечения кибербезопасности

Оценкой уровня обеспечения кибербезопасности является комплекс организационно-технических мероприятий, направленных на определение состояния защищенности информационных систем и ресурсов, а также эффективности принимаемых организационных мер.

Категории объектов информатизации и объектов критической информационной инфраструктуры, подлежащих обязательной оценке, определяются в соответствии с законодательством.

Порядок оценки уровня обеспечения кибербезопасности определяется уполномоченным государственным органом.

QMMB: 03/22/764/0313-son
16.04.2022-y.

Уполномоченный государственный орган дает обязательные к исполнению предписания об устранении недостатков, выявленных в результате оценки.

Глава 5. Инциденты кибербезопасности

Статья 22. Расследование инцидентов кибербезопасности

Инциденты кибербезопасности расследуются уполномоченным государственным органом или должностными лицами рабочего органа по обеспечению кибербезопасности.

Владелец информационного ресурса или информационной системы, в которой произошел инцидент кибербезопасности, может провести расследование инцидента кибербезопасности, если он обладает необходимыми ресурсами и техническими возможностями для проведения расследования. При этом уполномоченный государственный орган должен быть уведомлен о результатах расследования.

Статья 23. Принятие субъектами кибербезопасности мер по инцидентам кибербезопасности

Принятие мер субъектами кибербезопасности в отношении инцидентов кибербезопасности может осуществляться в следующих формах:

предотвращение уязвимостей и ошибок в программном обеспечении и устройствах;

уничтожение вредоносных программ, ограничение их распространения, техническое ограничение источника кибератак;

изоляция объектов информатизации от реальных киберугроз;

предоставление правоохранительным органам сведений об инцидентах кибербезопасности.

Статья 24. Раскрытие информации об инцидентах кибербезопасности

Информация о выявленных в информационных системах и ресурсах уязвимостях, киберугрозах, кибератаках и других подрывных действиях, а также об объектах информатизации может быть раскрыта с разрешения субъекта кибербезопасности после принятия соответствующих мер по их защите.

Информация о выявленных киберугрозах и уязвимостях должна быть использована исключительно для их устранения и предотвращения незаконных действий.

QMMB: 03/22/764/0313-son
16.04.2022-y.

Глава 6. Объекты критической информационной инфраструктуры

Статья 25. Основные направления обеспечения кибербезопасности объектов критической информационной инфраструктуры

Основными направлениями обеспечения кибербезопасности объектов критической информационной инфраструктуры являются:

создание единого комплекса мер по регулированию нормативно-правовой, организационной и технической защиты объектов критической информационной инфраструктуры;

установление требований по обеспечению кибербезопасности в информационных системах и ресурсах государственных органов и организаций, на объектах критической информационной инфраструктуры;

содействие созданию условий для эффективного обеспечения кибербезопасности объектов критической информационной инфраструктуры.

Статья 26. Категорирование объектов критической информационной инфраструктуры

Категорирование объектов критической информационной инфраструктуры осуществляется в целях определения соответствия объектов критической информационной инфраструктуры категориям, предусмотренным частью второй настоящей статьи, а также проверки сведений по результатам категорирования.

Объекты критической информационной инфраструктуры подразделяются на следующие категории:

объекты критической информационной инфраструктуры высокого уровня;

объекты критической информационной инфраструктуры среднего уровня;

объекты критической информационной инфраструктуры низкого уровня.

Критерии категорирования объектов критической информационной инфраструктуры определяются уполномоченным государственным органом.

Статья 27. Единый реестр объектов критической информационной инфраструктуры

Уполномоченный государственный орган ведет единый реестр объектов критической информационной инфраструктуры.

QMMB: 03/22/764/0313-son
16.04.2022-y.

Категории объектов кибербезопасности, подлежащих обязательному внесению в единый реестр объектов критической информационной инфраструктуры, определяются в соответствии с законодательством.

Порядок внесения объектов кибербезопасности в единый реестр объектов критической информационной инфраструктуры определяется уполномоченным государственным органом.

