Утверждены
постановлением Правительства
Республики Казахстан
от « 18 » января 2020 года
№ 12

Изменения и дополнения, которые вносятся в некоторые решения Правительства Республики Казахстан

1. В постановлении Правительства Республики Казахстан от 3 сентября 2013 года № 909 «Об утверждении Правил осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных»
(САПП Республики Казахстан, 2013 г., № 52, ст. 725):

Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных, утвержденные указанным постановлением, изложить в новой редакции согласно приложению 1 к настоящим изменениям и дополнениям.

2. В постановлении Правительства Республики Казахстан от 12 ноября
2013 года № 1214 «Об утверждении Правил определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач» (САПП Республики Казахстан, 2013 г., № 65, ст. 884):

Правила определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач, утвержденные указанным постановлением, изложить в новой редакции согласно приложению 2 к настоящим изменениям и дополнениям.

3. В постановлении Правительства Республики Казахстан от 8 сентября 2016 года № 529 «Об утверждении Правил и критериев отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры»
(САПП Республики Казахстан, 2016 г., № 48, ст. 306):

в Правилах отнесения объектов информационно-коммуникационной инфраструктуры к критически важным объектам информационно-коммуникационной инфраструктуры, утвержденных указанным постановлением:

подпункт 4) пункта 2 изложить в следующей редакции:

«4) критически важные объекты информационно-коммуникационной инфраструктуры (далее – КВОИКИ) – объекты информационно-коммуникационной инфраструктуры, нарушение или прекращение функционирования которых приводят к чрезвычайной ситуации

социального и (или) техногенного характера или значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства или жизнедеятельности населения, проживающего на соответствующей территории, в том числе инфраструктуры: теплоснабжения, электроснабжения, газоснабжения, водоснабжения, промышленности, здравоохранения, связи, банковской сферы, транспорта, гидротехнических сооружений, правоохранительной деятельности, «электронного правительства».»;

пункты 7 и 8 изложить в следующей редакции:

«7. Комиссия рассматривает представленные предложения, документы, материалы и выносит рекомендацию:

1) о включении объекта информационно-коммуникационной инфраструктуры в перечень;

2) об отклонении заявки о включении объекта информационно-коммуникационной инфраструктуры в перечень;

3) об исключении объекта информационно-коммуникационной инфраструктуры из перечня критически важной информационно-коммуникационной инфраструктуры в соответствии с пунктом 11 настоящих Правил.

8. Рекомендация комиссии оформляется протоколом, в котором должны содержаться следующие сведения:

1) дата и место проведения заседания;

2) состав комиссии;

3) количество рассмотренных заявок;

4) рекомендация комиссии по каждому объекту информационно-коммуникационной инфраструктуры с обоснованием соответствия либо несоответствия установленным критериям.»;

пункт 10 изложить в следующей редакции:

«10. Уполномоченный орган на основании протокола комиссии принимает одно из трех решений:

1) о включении объекта информационно-коммуникационной инфраструктуры в перечень;

2) об отклонении заявки о включении объекта информационно-коммуникационной инфраструктуры в перечень;

3) об исключении объекта информационно-коммуникационной инфраструктуры из перечня критически важной информационно-коммуникационной инфраструктуры.

Уполномоченный орган формирует перечень и ежегодно не позднее 1 июля в установленном законодательством порядке вносит его на утверждение в Правительство Республики Казахстан. К перечню прикладываются протокол комиссии и заявки центральных государственных и местных исполнительных органов, собственников (владельцев) стратегических объектов, особо важных государственных объектов, объектов отраслей экономики, имеющих стратегическое значение.».

4. В постановлении Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности» (САПП Республики Казахстан, 2016 г., № 65, ст. 428):

в единых требованиях в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденных указанным постановлением:

изменение вносится в текст на казахском языке, текст на русском языке не изменяется;

пункт 3 изложить в следующей редакции:

«3. Положения ЕТ не распространяются на:

1) отношения, возникающие при осуществлении Национальным Банком Республики Казахстан и организациями, входящими в его структуру, работ по созданию или развитию, эксплуатации интернет-ресурсов, информационных систем, не интегрируемых с объектами информационно-коммуникационной инфраструктуры «электронного правительства», локальных сетей и сетей телекоммуникаций, а также проведении закупок товаров, работ и услуг в сфере информатизации;

2) информационные системы в защищенном исполнении, отнесенные к государственным секретам в соответствии с законодательством Республики Казахстан о государственных секретах, а также сети телекоммуникаций специального назначения и/или президентской, правительственной, засекреченной, шифрованной и кодированной связи;

3) отношения, возникающие при осуществлении уполномоченным органом по регулированию, контролю и надзору финансового рынка и финансовых организаций работ по созданию или развитию информационных систем, интегрируемых с информационными системами Национального Банка Республики Казахстан, которые не интегрируются с объектами информационно-коммуникационной инфраструктуры «электронного правительства»;

4) организации в случаях, когда исполнение таких положений ведет к нарушению пункта 4 статьи 50 Закона Республики Казахстан «О банках и банковской деятельности в Республике Казахстан».»;

подпункт 3) пункта 5 изложить в следующей редакции:

«3) установление требований по унификации компонентов объектов информационно-коммуникационной инфраструктуры;»;

в пункте 6:

подпункт 17) изложить в следующей редакции:

«17) локальная сеть внешнего контура (далее – ЛС внешнего контура) – локальная сеть субъектов информатизации, определенных уполномоченным органом, отнесенная к внешнему контуру телекоммуникационной сети субъектов информатизации, имеющая соединение с Интернетом, доступ к которому для субъектов информатизации предоставляется операторами связи только через единый шлюз доступа к Интернету;»;

подпункт 23) изложить в следующей редакции:

