Қазақстан Республикасының Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 27 октября 2022 года № 399/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 31 октября 2022 года № 30354

Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан

О внесении изменений и дополнения в некоторые приказы

ПРИКАЗЫВАЮ:

1. Утвердить прилагаемый перечень некоторых приказов, в которые вносятся изменения и дополнение.

2. Комитету по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан обеспечить:

1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;

2) размещение настоящего приказа на интернет-ресурсе Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан после его официального опубликования;

3) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

4. Настоящий приказ вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования.

Министр цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан **Б. Мусин**

«СОГЛАСОВАН»
Комитет национальной безопасности
Республики Казахстан

Утвержден приказом
Министр цифрового развития,
инноваций и
аэрокосмической
промышленности
Республики Казахстан
от 27 октября 2022 года
№ 399/НҚ

Перечень некоторых приказов, в которые вносятся изменения и дополнение

1. Внести в приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 16 марта 2018 года № 45/НҚ «Об утверждении Правил передачи резервных копий электронных информационных ресурсов на единую платформу резервного хранения электронных информационных ресурсов» (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 16883) следующие изменения:

заголовок изложить в следующей редакции:

«Об утверждении Правил передачи резервных копий электронных информационных ресурсов на единую национальную резервную платформу хранения электронных информационных ресурсов»;

преамбулу изложить в следующей редакции:

«В соответствии с подпунктом 4) пункта 2-1 статьи 17 Закона Республики Казахстан «Об информатизации» **ПРИКАЗЫВАЮ**:»;

пункт 1 изложить в следующей редакции:

«1. Утвердить прилагаемые Правила передачи резервных копий электронных информационных ресурсов на единую национальную резервную платформу хранения электронных информационных ресурсов.»;

в Правилах передачи резервных копий электронных информационных ресурсов на единую платформу резервного хранения электронных информационных ресурсов, утвержденных указанным приказом:

заголовок изложить в следующей редакции:

«Правила передачи резервных копий электронных информационных ресурсов на единую национальную резервную платформу хранения электронных информационных ресурсов»;

пункт 1 изложить в следующей редакции:

«1. Настоящие Правила передачи резервных копий электронных информационных ресурсов на единую национальную резервную платформу хранения электронных информационных ресурсов (далее – Правила) разработаны на основании подпункта 4) пункта 2-1 статьи 17 Закона Республики Казахстан «Об информатизации» (далее – Закон) и определяют порядок и сроки передачи резервных копий электронных информационных ресурсов на единую национальную резервную платформу хранения электронных информационных ресурсов.»;

пункт 2 изложить в новой редакции:

«2. В настоящих Правилах используются следующие основные понятия:

1) уполномоченный орган в сфере обеспечения информационной безопасности (далее – уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство и межотраслевую координацию в сфере обеспечения информационной безопасности;

2) критически важные объекты информационно-коммуникационной инфраструктуры (далее - КВОИКИ) – объекты информационно-коммуникационной инфраструктуры, нарушение или прекращение функционирования которых приводит к незаконному сбору и обработке персональных данных ограниченного доступа и иных сведений, содержащих охраняемую законом тайну, чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства или для 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»;

3) горячее резервирование – использование дополнительных программных и технических средств и поддержание их в активном режиме, и (или) обеспечение передачи изменений в режиме реального времени (либо приближенного к реальному времени с задержкой не более 1 часа), и сохранности информации;

4) государственная техническая служба (далее – АО «ГТС») - акционерное общество, созданное по решению Правительства Республика Казахстан;

5) резервная копия – результат успешно завершенного процесса создания копии базы данных и при необходимости прикладного программного обеспечения на электронном носителе, предназначенной для восстановления базы данных и при необходимости прикладного программного обеспечения в исходном виде в случае их потери, повреждения, разрушения или неправомерного изменения и удаления;

6) долгосрочное хранение – разовая передача резервных копий электронных информационных ресурсов на единую национальную резервную платформу хранения электронных информационных ресурсов со сроком хранения более двух лет;

7) холодное резервирование – создание резервной копии средствами операционной системы с рабочего либо выключенного электронного информационного ресурса с целью обеспечения возможности восстановления данных;