Статья 28. Права и обязанности субъектов критической информационной инфраструктуры

Субъекты критической информационной инфраструктуры имеют право:

получать от уполномоченного государственного органа сведения о киберугрозах, уязвимостях программного обеспечения, оборудования и технологий в целях обеспечения кибербезопасности объектов критической информационной инфраструктуры;

получать сведения и консультации от уполномоченного государственного органа о средствах и методах защиты от кибератак, а также методах их выявления и предотвращения;

разрабатывать и реализовывать меры по обеспечению кибербезопасности объектов критической информационной инфраструктуры.

Субъекты критической информационной инфраструктуры обязаны:

обеспечивать непрерывное функционирование информационных систем объектов критической информационной инфраструктуры;

доводить до сведения уполномоченного государственного органа информацию об инцидентах кибербезопасности;

оказывать содействие должностным лицам уполномоченного государственного органа или рабочего органа по обеспечению кибербезопасности в выявлении, предотвращении и устранении последствий кибератак, определении причин и условий происхождения инцидентов кибербезопасности;

устанавливать и эксплуатировать мониторинговые системы с соблюдением технических требований эксплуатации аппаратных, программных и аппаратно-программных средств для предотвращения кибератак, устранения их последствий, а также принятия мер в отношении инцидентов кибербезопасности на объектах критической информационной инфраструктуры;

обеспечивать безопасность объектов критической информационной инфраструктуры в соответствии с требованиями кибербезопасности;

выполнять указания уполномоченного государственного органа по устранению выявленных правонарушений в части обеспечения кибербезопасности на объектах критической информационной инфраструктуры;

QMMB: 03/22/764/0313-son
16.04.2022-y.

принимать меры по устранению последствий инцидентов кибербезопасности и кибератак на объекты критической информационной инфраструктуры;

предоставлять уполномоченному государственному органу права доступа в мониторинговые системы или на объекты критической информационной инфраструктуры для осуществления организационно-технических мероприятий мониторинга состояния обеспечения кибербезопасности;

уведомлять уполномоченный государственный орган при изменении сведений об объекте, включенном в единый реестр объектов критической информационной инфраструктуры.

Статья 29. Требования по обеспечению кибербезопасности объектов критической информационной инфраструктуры

Субъекты критической информационной инфраструктуры обязаны выполнять установленные уполномоченным государственным органом требования по обеспечению кибербезопасности на принадлежащих им объектах критической информационной инфраструктуры.

Субъекты критической информационной инфраструктуры по согласованию с уполномоченным государственным органом, исходя из специфики работы объектов критической информационной инфраструктуры, могут устанавливать дополнительные требования для обеспечения кибербезопасности.

Сотрудники, ответственные за обеспечение кибербезопасности объектов критической информационной инфраструктуры, проходят аттестацию, проводимую уполномоченным государственным органом, в порядке, установленном законодательством.

Система обеспечения кибербезопасности объектов критической информационной инфраструктуры, созданная субъектом критической информационной инфраструктуры, на основании решения уполномоченного государственного органа подключается к системе мониторинга и управления инцидентами кибербезопасности объектов критической информационной инфраструктуры уполномоченного государственного органа.

Статья 30. Система обеспечения кибербезопасности объектов критической информационной инфраструктуры

Система обеспечения кибербезопасности объектов критической информационной инфраструктуры состоит из:

системы мониторинга и управления инцидентами кибербезопасности объектов критической информационной инфраструктуры уполномоченного государственного органа;

QMMB: 03/22/764/0313-son
16.04.2022-y.

систем обеспечения кибербезопасности объектов критической информационной инфраструктуры.

Информация об инцидентах кибербезопасности в системе обеспечения кибербезопасности является ограниченной к распространению. Данная информация может быть раскрыта после полного устранения инцидентов.

Статья 31. Оценка кибербезопасности объектов критической информационной инфраструктуры

Оценка кибербезопасности объектов критической информационной инфраструктуры осуществляется в целях определения состояния (уровня) защищенности данных объектов от различных киберугроз в рамках государственного контроля в сфере кибербезопасности.

Оценка кибербезопасности объектов критической информационной инфраструктуры осуществляется с разрешения уполномоченного государственного органа с привлечением специализированных организаций.