«23) локальная сеть внутреннего контура (далее – ЛС внутреннего контура) – локальная сеть субъектов информатизации, определенных уполномоченным органом, отнесенная к внутреннему контуру телекоммуникационной сети субъектов информатизации, имеющая соединение с единой транспортной средой государственных органов;»;

дополнить подпунктами 26) и 27) следующего содержания:

«26) межсетевой экран – аппаратно-программный или программный комплекс, функционирующий в информационно-коммуникационной инфраструктуре, осуществляющий контроль и фильтрацию сетевого трафика в соответствии с заданными правилами;

27) субъекты информатизации, определенные уполномоченным органом, – государственные органы, их подведомственные организации и органы местного самоуправления, а также иные субъекты информатизации, использующие единую транспортную среду государственных органов для взаимодействия локальных (за исключением локальных сетей, имеющих доступ к Интернету), ведомственных и корпоративных сетей.»;

пункт 7 дополнить подпунктом 18) следующего содержания:

«18) СИ – субъекты информатизации, определенные уполномоченным органом.»;

пункт 8 изложить в следующей редакции:

«8. Информатизация ГО осуществляется в соответствии с архитектурой ГО, разрабатываемой и утверждаемой в порядке, предусмотренном статьями 23 и 24 Закона, а в случае ее отсутствия – на основании решения государственного органа о необходимости автоматизации, согласованного с уполномоченным органом в сфере информатизации (далее – уполномоченный орган).

Государственные органы обеспечивают публичное обсуждение планируемой автоматизации деятельности в целях привлечения потенциальных поставщиков, уточнения технико-экономических, эксплуатационных и иных характеристик объекта информатизации «электронного правительства».

Публичное обсуждение планируемой автоматизации деятельности осуществляется на архитектурном портале «электронного правительства» (далее – архитектурный портал).

Срок для публичного обсуждения планируемой автоматизации должен составлять не менее десяти календарных дней с даты размещения на архитектурном портале.

Государственные органы рассматривают предложения, поступившие в рамках публичного обсуждения планируемой автоматизации, и принимают решения о принятии предложений либо их отклонении с указанием оснований для отклонения.

По истечении срока публичного обсуждения планируемой автоматизации в соответствии с результатами рассмотрения поступивших предложений на архитектурном портале формируется и публикуется отчет о завершении публичного обсуждения планируемой автоматизации (далее – отчет).

Отчет является основанием для уточнения технико-экономических, эксплуатационных и иных характеристик объекта информатизации «электронного правительства», выбора механизма реализации автоматизации деятельности государственного органа.

Государственный орган направляет запрос о необходимости автоматизации деятельности (далее – запрос) с приложением отчета в уполномоченный орган на согласование.

Уполномоченный орган для проведения анализа запроса государственного органа привлекает сервисного интегратора «электронного правительства» (далее – сервисный интегратор).

На основании заключения сервисного интегратора уполномоченный орган согласовывает либо отказывает в согласовании автоматизации деятельности государственного органа.»;

подпункт 1) пункта 13 изложить в следующей редакции:

«1) закупа, с учетом заключения уполномоченного органа в сфере информатизации на представленные администраторами бюджетных программ расчетов расходов на государственные закупки товаров, работ и услуг в сфере информатизации;»;

пункт 17 изложить в следующей редакции:

«17. Требования к унифицированному рабочему месту или терминальной системе ГО и МИО, а также компонентам объектов информационно-коммуникационной инфраструктуры утверждаются уполномоченным органом.»;

дополнить пунктом 17-1 следующего содержания:

«17-1. Обеспечивается соответствие рабочего места или терминальной системы ГО и МИО требованиям к унифицированному рабочему месту или терминальной системе ГО и МИО, утвержденным уполномоченным органом.

Требования обновляются и актуализируются по мере необходимости.»;

подпункт 2) пункта 20 изложить в следующей редакции:

«2) на регулярной основе проводится учет рабочих станций с проверкой конфигурации, а также электронных носителей информации с уникальными идентифицирующими данными;»;

пункты 29 и 30 изложить в следующей редакции:

«29. При организации, обеспечении и управлении ИБ в ГО, МИО или организации необходимо руководствоваться положениями стандарта Республики Казахстан СТ РК ISO/IEC 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации».

30. В целях разграничения ответственности и функций в сфере обеспечения ИБ создается подразделение ИБ, являющееся структурным подразделением, обособленным от других структурных подразделений, занимающихся вопросами создания, сопровождения и развития объектов информатизации, или определяется должностное лицо, ответственное за обеспечение ИБ.

Сотрудники, ответственные за обеспечение ИБ, проходят специализированные курсы в сфере обеспечения ИБ не реже одного раза в три года с выдачей сертификата.»;

дополнить пунктом 32-1 следующего содержания:

«32-1. Перечень внутренних документов финансовой организации, детализирующий требования политики ИБ, определяется в соответствии с нормативными правовыми актами уполномоченного органа по регулированию, контролю и надзору финансового рынка и финансовых организаций, регулирующими деятельность финансовых организаций по обеспечению информационной безопасности.»;

подпункт 4) пункта 37 изложить в следующей редакции:

«4) формирование каталога угроз (рисков) ИБ, включающего оценку (переоценку) идентифицированных рисков в соответствии с требованиями стандарта Республики Казахстан СТ РК ISO/IEC 27005-2013 «Информационные технологии. Методы обеспечения безопасности. Менеджмент риска информационной безопасности».»;

пункт 45 изложить в следующей редакции:

«45. При инициировании создания или развития объектов информатизации первого и второго классов в соответствии с классификатором объектов информатизации, утвержденным уполномоченным органом в сфере информатизации в соответствии с подпунктом 11) статьи 7 Закона (далее – классификатор), а также конфиденциальных ИС разрабатываются профили защиты для составных компонентов и задание по безопасности в соответствии с требованиями стандарта Республики Казахстан СТ РК ISO/IEC 15408-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».»;

дополнить пунктом 50-1 следующего содержания:

«50-1. Собственники или владельцы негосударственных информационных систем, интегрируемых с информационными системами государственных органов, до интеграции с информационными системами государственных органов создают собственный оперативный центр информационной безопасности и обеспечивают его функционирование или приобретают услуги оперативного центра информационной безопасности у третьих лиц в соответствии с Гражданским кодексом Республики Казахстан, а также взаимодействие его с Национальным координационным центром информационной безопасности.