8) единая национальная резервная платформа хранения электронных информационных ресурсов (далее – ЕНРП) – аппаратно-программный комплекс, предназначенный для хранения резервных копий электронных информационных ресурсов, в целях обеспечения их сохранности и восстановления данных в случае необходимости.»;

пункт 3 исключить;

заголовок главы 2 изложить в следующей редакции:

«Глава 2. Порядок передачи резервных копий электронных информационных ресурсов на единую национальную резервную платформу хранения электронных информационных ресурсов»;

пункт 5 изложить в следующей редакции:

«5. АО «ГТС» направляет информацию владельцам КВОИКИ о необходимости передачи резервных копий ЭИР на ЕНРП.»;

абзац первый пункта 6 изложить в следующей редакции:

«6. Владельцы КВОИКИ не позднее 15 (пятнадцати) рабочих дней с момента получения информации от АО «ГТС», направляют в АО «ГТС» по каждому ЭИР:»;

пункт 7 изложить в следующей редакции:

«7. На основании Перечня КВОИКИ (далее – Перечень), утверждаемого согласно подпункту 4) статьи 6 Закона и полученной от каждого владельца КВОИКИ информации, АО «ГТС», по согласованию с уполномоченным органом, устанавливает периодичность резервного копирования ЭИР для передачи на ЕНРП.»;

абзац первый пункта 8 изложить в следующей редакции:

«8. АО «ГТС» в течение 20 (двадцати) рабочих дней официально, в письменном виде, направляет владельцам КВОИКИ для ознакомления и исполнения, следующие сведения:»;

пункт 10 изложить в следующей редакции:

«10. Владельцы КВОИКИ за счет собственных средств организуют самостоятельную передачу на ЕНРП (в АО «ГТС») резервных копий ЭИР (в том числе, копии документации к ЭИР, инструкции, конфигурационные файлы и так далее) в объеме достаточном для восстановления КВОИКИ из хранящихся на ЕНРП резервных копий, с учетом случаев потери (разрушении) всей инфраструктуры владельцев КВОИКИ. Передача резервных копий КВОИКИ осуществляется в течение 20 (двадцати) рабочих дней со дня получения информации от АО «ГТС», кроме случаев временной отсрочки приема резервных копий на ЕНРП.»;

пункт 11 изложить в следующей редакции:

«11. В случае передачи резервной копии в шифрованном виде, ключи шифрования, средства, которыми производилось шифрование и средства для расшифрования, подлежат передаче в АО «ГТС» на электронном носителе для возможности восстановления в случае потери всей инфраструктуры на стороне владельцев ЭИР.»;

абзац первый пункта 13 изложить в следующей редакции:

«13. АО «ГТС» осуществляет временную отсрочку приема резервных копий ЭИР в следующих случаях:»;

пункт 14 изложить в следующей редакции:

«14. Основанием для временной отсрочки приема резервных копий ЭИР служит направленная АО «ГТС» информация в уполномоченный орган и владельцу КВОИКИ о необходимости приостановить процесс передачи резервных копий ЭИР с указанием причины. Срок отсрочки приема резервных копий ЭИР устанавливается до устранения обстоятельств, указанных в пункте 13 настоящих Правил, по согласованию с уполномоченным органом.»;

заголовок главы 3 изложить в следующей редакции:

«Глава 3. Сроки передачи резервных копий электронных информационных ресурсов на единую национальную резервную платформу хранения электронных информационных ресурсов»;

пункт 16 изложить в следующей редакции:

«16. В случае исключения ЭИР из Перечня, владелец КВОИКИ прекращает передачу резервных копий ЭИР на ЕНРП в течение 24 часов со дня получения информации от АО «ГТС».»;

приложение к настоящим Правилам изложить в новой редакции согласно приложению 1 к настоящему Перечню.

