Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры

Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 7 июня 2018 года № 17019.

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

Сноска. Преамбула - в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 27.10.2022 № 399/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

1. Утвердить прилагаемые Правила проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры.

2. Признать утратившим силу приказ исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 66 "Об утверждении Правил проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации " электронного правительства" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 13178, опубликован 10 марта 2016 года в информационно-правовой системе "Әділет").

3. Комитету по информационной безопасности Министерства оборонной и аэрокосмической промышленности Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

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

2) в течение десяти календарных дней со дня государственной регистрации в Министерстве юстиции Республики Казахстан настоящего приказа направление его копии в бумажном и электронном виде на казахском и русском языках в Республиканское государственное предприятие на праве хозяйственного ведения " Республиканский центр правовой информации" для официального опубликования и включения в Эталонный контрольный банк нормативных правовых актов Республики Казахстан;

3) в течение десяти календарных дней после государственной регистрации настоящего приказа направление его копии на официальное опубликование в периодические печатные издания;

4) размещение настоящего приказа на интернет-ресурсе Министерства оборонной и аэрокосмической промышленности Республики Казахстан после его официального опубликования;

5) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства оборонной и аэрокосмической промышленности Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1), 2), 3) и 4) настоящего пункта.

4. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра оборонной и аэрокосмической промышленности Республики Казахстан.

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

Министр оборонной
и аэрокосмической промышленности
Республики Казахстан *Б. Атамкулов*

"СОГЛАСОВАНО"
Председатель Комитета
национальной безопасности
Республики Казахстан
_____ К. Масимов
"___" _____ 2018 года

Утверждены
приказом
Министра оборонной
и аэрокосмической промышленности
Республики Казахстан
от 28 марта 2018 года № 52/НҚ

Правила проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры

Сноска. Правила в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 13.08.2019 № 195/НҚ (вводится в действие с 20.09.2019).

Глава 1. Общие положения

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.

Сноска. Пункт 1 - в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 27.10.2022 № 399/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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 – недостаток объекта информатизации, использование которого может привести к нарушению целостности и (или) конфиденциальности, и (или) доступности объекта информатизации;

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;

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";

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.

Сноска. Пункт 2 - в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 27.10.2022 № 399/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования); с изменением, внесенным приказом и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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:

мониторинг реагирования на инциденты ИБ;

мониторинг обеспечения защиты;

мониторинг обеспечения безопасного функционирования.

Сноска. Пункт 3 с изменением, внесенным приказом Министра цифрового развития , инноваций и аэрокосмической промышленности РК от 27.10.2022 № 399/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

4. Объектами МОИБ являются введенные в промышленную эксплуатацию ОИ ЭП, в том числе отнесенные к КВОИКИ, за исключением:

электронных информационных ресурсов, содержащих сведения, составляющие государственные секреты;

информационных систем в защищенном исполнении, отнесенных к государственным секретам;

объектов информатизации Национального банка Республики Казахстан, не интегрируемых с ОИ ЭП.

Сноска. Пункт 4 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

5. МОИБ проводится по одному из следующих вариантов:

1) по одному виду работ;

2) по нескольким видам работ;

3) в полном составе видов работ.

Сноска. Пункт 5 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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

Сноска. Пункт 6 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Глава 2. Порядок проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства"

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:

1) перечень программных и технических средств;

2) схемы сетей телекоммуникаций;

3) контрольные суммы исходных кодов и/или файлов программных средств;

4) структуры баз данных.

Сноска. Пункт 7 с изменением, внесенным приказом Министра цифрового развития , инноваций и аэрокосмической промышленности РК от 27.10.2022 № 399/НҚ (

вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

8. Собственник или владелец объекта МОИБ уведомляет АО "ГТС" о вводе объекта МОИБ в промышленную эксплуатацию, либо о прекращении эксплуатации в течение 10 рабочих дней со дня ввода в промышленную эксплуатацию, либо прекращения эксплуатации официальным письмом и предоставляет в бумажном и электронном виде сведения об ОИ ЭП по форме, согласно приложению 1 к настоящим Правилам (далее – Сведения).