Собственники или владельцы критически важных объектов информационно-коммуникационной инфраструктуры, за исключением государственных органов, органов местного самоуправления, государственных юридических лиц, субъектов квазигосударственного сектора, в течение года со дня включения в перечень критически важных объектов информационно-коммуникационной инфраструктуры создают собственный оперативный центр информационной безопасности и обеспечивают его функционирование или приобретают услуги оперативного центра информационной безопасности у третьих лиц в соответствии с Гражданским

кодексом Республики Казахстан, а также обеспечивают взаимодействие его с Национальным координационным центром информационной безопасности.»;

пункты 54 и 54-1 изложить в следующей редакции:

«54. На этапе опытной и промышленной эксплуатации объектов информатизации используются средства и системы:

обнаружения и предотвращения вредоносного кода;

мониторинга и управления инцидентами и событиями ИБ;

обнаружения и предотвращения вторжений;

мониторинга и управления информационной инфраструктурой.

54-1. Для защиты объектов информатизации допускается применение системы предотвращения утечки данных (DLP), в том числе отечественной разработки, соответствующих оценочным уровням доверия не ниже ОУД4, согласно СТ РК ISO/IEC 15408-2-2017 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

При этом, обеспечиваются:

визуальное уведомление пользователя о проводимом контроле действий;

получение письменного согласия пользователя на осуществление контроля его действий;

размещение центра управления и серверов системы предотвращения утечки данных в пределах локальной сети.»;

дополнить пунктом 56-1 следующего содержания:

«56-1. Владелец критически важных объектов информационно-коммуникационной инфраструктуры, обрабатывающий данные, содержащие охраняемую законом тайну, проводит аудит информационной безопасности не реже одного раз в год. Аудит информационной безопасности банков второго уровня проводится в соответствии с требованиями банковского законодательства Республики Казахстан.»;

дополнить пунктами 62-1 и 62-2 следующего содержания:

«62-1. Интернет-ресурс с зарегистрированным доменным именем .KZ и (или) .ҚАЗ размещается на аппаратно-программном комплексе, который расположен на территории Республики Казахстан;

62-2. Использование доменных имен .KZ и (или) .ҚАЗ в пространстве казахстанского сегмента Интернета при передаче данных интернет-ресурсами осуществляется с применением сертификатов безопасности.»;

пункт 85 изложить в следующей редакции:

«85. Опытная эксплуатация ИС ГО или МИО включает:

документирование процедур проведения опытной эксплуатации;

оптимизацию и устранение выявленных дефектов и недоработок с последующим их исправлением;

оформление акта о завершении опытной эксплуатации ИС;

срок проведения опытной эксплуатации не должен превышать один год.»;

дополнить пунктом 85-1 следующего содержания:

«85-1. Внедрение объекта информатизации «электронного правительства» осуществляется в соответствии с действующими на территории Республики Казахстан стандартами.»;

дополнить пунктом 92-3 следующего содержания:

«92-3. Собственники и владельцы информационных систем государственного органа создают собственный оперативный центр информационной безопасности и обеспечивают его функционирование или приобретают услуги оперативного центра информационной безопасности у третьих лиц в соответствии с Гражданским кодексом, а также обеспечивают взаимодействие его с Национальным координационным центром информационной безопасности.»;

пункт 128 изложить в следующей редакции:

«128. В целях обеспечения ИБ:

1) при организации выделенного канала связи, объединяющего локальные сети, применяются программно-технические средства защиты информации, в том числе криптографического шифрования, с использованием СКЗИ;

2) выделенный канал связи подключается к локальной сети посредством пограничного шлюза с прописанными правилами маршрутизации и политиками безопасности. Пограничный шлюз обеспечивает следующий минимальный набор функций:

централизованную авторизацию узлов сети;

конфигурацию уровней привилегий администраторов;

протоколирование действий администраторов;

статическую трансляцию сетевых адресов;

защиту от сетевых атак;

контроль состояния физических и логических портов;

фильтрацию входящих и исходящих пакетов на каждом интерфейсе;

криптографическую защиту передаваемого трафика с использованием СКЗИ;

3) при подключении ведомственной (корпоративной) сети телекоммуникаций и локальных сетей СИ между собой используются:

средства разделения и изоляции информационных потоков;

оборудование с компонентами, обеспечивающими ИБ и безопасное управление;

выделенные и интегрированные с оборудованием доступа межсетевые экраны, установленные в каждой точке подключения, с целью защиты периметра ЕТС ГО;

4) при подключении ведомственной (корпоративной) сети телекоммуникаций и локальных сетей к Интернету через ЕШДИ ГО, МИО, государственные юридические лица, субъекты квазигосударственного сектора, а также владельцы критически важных объектов ИКИ используют услуги оператора ИКИ или другого оператора связи, имеющего зарезервированные каналы связи на оборудовании ЕШДИ.

Подключение ведомственной (корпоративной) сети телекоммуникаций и локальных сетей к Интернету через ЕШДИ осуществляется в соответствии с

правилами функционирования единого шлюза доступа к Интернету, утвержденными уполномоченным органом в сфере обеспечения информационной безопасности.