2. Внести в приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ «Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры» (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 17019) следующие изменения и дополнение:

преамбулу изложить в следующей редакции:

«В соответствии с подпунктом 7) статьи 7-1 Закона Республики Казахстан «Об информатизации» **ПРИКАЗЫВАЮ**:»;

в Правилах проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры, утвержденных указанным приказом:

пункт 1 изложить в следующей редакции:

«1. Настоящие Правила проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры (далее – Правила) разработаны в соответствии с подпунктом 7) статьи 7-1 Закона Республики Казахстан «Об информатизации» (далее – Закон) и определяют порядок проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры.»;

пункт 2 изложить в новой редакции:

2. В настоящих Правилах используются следующие понятия и сокращения:

1) объекты информатизации – электронные информационные ресурсы, программное обеспечение, интернет-ресурс и информационно-коммуникационная инфраструктура;

2) владелец объектов информатизации – субъект, которому собственник объектов информатизации предоставил права владения и пользования объектами информатизации в определенных законом или соглашением пределах и порядке;

3) уязвимость объекта информатизации – недостаток в программном или аппаратном обеспечении, обуславливающий возможность нарушения его работоспособности, либо выполнения каких-либо несанкционированных действий в обход разрешений, установленных в программном или аппаратном обеспечении;

4) техническая документация по информационной безопасности – документация, устанавливающая политику, правила, защитные меры, касающиеся процессов обеспечения информационной безопасности (далее – ИБ) объектов информатизации и (или) организации;

5) система управления событиями информационной безопасности – программное обеспечение или аппаратно-программный комплекс, предназначенные для автоматизированного выявления событий информационной безопасности и инцидентов информационной безопасности путем сбора и анализа журналов регистрации событий объекта информатизации;

6) агент системы управления событиями информационной безопасности – программное обеспечение, устанавливаемое на серверное оборудование объекта информатизации для сбора журналов регистрации событий;

7) событие информационной безопасности – состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объекта информатизации;

8) уполномоченный орган в сфере обеспечения информационной безопасности (далее – уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство и межотраслевую координацию в сфере обеспечения информационной безопасности;

9) система мониторинга обеспечения информационной безопасности – организационные и технические мероприятия, направленные на проведение мониторинга безопасного использования информационно-коммуникационных технологий;

10) оперативный центр информационной безопасности (далее – ОЦИБ) – юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации;

11) инцидент информационной безопасности – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов;

12) государственная техническая служба (далее – АО «ГТС») - акционерное общество, созданное по решению Правительства Республики Казахстан;

13) критически важные объекты информационно-коммуникационной инфраструктуры – объекты информационно-коммуникационной инфраструктуры, нарушение или прекращение функционирования которых приводит к незаконному сбору и обработке персональных данных ограниченного доступа и иных сведений, содержащих охраняемую законом тайну, чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства или для 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»;

14) журналирование событий – процесс записи информации о происходящих с объектом информатизации программных или аппаратных событиях в журнал регистрации событий;

15) система сбора журналов регистрации событий – аппаратно-программный комплекс, обеспечивающий централизованный сбор журналов регистрации событий объектов информатизации, их хранение и дальнейшую передачу в систему управления событиями информационной безопасности;

16) объекты информатизации «электронного правительства» (далее – ОИ ЭП) – государственные электронные информационные ресурсы, программное обеспечение государственных органов, интернет - ресурс государственного органа, объекты информационно-коммуникационной инфраструктуры «электронного правительства», в том числе объекты информатизации иных лиц, предназначенные для формирования государственных электронных информационных ресурсов, осуществления государственных функций и оказания государственных услуг;

17) мониторинг обеспечения информационной безопасности объектов информатизации «электронного правительства» (далее – МОИБ) – отслеживание полноты и качества реализации собственниками и (или) владельцами объектов

информатизации «электронного правительства» технических и организационных мероприятий по обеспечению ИБ ОИ ЭП посредством выявления угроз и инцидентов ИБ;

18) архитектурный портал «электронного правительства» – объект информатизации, предназначенный для осуществления учета, хранения и систематизации сведений об объектах информатизации «электронного правительства», архитектуры «электронного правительства» в целях дальнейшего использования государственными органами для мониторинга, анализа и планирования в сфере информатизации.»;

абзац первый пункта 3 изложить в следующей редакции:

«3. МОИБ проводится АО «ГТС», реализующим задачи и функции Национального координационного центра информационной безопасности (далее – НКЦИБ), в соответствии с подпунктом 15) пункта 1 статьи 14 Закона, посредством системы МОИБ НКЦИБ и включает в себя следующие виды работ:»;

пункт 6 изложить в следующей редакции:

«6. МОИБ ОИ ЭП, отнесенных к КВОИКИ, осуществляется на основании договорных отношений между Комитетом национальной безопасности Республики Казахстан (далее – КНБ РК) и АО «ГТС».»;

абзац первый пункта 7 изложить в следующей редакции:

«7. АО «ГТС» для проведения МОИБ в качестве первичной информации использует сведения об объекте МОИБ из архитектурного портала «электронного правительства», а также сведения, полученные на этапах проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы «электронного правительства», интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности (далее - ИБ), включая:»;

пункт 8 изложить в следующей редакции:

«8. Собственник или владелец объекта МОИБ уведомляет официальным письмом АО «ГТС» о вводе в промышленную эксплуатацию, либо о прекращении эксплуатации объекта МОИБ в течение 10 рабочих дней со дня его ввода в

промышленную эксплуатацию, либо прекращения эксплуатации, и предоставляет в бумажном и электронном виде сведения об ОИ ЭП по форме, согласно приложению 1 настоящих Правил (далее – Сведения).»;

пункт 9 изложить в следующей редакции:

«9. АО «ГТС» разрабатывает график проведения работ по МОИБ и согласовывает его с КНБ РК.»;

пункт 10 изложить в следующей редакции:

«10. АО «ГТС» при проведении МОИБ осуществляет:

1) в рамках мониторинга реагирования на инциденты ИБ:

анализ объекта МОИБ на предмет определения перечня журналов регистрации событий, необходимых для передачи в систему управления событиями ИБ НКЦИБ;

установку агентов системы управления событиями ИБ на систему сбора журналов регистрации событий объекта МОИБ и, при необходимости, на иные объекты информационно-коммуникационной инфраструктуры собственника или владельца объекта МОИБ;

сбор журналов регистрации событий объекта МОИБ и относящихся к нему средств защиты информации, в системе управления событиями ИБ НКЦИБ, их обработку и анализ с целью выявления событий ИБ и инцидентов ИБ;

первичный анализ событий ИБ или инцидентов ИБ, выявленных на объекте МОИБ;

уведомление ответственных лиц за обеспечение ИБ объекта МОИБ с предоставлением перечня данных об инциденте ИБ, согласно приложению 2 настоящих Правил (далее – Перечень данных), в течение 30 минут с момента выявления события ИБ или инцидента ИБ;

выдачу первичных рекомендаций по приостановлению распространения инцидента ИБ собственнику или владельцу объекта МОИБ;

направление, при необходимости, к месту размещения объекта МОИБ работника АО «ГТС» в рамках реагирования на инцидент ИБ (необходимость определяется КНБ РК или АО «ГТС» самостоятельно);

уведомление КНБ РК о неустранении собственником или владельцем объекта МОИБ или уполномоченным им лицом причин и последствий инцидента ИБ по истечении 72 часов с момента выявления инцидента ИБ;

2) в рамках мониторинга обеспечения защиты:

обследование объектов МОИБ, в том числе локальной вычислительной сети (при ее наличии), имеющей сопряжение с локальной вычислительной сетью, в которой размещен объект МОИБ на предмет наличия уязвимостей (далее – обследование на уязвимости) согласно графику проведения работ по МОИБ:

в режиме «тестирование на проникновение» – 8 раз в год (4 основных, 4 контрольных);

в режиме «контроль обновлений и анализ конфигураций» – 2 раза в год (основное, контрольное);

анализ исходного кода – 4 раза в год (2 основных, 2 контрольных);

«ручное» тестирование на проникновение – 2 раза в год (основное, контрольное);

предоставление результатов обследования на уязвимости и рекомендаций по устранению уязвимостей объектов МОИБ собственникам или владельцам объектов МОИБ в течение 10 рабочих дней после завершения работ по обследованию на уязвимости;

консультирование собственников или владельцев объектов МОИБ по вопросам устранения уязвимостей объектов МОИБ, выявленных в рамках обследования на уязвимости;

3) в рамках мониторинга обеспечения безопасного функционирования:

обследование объекта МОИБ на предмет исполнения требований технической документации по информационной безопасности (далее – ТД по ИБ), приведенной в приложении 3 настоящих Правил, согласно графику проведения работ по МОИБ;