Глава 7. Поддержка и развитие в сфере кибербезопасности

Статья 32. Государственная поддержка субъектов кибербезопасности

Государственной поддержкой субъектов кибербезопасности являются:

совершенствование нормативно-правовой базы в сфере кибербезопасности;

предоставление субъектам кибербезопасности налоговых, таможенных льгот и преференций;

создание условий для привлечения средств хозяйствующих субъектов для финансирования сферы кибербезопасности;

организация государственных закупок в сфере кибербезопасности, нацеленных на обеспечение гарантированного внедрения продуктов и передовых технологий, основанных на научно-технических достижениях;

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

Статья 33. Поддержка научно-технической и инновационной деятельности в сфере кибербезопасности

Поддержка научно-технической и инновационной деятельности в сфере кибербезопасности осуществляется органами государственного управления, органами государственной власти на местах и хозяйствующими субъектами посредством:

QMMB: 03/22/764/0313-son
16.04.2022-y.

размещения заказа для выполнения научно-исследовательских, опытно-конструкторских и технологических работ в рамках государственного заказа;

выделения субсидий субъектам кибербезопасности для финансирования научно-исследовательских, конструкторских и технологических работ, проводимых в процессе реализации инвестиционных проектов;

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

оказания финансовой помощи организациям, реализующим проекты по улучшению уровня кибербезопасности, в том числе занимающимся инновационной деятельностью в оказании услуг с использованием имеющихся передовых технологий;

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

предоставления приоритета продукции отечественного производства при проведении государственных закупок, связанных с обеспечением кибербезопасности.

Статья 34. Развитие и поддержка кадрового потенциала в сфере обеспечения кибербезопасности

Поддержка развития кадрового потенциала органов государственного управления, органов государственной власти на местах и хозяйствующих субъектов в сфере обеспечения кибербезопасности может осуществляться посредством:

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

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

Работники, ответственные за обеспечение кибербезопасности субъектов критической информационной инфраструктуры, на постоянной основе должны повышать свою квалификацию в соответствии с международными и государственными стандартами и требованиями.

Статья 35. Стимулирование работников, ответственных за обеспечение кибербезопасности объектов критической информационной инфраструктуры

Стимулирование работников, ответственных за обеспечение кибербезопасности объектов критической информационной инфраструктуры, осуществляется в установленном законодательством порядке.

QMMB: 03/22/764/0313-son
16.04.2022-y.

Глава 8. Заключительные положения

Статья 36. Международное сотрудничество в сфере кибербезопасности

Уполномоченный государственный орган в пределах своих полномочий осуществляет международное сотрудничество в сфере кибербезопасности.

Уполномоченный государственный орган в соответствии с законодательством и международными договорами Республики Узбекистан по запросу предоставляет иностранным государствам и международным организациям информацию по вопросам борьбы с международной киберпреступностью.

Информация по вопросам борьбы с международной киберпреступностью может быть представлена иностранным государствам и международным организациям предварительно без запроса, если такие сведения не препятствуют следственным действиям или судебному процессу и служат приостановлению кибератак, своевременному выявлению и устранению преступных действий, совершаемых с использованием киберпространства.

Статья 37. Ответственность за нарушение законодательства о кибербезопасности

Лица, виновные в нарушении законодательства о кибербезопасности, несут ответственность в установленном порядке.

Статья 38. Обеспечение исполнения, доведения, разъяснения сути и значения настоящего Закона

Службе государственной безопасности Республики Узбекистан и другим заинтересованным организациям обеспечить исполнение, доведение до исполнителей и разъяснение среди населения сути и значения настоящего Закона.

Статья 39. Приведение законодательства в соответствие с настоящим Законом

Кабинету Министров Республики Узбекистан:

привести решения правительства в соответствие с настоящим Законом;

обеспечить пересмотр и отмену органами государственного управления их нормативно-правовых актов, противоречащих настоящему Закону.

QMMB: 03/22/764/0313-son
16.04.2022-y.

Статья 40. Вступление в силу настоящего Закона

Настоящий Закон вступает в силу по истечении трех месяцев со дня его официального опубликования.

Президент
Республики Узбекистан **Ш. Мирзиёев**

O'ZBEKISTON RESPUBLIKASI PREZIDENTI ADMINISTRATSIYASI
KANSELYARIYA
1

город Ташкент,
15 апреля 2022 года
№ ЗРУ–764