5) служащие ГО, МИО и работники государственных юридических лиц, субъектов квазигосударственного сектора, а также владельцев критически важных объектов ИКИ для осуществления оперативного информационного обмена (служебной переписки) в электронной форме при исполнении ими служебных обязанностей используют:

ведомственную электронную почту, службу мгновенных сообщений и иные сервисы;

электронную почту, службу мгновенных сообщений и иные сервисы, центры управления и сервера которых физически размещены на территории Республики Казахстан, если иное не установлено уполномоченным органом;

6) взаимодействие ведомственной электронной почты ГО и МИО с внешними электронными почтовыми системами осуществляется только через единый шлюз электронной почты;

7) служащие ГО, МИО и работники государственных юридических лиц, субъектов квазигосударственного сектора, а также владельцев критически важных объектов ИКИ осуществляют доступ к ИР из ЛС внешнего конура только через ЕШДИ с использованием веб-обозревателя, являющегося СПО и соответствующего требованиям правил функционирования ЕШДИ, утвержденных уполномоченным органом в сфере обеспечения информационной безопасности.»;

пункт 129 изложить в следующей редакции:

«129. Подключение СИ к ЕТС ГО осуществляется в соответствии с правилами подключения к ЕТС ГО и предоставления доступа к интернет-ресурсу через ЕТС ГО, определяемыми уполномоченным органом.»;

пункт 131 изложить в следующей редакции:

«131. Не допускается подключение к ЕТС ГО, локальной сети СИ, а также техническим средствам, входящим в состав ЕТС ГО, локальной сети СИ, устройств для организации удаленного доступа посредством беспроводных сетей, беспроводного доступа, модемов, радиомодемов, модемов сетей операторов сотовой связи, абонентских устройств сотовой связи и других беспроводных сетевых устройств, за исключением организованных оператором ИКИ ЭП беспроводных каналов связи ЕТС ГО, с использованием СКЗИ в соответствии с пунктом 48 настоящих ЕТ.»;

дополнить пунктом 131-1 следующего содержания:

«131-1. Необходимо осуществлять контроль подключения абонентских устройств сотовой связи, модемов сетей операторов сотовой связи, а также электронных носителей информации, не разрешенных политикой ИБ, принятой в ГО или МИО.»;

пункт 132 изложить в следующей редакции:

«132. Оператор ИКИ ЭП по заявкам СИ осуществляет:

распределение, регистрацию и перерегистрацию IP-адресов локальных сетей СИ, подключенных к ЕТС ГО, по заявкам СИ;

регистрацию доменных имен в доменных зонах Интернета gov.kz и мем.қаз по заявкам СИ;

регистрацию доменных имен в сети ЕТС ГО по заявкам СИ;

предоставление сервиса DNS в сети ЕТС ГО.»;

пункт 133 дополнить подпунктом 4) следующего содержания:

«4) направляют в государственную техническую службу, в случае производственной необходимости организации VPN-каналов, техническую информацию по требуемым VPN-каналам (IP-адреса источника и назначения, порты, протокол), согласованную с уполномоченным органом в сфере обеспечения информационной безопасности.»;

дополнить пунктом 133-1 следующего содержания:

«133-1. Не допускаются установка и применение на объектах информатизации, размещенных в ЛС внешнего контура ГО или МИО, программных или технических средств для удаленного управления ими извне ЛС внешнего контура ГО или МИО.»;

пункт 134 исключить;

дополнить пунктами 134-1 и 134-2 следующего содержания:

«134-1. Государственная техническая служба применяет на оборудовании ЕШДИ политику блокировки следующих категорий ИР и ПО (по умолчанию):

- VPN;
- удаленный доступ;
- p2p;
- игровые ресурсы;
- неизвестные приложения, не входящие по умолчанию в перечень категорий ИР и ПО;
- вредоносные ИР и ПО.

134-2. Возможность разблокировки отдельных категорий ИР и ПО, указанных в пункте 134-1, рассматривается государственной технической службой на основании официального запроса, поступившего от ГО, МИО, государственных организаций, субъектов квазигосударственного сектора, а также владельцев критически важных объектов ИКИ.»;

пункт 139 изложить в следующей редакции:

«139. Для обеспечения ИБ:

1) неиспользуемые порты кабельной системы локальной сети физически отключаются от активного оборудования;

2) разрабатывается и утверждается ТД ИБ, включающая правила:

использования сетей и сетевых услуг;

подключения к международным (территориальным) сетям передачи данных;

подключения к Интернету и (или) сетям телекоммуникаций, сетям связи, имеющим выход в международные (территориальные) сети передачи данных;

использования беспроводного доступа к сетевым ресурсам;

3) служебная информация ограниченного распространения, информация конфиденциальных ИС, конфиденциальных ЭИР и ЭИР, содержащих персональные данные ограниченного доступа, не передается по незащищенным

проводным каналам связи и радиоканалам, не оборудованным соответствующими СКЗИ.

Передача служебной информации ограниченного распространения производится с соблюдением специальных требований по защите информации ограниченного распространения в соответствии с Правилами отнесения сведений к служебной информации ограниченного распространения и работы с ней, установленными Правительством Республики Казахстан.