Сноска. Пункт 8 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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

Сноска. Пункт 9 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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 в систему управления событиями ИБ НКЦИБ журналов регистрации событий объекта МОИБ и относящихся к нему средств защиты информации, 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 в течение 30 минут с момента выявления события ИБ или инцидента ИБ с предоставлением перечня данных о выявленном событии ИБ или инциденте ИБ согласно приложению 7 к настоящим Правилам;

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 при не устранении собственником или владельцем объекта МОИБ или уполномоченным им лицом причин и последствий инцидента ИБ в течение 72 часов с момента подтверждения инцидента ИБ;

2) в рамках мониторинга обеспечения защиты:

обследование объектов 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);

при проведении ручного тестирования на проникновение обследование локальной вычислительной сети (при ее наличии), имеющей сопряжение с локальной вычислительной сетью, в которой размещен объект МОИБ;

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;

по запросу собственника или владельца объектов МОИБ консультирование 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 к настоящим Правилам, согласно графику проведения работ по МОИБ;

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

Сноска. Пункт 10 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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 ТД по ИБ, утвержденной собственником или владельцем объекта МОИБ, заверенной его подписью и печатью (при наличии);

физический доступ к серверному и сетевому оборудованию, сети телекоммуникаций объекта МОИБ с проведением фото и видео фиксации и к документации на объект МОИБ и сопутствующей документации, в том числе к договорам на сопровождение и техническую поддержку объекта МОИБ.

Сноска. Пункт 11 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

12. При проведении АО "ГТС" мониторинга реагирования на инциденты ИБ собственник или владелец объекта МОИБ или лицо, оказывающее ему услуги ОЦИБ:

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 к настоящим Правилам;

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;

при самостоятельном обнаружении инцидента ИБ на объекте МОИБ, уведомляет АО "ГТС" в течение 15 минут с момента подтверждения инцидента ИБ и направляет в АО "ГТС" информацию о принятых мерах по устранению инцидента ИБ в течение 72 часов с момента его подтверждения, в соответствии с Приложением 2 к настоящим Правилам;

в случае уведомления АО "ГТС" о событии ИБ или инциденте ИБ, в течение 72 часов с момента уведомления направляет в АО "ГТС":

при подтверждении события ИБ - результаты анализа события ИБ;

при подтверждении инцидента ИБ - информацию о принятых мерах по устранению инцидента ИБ в соответствии с Приложением 2 к настоящим Правилам.

Сноска. Пункт 12 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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

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

при самостоятельном обнаружении уязвимости объекта МОИБ, предоставляет в АО "ГТС" перечень данных об уязвимости ОИ ЭП по форме согласно приложению 5 к настоящим Правилам в течение 24 часов с момента выявления уязвимости;

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 к настоящим Правилам.

Сноска. Пункт 13 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

14. При проведении АО "ГТС" мониторинга обеспечения безопасного функционирования собственник или владелец объекта МОИБ:

в течение 10 рабочих дней со дня получения уведомления о проведении работ по обследованию объекта МОИБ на предмет исполнения требований ТД по ИБ предоставляет в АО "ГТС" копии ТД по ИБ, утвержденной собственником или владельцем объекта МОИБ, заверенной его подписью и печатью (при наличии), приведенной в приложении 3 к настоящим Правилам;

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.

Сноска. Пункт 14 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

15. АО "ГТС" направляет запрос собственникам или владельцам объектов МОИБ о предоставлении Сведений с целью формирования перечня объектов МОИБ.

Собственник или владелец объекта МОИБ в течение 10 рабочих дней с момента получения запроса от АО "ГТС" предоставляет в АО "ГТС" Сведения в электронной форме.

Сноска. Пункт 15 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

16. Собственник или владелец объекта МОИБ при изменении контактных данных лица, ответственного за обеспечение ИБ объекта МОИБ, в течение 48 часов с момента данного изменения направляет в АО "ГТС" актуальные контактные данные.

Сноска. Пункт 16 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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.

Сноска. Пункт 17 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

18. КНБ РК ежеквартально направляет в уполномоченный орган сводную информацию по выявленным 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.

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

Сноска. Заголовок главы 3 - в редакции приказа Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 27.10.2022 № 399/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

19. Мониторинг обеспечения информационной безопасности КВОИКИ, не относящихся к ОИ ЭП, осуществляется собственным подразделением по ИБ владельца КВОИКИ или путем приобретения услуг третьих лиц в соответствии со статьей 683 Гражданского кодекса Республики Казахстан.

Сноска. Пункт 19 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится

в действие по истечении десяти календарных дней после дня его первого официального опубликования).

20. Собственник или владелец КВОИКИ обеспечивает подключение системы мониторинга обеспечения ИБ (далее – СМО ИБ) КВОИКИ к техническим средствам ОЦИБ, а также определяет ответственного по ИБ КВОИКИ в течение девяноста календарных дней со дня включения в перечень КВОИКИ, утверждаемый уполномоченным органом в сфере обеспечения информационной безопасности.