предоставление результатов обследования объекта МОИБ на предмет исполнения требований ТД по ИБ и рекомендаций по устранению выявленных нарушений ТД по ИБ собственникам или владельцам объектов МОИБ в течение 10 рабочих дней со дня завершения данного обследования.»;

пункт 11 изложить в следующей редакции:

«11. Собственник или владелец объекта МОИБ обеспечивает условия для проведения АО «ГТС» работ по МОИБ, включая:

физический доступ работникам АО «ГТС» к объекту МОИБ, к системе сбора журналов регистрации событий объекта МОИБ в сопровождении работников собственника или владельца объекта МОИБ или уполномоченного им лица;

два рабочих места для работников АО «ГТС» с предоставлением круглосуточного сетевого доступа к объекту МОИБ на безвозмездной основе;

сетевой доступ для АО «ГТС» к системе сбора журналов регистрации событий объекта МОИБ с правами на исполнение всех без исключения операций;

доступ к технической документации по информационной безопасности, утвержденной собственником или владельцем объекта МОИБ, заверенной его подписью и печатью (при наличии).»;

пункт 12 изложить в следующей редакции:

«12. При проведении АО «ГТС» мониторинга реагирования на инциденты ИБ собственник или владелец объекта МОИБ:

организует журналирование событий объекта МОИБ и относящихся к нему средств защиты информации, в соответствии с форматами и типами записей журналов регистрации событий ОИ ЭП, приведенными в приложении 4 настоящих Правил;

организует систему сбора журналов регистрации событий в контуре телекоммуникационной сети, в котором функционирует объект МОИБ;

организует передачу журналов регистрации событий объекта МОИБ и относящихся к нему средств защиты информации, в систему сбора журналов регистрации событий объекта МОИБ;

уведомляет АО «ГТС» о планируемых работах по внесению изменений в журналирование событий объекта МОИБ за 5 рабочих дней до внесения изменений. К уведомлению прикладываются образцы изменяемых журналов регистрации событий и их описание;

обеспечивает условия, согласованные с АО «ГТС», для передачи журналов регистрации событий объекта МОИБ из системы сбора журналов регистрации событий объекта МОИБ в систему управления событиями ИБ НКЦИБ;

уведомляет АО «ГТС» о самостоятельно выявленном инциденте ИБ на объекте МОИБ в течение 15 минут с момента выявления;

предоставляет в АО «ГТС» Перечень данных в течение 24 часов с момента обнаружения инцидента ИБ.»;

пункт 13 изложить в следующей редакции:

«13. При проведении АО «ГТС» мониторинга обеспечения защиты собственник или владелец объектов МОИБ:

направляет в АО «ГТС» информацию о мерах, принятых для устранения уязвимостей объекта МОИБ, в течение двадцати календарных дней со дня получения результатов обследования на наличие уязвимостей;

При самостоятельном обнаружении уязвимости объекта МОИБ, предоставляет в АО «ГТС» перечень данных об уязвимости ОИ ЭП по форме согласно приложению 5 настоящих Правил в течение 24 часов с момента выявления уязвимости объекта МОИБ;

При неустранении уязвимости объекта МОИБ может присвоить уязвимости одну из категорий (производственная необходимость, уязвимость нулевого дня, ложное срабатывание) и предоставляет в АО «ГТС» категории причин неустранения уязвимости и обоснование причины неустранения согласно приложению 6 настоящих Правил.»;

пункт 14 изложить в следующей редакции:

«14. При проведении АО «ГТС» мониторинга обеспечения безопасного функционирования собственник или владелец объекта МОИБ в течение одного месяца со дня получения результатов обследования объекта МОИБ на предмет исполнения требований ТД по ИБ предоставляет в АО «ГТС» информацию о мерах, принятых по выявленным нарушениям требований ТД по ИБ.»;

пункт 15 изложить в следующей редакции:

«15. С целью формирования перечня объектов МОИБ, АО «ГТС» направляет запрос собственникам или владельцам объектов МОИБ о

предоставлении Сведений. Собственник или владелец объекта МОИБ предоставляет в АО «ГТС» Сведения в электронной форме в течение 10 рабочих дней с момента получения запроса от АО «ГТС».»;

пункт 16 изложить в следующей редакции:

«16. При изменении контактных данных лица, ответственного за обеспечение ИБ объекта МОИБ, собственник или владелец объекта МОИБ в течение 48 часов с момента данного изменения направляет в АО «ГТС» актуальные контактные данные.»;

пункт 17 изложить в следующей редакции:

«17. АО «ГТС» ежеквартально направляет в КНБ РК сводную информацию по выявленным событиям ИБ, инцидентам ИБ, уязвимостям ОИ ЭП, изменениям ОИ ЭП и выявленным нарушениям требований ТД по ИБ, а также сведения о принятых собственниками или владельцами объектов МОИБ мерах.»;

заголовок главы 3 изложить в следующей редакции:

«Глава 3. Порядок проведения мониторинга обеспечения информационной безопасности критически важных объектов информационно-коммуникационной инфраструктуры»;

пункт 19 изложить в следующей редакции:

«19. МОИБ объектов информатизации КВОИКИ осуществляется собственным подразделением по ИБ владельца КВОИКИ или путем приобретения услуг третьих лиц в соответствии со статьей 683 Гражданского кодекса Республики Казахстан.»;

пункт 21 изложить в следующей редакции:

«21. Подключение СМО ИБ КВОИКИ к техническим средствам ОЦИБ осуществляется подразделением по ИБ собственника или владельца КВОИКИ или приобретением услуг третьих лиц в соответствии со статьей 683 Гражданского кодекса Республики Казахстан.»;

пункт 24 изложить в следующей редакции:

«24. В случае самостоятельного выявления инцидента ИБ подразделением по ИБ КВОИКИ, ответственный по ИБ КВОИКИ оповещает АО «ГТС» и ОЦИБ путем направления Перечня данных в течение 24 часов с момента выявления инцидента ИБ.»;

дополнить пунктом 25 следующего содержания:

«Порядок и требования, изложенные в настоящей главе, установлены для КВОИКИ, не относящихся к ОИ ЭП.».

3. Внести в приказ и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 16 августа 2019 года № 199/НҚ «Об утверждении Правил проведения мониторинга событий информационной безопасности объектов информатизации государственных органов» (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 19286) следующие изменения:

преамбулу изложить в следующей редакции:

«В соответствии с подпунктом 5-1) статьи 7-1 Закона Республики Казахстан «Об информатизации» **ПРИКАЗЫВАЮ**:»;

Правила проведения мониторинга событий информационной безопасности объектов информатизации государственных органов, утвержденные указанным приказом, изложить в новой редакции согласно приложению 2 к настоящему Перечню.

Приложение 1 к Перечню
в некоторые приказы, в которые
вносятся изменения и дополнение

Приложение к Правилам
и срокам передачи
резервных копий
электронных информационных
ресурсов на единую
национальную резервную
платформу хранения
электронных информационных
ресурсов

Форма

Сведения о технических характеристиках электронных информационных ресурсов

№	Полное наименование ЭИР	Операционная система (версия)	СУБД / ПО / ППО (Наименование/версия)	Размер Базы данных, Гб	Размер резервной копии (дампа), Гб	Планируемый ежегодный прирост размера БД, Гб

Продолжение таблицы

Кол-во CPU сервера	Уровень загрузки CPU сервера (в %)	Объем ОЗУ сервера, Гб	Средства резервного копирования	Владелец КВОИКИ	Класс ЭИР	Фамилия, имя, отчество ответственного лица ЭИР/номер телефона

Примечание по расшифровке аббревиатур:

СУБД – система управления базами данных;

ПО – программное обеспечение;

ППО – прикладное программное обеспечение;

CPU – центральный процессор компьютера;

Гб – гигабайт;

БД – база данных;

ОЗУ – оперативно запоминающее устройство;

ЭИР – электронный информационный ресурс.

Приложение 2 к Перечню в
некоторые
приказы, в которые вносятся
изменения и дополнение

Утверждены
приказом Министра
цифрового развития, инноваций
и аэрокосмической промышленности
Республики Казахстан
от 16 августа 2019 года № 199/НҚ

Правила проведения мониторинга событий информационной безопасности объектов информатизации государственных органов

Глава 1. Общие положения

1. Настоящие Правила проведения мониторинга событий информационной безопасности объектов информатизации государственных органов (далее - Правила) разработаны в соответствии с подпунктом 5-1) статьи 7-1 Закона Республики Казахстан «Об информатизации» (далее – Закон) и определяют порядок проведения мониторинга событий информационной безопасности объектов информатизации государственных органов.