4) применяются средства:

идентификации, аутентификации и управления доступом пользователей;

идентификации оборудования;

защиты диагностических и конфигурационных портов;

физического сегментирования локальной сети;

логического сегментирования локальной сети;

управления сетевыми соединениями;

межсетевого экранирования;

сокрытия внутреннего адресного пространства локальной сети;

контроля целостности данных, сообщений и конфигураций;

криптографической защиты информации в соответствии с пунктом 48 настоящих ЕТ;

физической защиты каналов передачи данных и сетевого оборудования;

регистрации событий ИБ;

мониторинга и анализа сетевого трафика;

управления сетью;

5) осуществляется взаимодействие локальных сетей ГО, а также МИО между собой только через ЕТС ГО, за исключением сетей телекоммуникаций специального назначения и/или правительственной, засекреченной, шифрованной и кодированной связи;

6) осуществляется взаимодействие локальных сетей центрального исполнительного государственного органа и его территориальных подразделений между собой только через ЕТС ГО, за исключением сетей телекоммуникаций специального назначения и/или правительственной, засекреченной, шифрованной и кодированной связи;

7) исключаются сопряжения ЛС внутреннего контура и ЛС внешнего контура СИ между собой, за исключением организованных каналов связи с использованием СКЗИ, в соответствии с пунктом 48 настоящих ЕТ для учреждений Республики Казахстан, находящихся за границей;

8) исключается подключение ЛС внутреннего контура СИ к Интернету;

9) осуществляется соединение ЛС внешнего контура СИ с Интернетом только через ЕШДИ. Подключение к Интернету иным способом не допускается, за исключением специальных и правоохранительных ГО в оперативных целях. Взаимодействие ВШЭП с Интернетом осуществляется через ЕШДИ.

10) размещаются ИС СИ, реализующие информационное взаимодействие через Интернет, в выделенном сегменте ЛС внешнего контура СИ, и

осуществляется взаимодействие с ИС СИ, размещенными в ЛС внутреннего контура СИ, через ВШЭП;

11) осуществляется информационное взаимодействие ИС, размещенных в Интернете, с ИС СИ, размещенными в ЛС внутреннего контура СИ, только через ВШЭП;

12) сервера инфраструктуры источника времени верхнего уровня синхронизируются с эталоном времени и частоты, воспроизводящим национальную шкалу всемирного координированного времени UTC(kz).

Сервера инфраструктуры точного времени синхронизируются с сервером инфраструктуры точного времени верхнего уровня.

Сервера инфраструктуры точного времени предоставляют доступ клиентам для синхронизации времени.

13) отключаются открытые неиспользуемые сетевые порты.».

5. В постановлении Правительства Республики Казахстан от 12 июля 2019 года № 501 «О мерах по реализации Указа Президента Республики Казахстан от 17 июня 2019 года № 24 «О мерах по дальнейшему совершенствованию системы государственного управления Республики Казахстан» (САПП Республики Казахстан, 2019 г., № 29 ст. 248):

в Положении о Министерстве цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан, утвержденном указанным постановлением:

пункт 1 изложить в следующей редакции:

«1. Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан (далее – Министерство) является государственным органом Республики Казахстан, осуществляющим руководство в сферах аэрокосмической и электронной промышленности, в области инновационной деятельности, научно-технического развития страны, геодезии и картографии, обеспечения информационной безопасности в сфере информатизации, в сфере персональных данных и их защиты, руководство в области связи, информатизации, «электронного правительства», развития государственной политики в сфере оказания государственных услуг (далее – регулируемые сферы).»;

пункт 14 изложить в следующей редакции:

«14. Миссия Министерства:

формирование и проведение эффективной государственной политики в регулируемых сферах, а также развитие конкурентоспособной аэрокосмической промышленности, отрасли геодезии и картографии, обеспечение информационной безопасности в сфере информатизации, в сфере персональных данных и их защиты, формирование и обеспечение развития информационно-коммуникационной инфраструктуры, инновационной деятельности, научно-технического развития страны, эффективное функционирование рынка услуг связи.»;

в пункте 15:

подпункт 1) изложить в следующей редакции:

«1) формирование и проведение эффективной государственной политики в регулируемых сферах, а также развитие конкурентоспособной аэрокосмической промышленности и обеспечение информационной безопасности в сфере информатизации, реализации государственной политики в сфере персональных данных и их защиты, формирование и обеспечение развития информационно-коммуникационной инфраструктуры, отрасли геодезии и картографии, в сфере государственной поддержки инновационной деятельности, развития местного содержания в сфере инновационной деятельности, научно-технического развития страны, эффективное функционирование рынка услуг связи;»;

дополнить подпунктами 18-1) и 18-2) следующего содержания:

«18-1) участие в реализации государственной политики в сфере персональных данных и их защиты;

18-2) участие в формировании и реализации государственной политики в сфере государственной поддержки инновационной деятельности;»;

в пункте 16:

в подпункте 1):

абзацы сорок третий, сорок восьмой, пятидесятый, сто тридцать пятый, сто тридцать шестой, сто тридцать девятый изложить в следующей редакции:

«утверждение правил проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры по согласованию с Комитетом национальной безопасности Республики Казахстан;»;

«утверждение правил функционирования единой национальной резервной платформы хранения электронных информационных ресурсов, периодичность резервного копирования электронных информационных ресурсов критически важных объектов информационно-коммуникационной инфраструктуры;»;

«утверждение правил по подтверждению соответствия информационных систем, технических, программно-технических и программных средств (изделий), технических средств защиты информации требованиям информационной безопасности;»;

«утверждение перечня объектов информационно-коммуникационной инфраструктуры «электронного правительства», закрепляемых за оператором информационно-коммуникационной инфраструктуры «электронного правительства»;

«утверждение правил формирования перечня объектов информационно-коммуникационной инфраструктуры «электронного правительства», закрепляемых за оператором;»;

«утверждение правил интеграции объектов информатизации «электронного правительства» по согласованию с уполномоченным органом в сфере обеспечения информационной безопасности и Комитетом национальной безопасности Республики Казахстан;»;

после абзаца двести сорок восьмого дополнить абзацами двести сорок девятым – двести семьдесят пятым следующего содержания:

«утверждение правил по сбору, обработке, хранению, передаче электронных информационных ресурсов для осуществления аналитики данных в целях реализации функций государственными органами по согласованию с уполномоченным органом в сфере защиты персональных данных;

обеспечение реализации государственной политики в сфере электронной промышленности;

обеспечение реализации проектов и программ в области электронной промышленности, включая проведение научно-исследовательских и опытно-конструкторских работ;

разработка и утверждение правил осуществления отраслевой экспертизы в сфере электронной промышленности;

осуществление отраслевой экспертизы проектов в сфере электронной промышленности;

осуществление международного сотрудничества в сфере электронной промышленности и представление интересов Республики Казахстан в международных организациях и иностранных государствах;

разработка и утверждение правил формирования и ведения реестра доверенного программного обеспечения и продукции электронной промышленности, а также критериев по включению программного обеспечения и продукции электронной промышленности в реестр доверенного программного обеспечения и продукции электронной промышленности;

утверждение требований к унифицированному рабочему месту или терминальной системе государственных органов и местных исполнительных органов, а также требований по унификации компонентов объектов информационно-коммуникационной инфраструктуры;

утверждение совместно с уполномоченным органом в области углеводородов и добычи урана правил финансирования проектов цифровизации в области углеводородов и добычи урана в размере одного процента от затрат на добычу, понесенных недропользователем в период добычи углеводородов и урана по итогам предыдущего года;

заключение с национальными управляющими холдингами, национальными холдингами, национальными компаниями и аффилированными с ними юридическими лицами технологических меморандумов и определение перечня закупаемых товаров, работ и услуг;

реализация государственной политики в области коммерциализации результатов научной и (или) научно-технической деятельности в соответствующей отрасли;

утверждение отчетов по выполненным программам содействия коммерциализации результатов научной и (или) научно-технической деятельности в соответствующей отрасли, финансируемым за счет бюджетных средств;

представление информации о реализации мер по коммерциализации результатов научной и (или) научно-технической деятельности в соответствующей отрасли в уполномоченный орган;

методологическое обеспечение коммерциализации результатов научной и (или) научно-технической деятельности в соответствующей отрасли;

планирование, реализация мер по стимулированию коммерциализации результатов научной и (или) научно-технической деятельности в соответствующей отрасли;

участие в реализации программы по подготовке, переподготовке кадров и повышению квалификации в области коммерциализации результатов научной и (или) научно-технической деятельности в соответствующей отрасли;

осуществление мониторинга реализации программ содействия коммерциализации результатов научной и (или) научно-технической деятельности в соответствующей отрасли;

участие в разработке порядка финансирования проектов коммерциализации результатов научной и (или) научно-технической деятельности в соответствующей отрасли;

участие в разработке порядка организации и проведения экспертизы проектов коммерциализации результатов научной и (или) научно-технической деятельности в соответствующей отрасли;

утверждение правил формирования, проверки и использования электронных документов с применением сервиса цифровых документов;

утверждение правил сбора, обработки и хранения биометрических данных физических лиц для биометрической аутентификации при оказании государственных услуг по согласованию с уполномоченным органом в сфере защиты персональных данных;

утверждение правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре по согласованию с уполномоченным органом в сфере обеспечения информационной безопасности;

определение порядка информирования о деятельности по осуществлению цифрового майнинга;

утверждение порядка выпуска и оборота обеспеченных цифровых активов;

утверждение правил функционирования единого шлюза доступа к Интернету и единого шлюза электронной почты «электронного правительства» по согласованию с Комитетом национальной безопасности Республики Казахстан;

утверждение правил сбора, обработки персональных данных;

утверждение совместно с органами внутренних дел, уполномоченными органами в области здравоохранения, социальной защиты населения и уполномоченным государственным органом по труду типового положения о единой дежурно-диспетчерской службе «112», а также правил координации деятельности единой дежурно-диспетчерской службы «112» и дежурных диспетчерских служб на территории Республики Казахстан;»;

в подпункте 2):

абзацы сорок седьмой, пятьдесят второй, сто двадцать восьмой и сто двадцать девятый изложить в следующей редакции:

«разработка правил проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры по согласованию с Комитетом национальной безопасности Республики Казахстан;»;

«разработка правил функционирования единой национальной резервной платформы хранения электронных информационных ресурсов, периодичность резервного копирования электронных информационных ресурсов критически важных объектов информационно-коммуникационной инфраструктуры;»;

«разработка правил формирования перечня объектов информационно-коммуникационной инфраструктуры «электронного правительства», закрепляемых за оператором информационно-коммуникационной инфраструктуры «электронного правительства»;

разработка правил интеграции объектов информатизации «электронного правительства» по согласованию с уполномоченным органом в сфере обеспечения информационной безопасности и Комитетом национальной безопасности Республики Казахстан;»;

после абзаца сто шестьдесят восьмого дополнить абзацами сто шестьдесят девятым – сто восьмидесятым следующего содержания:

«разработка правил формирования, проверки и использования электронных документов с применением сервиса цифровых документов;

разработка правил создания, использования и хранения закрытых ключей электронной цифровой подписи в удостоверяющем центре по согласованию с уполномоченным органом в сфере обеспечения информационной безопасности;

разработка правил по подтверждению соответствия информационных систем, технических, программно-технических и программных средств (изделий), технических средств защиты информации требованиям информационной безопасности;

разработка порядка выпуска и оборота обеспеченных цифровых активов;

разработка правил функционирования единого шлюза доступа к Интернету и единого шлюза электронной почты «электронного правительства» по согласованию с Комитетом национальной безопасности Республики Казахстан;

разработка порядка осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных;

рассмотрение обращений субъекта персональных данных о соответствии содержания персональных данных и способов их обработки целям их обработки и принятие соответствующего решения;

принятие мер по привлечению лиц, допустивших нарушения законодательства Республики Казахстан о персональных данных и их защите, к ответственности, установленной законами Республики Казахстан;

требование от собственника и (или) оператора, а также третьего лица уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

осуществление мер, направленных на совершенствование защиты прав субъектов;

разработка правил сбора, обработки персональных данных;

осуществление государственного контроля за соблюдением законодательства Республики Казахстан об электронном документе и электронной цифровой подписи;».