2. В настоящих Правилах используются следующие понятия и определения:

1) объекты информатизации - электронные информационные ресурсы, программное обеспечение, интернет-ресурс и информационно-коммуникационная инфраструктура;

2) информационная безопасность в сфере информатизации (далее - информационная безопасность) - состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

3) мониторинг событий информационной безопасности - постоянное наблюдение за объектом информатизации с целью выявления и идентификации событий информационной безопасности;

4) событие информационной безопасности (далее - событие ИБ) - состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объекта информатизации;

5) инцидент информационной безопасности (далее - инцидент ИБ) - отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов;

6) государственная техническая служба (далее – АО «ГТС») – акционерное общество, созданное по решению Правительства Республики Казахстан;

7) журналирование событий – процесс записи информации о происходящих с объектом информатизации программных или аппаратных событиях в журнал регистрации событий;

8) система сбора журналов регистрации событий – аппаратно-программный комплекс, обеспечивающий централизованный сбор журналов регистрации событий объектов информатизации, их хранение и дальнейшую передачу в систему управления событиями ИБ;

9) координатор информационной безопасности – работник АО «ГТС», располагающийся на постоянной основе в государственном органе и осуществляющий координацию мероприятий, направленных на поддержание состояния защищенности объектов информатизации государственных органов.

Иные понятия, используемые в настоящих Правилах, применяются в соответствии с Законом.

3. Мониторинг событий информационной безопасности объектов информатизации государственных органов (далее – МСИБ) проводится АО «ГТС», реализующим задачи и функции Национального координационного центра информационной безопасности (далее – НКЦИБ).

4. Объектами МСИБ являются объекты информатизации государственного органа (далее – ГО).

5. К объектам МСИБ не относятся:

1) электронные информационные ресурсы, содержащие сведения, составляющие государственные секреты;

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 правительственной, засекреченной, шифрованной и кодированной связи;

3) объекты информатизации Национального Банка Республики Казахстан, не интегрируемые с объектами информационно-коммуникационной инфраструктуры «электронного правительства».

6. В рамках МСИБ источниками событий ИБ являются:

средства защиты информации в информационно-коммуникационной инфраструктуре (далее – ИКИ) объектов МСИБ, в том числе, устанавливаемые и сопровождаемые АО «ГТС» (далее – источники событий ИБ);

система управления событиями ИБ НКЦИБ.

7. МСИБ включает в себя следующие виды работ:

1) установку источников событий ИБ в ИКИ объектов МСИБ;

2) техническое сопровождение источников событий ИБ в ИКИ объектов МСИБ;

3) отслеживание событий ИБ объектов МСИБ с целью обнаружения инцидентов ИБ и последующего на них реагирования.

8. МСИБ проводится по одному из следующих вариантов:

1) по одному виду работ;

2) по нескольким видам работ.

9. МСИБ проводится АО «ГТС» на основании договорных отношений между Комитетом национальной безопасности Республики Казахстан (далее – КНБ РК) и АО «ГТС», в отношении объектов МСИБ, расположенных на территории Республики Казахстан.

Глава 2. Порядок проведения мониторинга событий информационной безопасности объектов информатизации государственных органов

10. При проведении МСИБ АО «ГТС» осуществляет:

1) в рамках установки источников событий ИБ:

изучение ИКИ объектов МСИБ;

развертывание аппаратно-программного комплекса источников событий ИБ в ИКИ объектов МСИБ;

настройку отдельных механизмов функционирования и политик безопасности источников событий ИБ, а также проверку корректности их работы;

2) в рамках технического сопровождения источников событий ИБ:

установку обновлений источников событий ИБ по мере их выпуска производителем;

контроль состояния источников событий ИБ, их параметров и режимов защиты, в том числе устранение ошибок и недостатков в их функционировании;

отработку заявок от ГО по вопросам функционирования источников событий ИБ;

3) в рамках отслеживания событий ИБ объектов МСИБ, с целью обнаружения инцидентов ИБ и последующего на них реагирования:

определение перечня журналов регистрации событий, необходимых для передачи в систему управления событиями ИБ НКЦИБ;

организацию журналирования событий источников событий ИБ, сопровождаемых АО «ГТС»;

организацию систем сбора журналов регистрации событий НКЦИБ в контурах сетей телекоммуникаций ГО, в которых функционируют объекты МСИБ;

организацию сбора журналов регистрации событий объектов МСИБ и источников событий ИБ в систему сбора журналов регистрации событий НКЦИБ;

организацию передачи журналов регистрации событий объектов МСИБ и источников событий ИБ в систему управления событиями ИБ НКЦИБ их обработку и анализ с целью выявления событий ИБ и инцидентов ИБ;

первичный анализ событий ИБ или инцидентов ИБ, выявленных на объекте МСИБ;

уведомление ГО или уполномоченного им лица о выявленных событиях ИБ и инцидентах ИБ в течение 30 минут с момента выявления события ИБ или инцидента ИБ, КНБ РК – в течение 3 часов;

выдачу первичных рекомендаций по приостановлению распространения инцидента ИБ ГО или уполномоченному им лицу;

при наличии технической возможности принятие мер по приостановлению распространения инцидента ИБ посредством источников событий ИБ;

направление, при необходимости, к месту размещения объектов МСИБ работника АО «ГТС» в рамках реагирования на инцидент ИБ (необходимость определяется КНБ РК или АО «ГТС» самостоятельно);

уведомление уполномоченного органа в сфере обеспечения информационной безопасности (далее – уполномоченный орган) и КНБ РК о неустранении ГО или уполномоченным им лицом причин и последствий инцидента ИБ по истечении 48 часов с момента выявления инцидента ИБ.

11. Координатор информационной безопасности осуществляет:

изучение информационно-коммуникационной инфраструктуры ГО в целях формирования рекомендаций по повышению уровня защищенности ОИ ГО;

изучение технической документации по ИБ ГО в целях формирования рекомендаций по ее актуализации и пересмотра требований технической документации;

координирование мероприятий по реагированию на инциденты ИБ, выявленных в информационно-коммуникационной инфраструктуре ГО;

содействие в реагировании на инциденты ИБ посредством средств защиты информации, установленных работниками АО «ГТС» (при технической возможности);

содействие в проведении мероприятий по повышению осведомленности в сфере ИБ у работников ГО.

12. ГО или уполномоченное им лицо при проведении МСИБ:

предоставляют физический и сетевой доступ сотрудникам АО «ГТС» к информационно-коммуникационной инфраструктуре ГО и учетные записи с необходимыми правами для установки и сопровождения средств защиты информации;

предоставляют АО «ГТС» IP-адреса в контурах сетей телекоммуникаций для организации передачи журналов регистрации событий объектов МСИБ и источников событий ИБ в систему управления событиями ИБ НКЦИБ;

на ежеквартальной основе предоставляют АО «ГТС» актуальные сведения, согласно приложению, к настоящим Правилам;

осуществляют обновление до актуальных версий пользовательских и серверных операционных систем;

оповещают АО «ГТС» о результатах анализа события ИБ и (или) о мерах, принятых по устранению инцидента ИБ, в течение 48 часов с момента получения уведомления от АО «ГТС» о выявлении события ИБ или инцидента ИБ соответственно.

13. АО «ГТС», согласно договорам, на оказание услуг МСИБ, ежеквартально направляет в КНБ РК сводную информацию по выявленным угрозам ИБ, событиям ИБ и инцидентам ИБ, а также сведения о принятых ГО мерах по ним.

14. КНБ РК ежеквартально направляет в уполномоченный орган сводную информацию по выявленным инцидентам ИБ, а также сведения о принятых ГО мерах по ним.

Приложение к Правилам
проведения мониторинга событий
информационной безопасности
объектов информатизации
государственных органов

Сведения об объекте МСИБ

№	Наименование государственного органа	Структурное подразделение (департамент)	Физическое месторасположение (*этаж, кабинет*)	ФИО пользователя/ответственного лица	Сетевое имя рабочей станции/серверного оборудования	IP-адрес	Наименование операционной системы
1	2	3	4	5	6	7	8
Локальная сеть внутреннего контура							
Локальная сеть внешнего контура							