Приложение 1
к изменениям и дополнениям,
которые вносятся
в некоторые решения
Правительства Республики
Казахстан

Утверждены
постановлением Правительства
Республики Казахстан
от 3 сентября 2013 года
№ 909

Правила
осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных

Глава 1. Общие положения

1. Настоящие Правила осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных (далее – Правила) разработаны в соответствии с подпунктом 4) статьи 26 Закона Республики Казахстан от 21 мая 2013 года «О персональных данных и их защите» (далее – Закон) и определяют порядок осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных.

2. В настоящих Правилах используются следующие основные понятия:

1) персональные данные – сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе;

2) блокирование персональных данных – действия по временному прекращению сбора, накопления, изменения, дополнения, использования, распространения, обезличивания и уничтожения персональных данных;

3) сбор персональных данных – действия, направленные на получение персональных данных;

4) уничтожение персональных данных – действия, в результате совершения которых невозможно восстановить персональные данные;

5) обезличивание персональных данных – действия, в результате совершения которых определение принадлежности персональных данных субъекту персональных данных невозможно;

6) база, содержащая персональные данные (далее – база), – совокупность упорядоченных персональных данных;

7) собственник базы, содержащей персональные данные (далее – собственник), – государственный орган, физическое и (или) юридическое лицо, реализующие в соответствии с законами Республики Казахстан право владения, пользования и распоряжения базой, содержащей персональные данные;

8) оператор базы, содержащей персональные данные (далее – оператор), – государственный орган, физическое и (или) юридическое лицо, осуществляющие сбор, обработку и защиту персональных данных;

9) защита персональных данных – комплекс мер, в том числе правовых, организационных и технических, осуществляемых в целях, установленных Законом;

10) уполномоченный орган в сфере защиты персональных данных – центральный исполнительный орган, осуществляющий руководство в сфере защиты персональных данных;

11) обработка персональных данных – действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных;

12) субъект персональных данных (далее – субъект) – физическое лицо, к которому относятся персональные данные;

13) общедоступные персональные данные – персональные данные или сведения, на которые в соответствии с законодательством Республики Казахстан не распространяются требования соблюдения конфиденциальности, доступ к которым является свободным с согласия субъекта;

14) персональные данные ограниченного доступа – персональные данные, доступ к которым ограничен законодательством Республики Казахстан;

15) третье лицо – лицо, не являющееся субъектом, собственником и (или) оператором, но связанное с ними (ним) обстоятельствами или правоотношениями по сбору, обработке и защите персональных данных;

16) электронные информационные ресурсы – информация в электронно-цифровой форме, содержащаяся на электронном носителе и в объектах информатизации.

Иные понятия, используемые в настоящих Правилах, применяются в соответствии с Законом и Законом Республики Казахстан от 24 ноября 2015 года «Об информатизации».

Глава 2. Порядок осуществления собственником и (или) оператором, а также третьим лицом мер по защите персональных данных

3. Собственник и (или) оператор, а также третье лицо обязаны принимать необходимые меры по защите персональных данных, обеспечивающие:

1) предотвращение несанкционированного доступа к персональным данным;

2) своевременное обнаружение фактов несанкционированного доступа к персональным данным, если такой несанкционированный доступ не удалось предотвратить;

3) минимизацию неблагоприятных последствий несанкционированного доступа к персональным данным.

4. Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих возможность несанкционированного, в том числе случайного, доступа к персональным данным при их сборе и обработке, результатом которого могут стать уничтожение, изменение, блокирование, копирование, несанкционированное предоставление третьим лицам, несанкционированное распространение персональных данных, а также иные неправомерные действия.

5. Защита персональных данных осуществляется путем применения комплекса мер, в том числе правовых, организационных и технических, в целях:

1) реализации прав на неприкосновенность частной жизни, личную и семейную тайну;

2) обеспечения их целостности и сохранности;

3) соблюдения их конфиденциальности;

4) реализации права на доступ к ним;

5) предотвращения незаконного их сбора и обработки.

6. Обязанности собственника и (или) оператора, а также третьего лица по защите персональных данных возникают с момента сбора персональных данных и действуют до момента их уничтожения либо обезличивания.

7. Для обеспечения защиты персональных данных необходимо:

1) выделение бизнес-процессов, содержащих персональные данные;

2) разделение персональных данных на общедоступные и ограниченного доступа;

3) определение перечня лиц, осуществляющих сбор и обработку персональных данных либо имеющих к ним доступ;

4) назначение лица, ответственного за организацию обработки персональных данных в случае, если собственник и (или) оператор являются юридическими лицами. Обязанности лица, ответственного за организацию обработки персональных данных, указаны в пункте 3 статьи 25 Закона. Действие подпункта 4) настоящего пункта не распространяется на обработку персональных данных в деятельности судов.

5) установление порядка доступа к персональным данным.

При сборе и обработке персональных данных в объектах информатизации дополнительно необходимо обеспечение сохранности носителей персональных данных.

8. Иные особенности защиты персональных данных при их сборе и обработке в объектах информатизации устанавливаются в соответствии с законодательством Республики Казахстан об информатизации.

9. Собственник и (или) оператор при обработке персональных данных ограниченного доступа:

1) устанавливают цели обработки персональных данных ограниченного доступа. Персональные данные ограниченного доступа используются в соответствии с декларируемыми целями.

2) определяют порядок обработки, распространения и доступа к персональным данным ограниченного доступа;

3) определяют порядок блокирования персональных данных ограниченного доступа, относящихся к субъекту, при обращении субъекта.

Собственник и (или) оператор, а также третье лицо при обработке персональных данных ограниченного доступа:

1) определяют перечень лиц, имеющих доступ к персональным данным ограниченного доступа;

2) оповещают уполномоченный орган в сфере защиты персональных данных об инцидентах информационной безопасности, связанных с незаконным доступом к персональным данным ограниченного доступа;

3) обеспечивают установку средств защиты информации, обновлений программного обеспечения на технических средствах, осуществляющих обработку персональных данных ограниченного доступа;

4) обеспечивают ведение журнала событий систем управления базами;

5) обеспечивают ведение журнала действий пользователей, имеющих доступ к персональным данным ограниченного доступа;

6) применяют средства контроля целостности персональных данных ограниченного доступа;

7) обеспечивают передачу персональных данных ограниченного доступа иным лицам по защищенным каналам связи и (или) с применением шифрования и при наличии согласия субъекта персональных данных, если иное не предусмотрено законодательством Республики Казахстан;

8) выделяют бизнес-процессы, содержащие персональные данные ограниченного доступа;

9) обеспечивают применение средств криптографической защиты информации для надежного хранения персональных данных ограниченного доступа;

10) применяют средства идентификации и (или) аутентификации пользователей при работе с персональными данными ограниченного доступа.

10. Сбор и обработка персональных данных ограниченного доступа осуществляются посредством объектов информатизации, размещенных на территории Республики Казахстан.

Хранение и передача персональных данных ограниченного доступа осуществляются с использованием средств криптографической защиты информации, имеющих параметры не ниже третьего уровня безопасности согласно стандарту Республики Казахстан СТ РК 1073-2007 «Средства криптографической защиты информации. Общие технические требования».

Требования данного пункта не распространяются на случаи трансграничной передачи данных.

_____

Приложение 2
к изменениям и дополнениям,
которые вносятся
в некоторые решения
Правительства Республики
Казахстан

Утверждены
постановлением Правительства
Республики Казахстан
от 12 ноября 2013 года
№ 1214

Правила
определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач

Глава 1. Общие положения

1. Настоящие Правила определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач (далее – Правила), разработаны в соответствии с подпунктом 3) статьи 26 Закона Республики Казахстан от 21 мая 2013 года
«О персональных данных и их защите» (далее – Закон) и определяют порядок определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач.

2. В настоящих Правилах используются следующие основные понятия:

1) персональные данные – сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе;

2) сбор персональных данных – действия, направленные на получение персональных данных;

3) собственник базы, содержащей персональные данные (далее – собственник), – государственный орган, физическое и (или) юридическое лицо, реализующие в соответствии с законами Республики Казахстан право владения, пользования и распоряжения базой, содержащей персональные данные;

4) оператор базы, содержащей персональные данные (далее – оператор), – государственный орган, физическое и (или) юридическое лицо, осуществляющие сбор, обработку и защиту персональных данных;

5) уполномоченный орган в сфере защиты персональных данных (далее – уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство в сфере защиты персональных данных;

6) обработка персональных данных – действия, направленные на накопление, хранение, изменение, дополнение, использование, распространение, обезличивание, блокирование и уничтожение персональных данных;

7) субъект персональных данных – физическое лицо, к которому относятся персональные данные.

Глава 2. Порядок определения собственником и (или) оператором перечня персональных данных, необходимого и достаточного для выполнения осуществляемых ими задач

3. Собственник и (или) оператор до начала сбора и обработки персональных данных проводят анализ осуществляемых ими задач на предмет использования персональных данных.

При осуществлении текущей деятельности собственник и (или) оператор ежегодно проводят повторный анализ осуществляемых ими задач на предмет использования персональных данных, на основании которого вносятся изменения в перечень персональных данных, необходимый и достаточный для выполнения осуществляемых ими задач, в соответствии с пунктом 6 настоящих Правил.

4. На основании проведенного анализа собственник и (или) оператор по форме, согласно приложению к настоящим Правилам, определяют перечень персональных данных, необходимый и достаточный для выполнения осуществляемых ими задач с указанием целей их сбора и обработки в рамках задач.

Цели являются однозначными, законными и соответствуют осуществляемым собственником и (или) оператором задачам.

Персональные данные, содержание и объем которых являются избыточными по отношению к осуществляемым собственником и (или) оператором задач, не включаются в перечень персональных данных, необходимый и достаточный для выполнения осуществляемых ими задач.

5. Перечень персональных данных, необходимый и достаточный для выполнения осуществляемых ими задач, утверждается собственником и (или) оператором.

Защита персональных данных осуществляется в соответствии с Правилами осуществления собственником и (или) оператором, а также третьим

лицом мер по защите персональных данных, утверждаемых Правительством Республики Казахстан.

6. По результатам текущей деятельности собственником (или) оператором ежегодно вносятся изменения и дополнения в перечень персональных данных, необходимых и достаточных для выполнения осуществляемых ими задач,
в порядке, предусмотренном пунктами 3, 4 и 5 настоящих Правил.

Изменения и дополнения, внесенные в перечень персональных данных, необходимый и достаточный для выполнения осуществляемых ими задач, действуют с момента их утверждения и не распространяются на отношения, возникшие до их введения в действие.

7. Собственник и (или) оператор обеспечивают доступ к перечню персональных данных, необходимому и достаточному для выполнения осуществляемых ими задач, способами, не запрещенными законодательством Республики Казахстан.

Приложение
к Правилам определения собственником
и (или) оператором перечня
персональных данных, необходимого и
достаточного для выполнения
осуществляемых ими задач

Перечень
персональных данных, необходимый и достаточный
для выполнения осуществляемых задач

№ п/п	Наименование задачи, в том числе функций, полномочий, обязанностей	Цели сбора и обработки в рамках осуществляемой задачи	Наименование персональных данных для определённой цели	Указание на документы или нормативные правовые акты, имеющие прямые указания на осуществляемые собственником и (или) оператором задачи

_____