Сноска. Пункт 20 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

21. Исключен приказом и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 31.03.2023 № 128/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

22. После подключения СМО ИБ КВОИКИ к техническим средствам ОЦИБ, при выявлении СМО ИБ ОЦИБ инцидента ИБ, ОЦИБ в течение 15 минут с момента подтверждения инцидента ИБ уведомляет АО "ГТС" и собственника или владельца КВОИКИ путем оповещения ответственного по ИБ КВОИКИ. ОЦИБ в течение 72 часов с момента подтверждения инцидента ИБ направляет в АО "ГТС" информацию о принятых мерах по устранению инцидента ИБ в соответствии с Приложением 2 к настоящим Правилам.

Сноска. Пункт 22 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

23. Собственник или владелец КВОИКИ исправляет выявленные уязвимости в течение тридцати календарных дней после получения уведомления.

24. В случае самостоятельного выявления инцидента ИБ подразделением по ИБ КВОИКИ, ответственный по ИБ КВОИКИ в течение 15 минут с момента подтверждения инцидента ИБ уведомляет АО "ГТС" и ОЦИБ. ОЦИБ в течение 72 часов с момента подтверждения инцидента ИБ направляет в АО "ГТС" информацию о принятых мерах по устранению инцидента ИБ в соответствии с Приложением 2 к настоящим Правилам. В случае отсутствия лица, оказывающего услуги ОЦИБ, информацию о принятых мерах по устранению инцидента ИБ в АО "ГТС" направляет подразделение по ИБ КВОИКИ.

Сноска. Пункт 24 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится

в действие по истечении десяти календарных дней после дня его первого официального опубликования).

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

Сноска. Правила дополнены пунктом 25 в соответствии с приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 27.10.2022 № 399/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Приложение 1
к Правилам проведения
мониторинга обеспечения
информационной безопасности
объектов информатизации
"электронного правительства"
и критически важных объектов
информационно-коммуникационной
инфраструктуры
Форма

Сведения об объекте информатизации "электронного правительства"

Сноска. Приложение 1 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

1. Официальное наименование объекта информатизации "электронного правительства" (далее - ОИ ЭП).

2. Собственник ОИ ЭП.

3. Владелец ОИ ЭП (при наличии).

4. Физическое месторасположение ОИ ЭП (улица, город, область).

5. Организация, осуществляющая сопровождение и (или) системно-техническое обслуживание ОИ ЭП (с указанием полных контактных данных).

6. Уровень критичности согласно классификатору объектов информатизации: высокий, средний, низкий.

7. Информация о наличии подключения ОИ ЭП к Единой транспортной среде государственных органов и пропускной способности канала связи.

8. Информация о наличии подключения ОИ ЭП к Интернету и пропускной способности канала связи.

9. Логическая и физическая архитектурные схемы ОИ ЭП, утвержденные собственником или владельцем ОИ ЭП и заверенные его подписью и печатью (при наличии).

10. Информация о наличии системы сбора журналов регистрации событий с указанием наименования системы и контура локальной сети, в котором функционирует система.

11. Контактные данные ОЦИБ или лица, ответственного за обеспечение информационной безопасности ОИ ЭП.

12. Сведения о технических и программных средствах ОИ ЭП, в том числе, резервных технических и программных средствах и средствах защиты информации, относящихся к ОИ ЭП, с указанием IP-адресов, доменных имен (при наличии), назначения технического и программного средства и версии (при наличии), к которому относится IP-адрес.

Приложение 1
к Сведениям об объекте
информатизации "электронного
правительства"
Форма

Сноска. Приложение 1 исключено приказом и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Приложение 2
к Сведениям об объекте
информатизации "электронного
правительства"
Форма

Сноска. Приложение 2 исключено приказом и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Приложение 2
к Правилам проведения
мониторинга обеспечения
информационной безопасности
объектов информатизации
"электронного правительства"
и критически важных объектов
информационно-коммуникационной
инфраструктуры
Форма

Перечень данных об инциденте информационной безопасности

Сноска. Приложение 2 - в редакции приказа и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Дата регистрации инцидента ИБ	
Уровень критичности инцидента ИБ*	Высокий (4); Средний (3); Низкий (2); Не определено (1).
Тип инцидента ИБ	Отказ в облуживании (DoS, DDoS); Несанкционированный доступ и модификация содержания; Ботнет; Вирусная атака; Шифровальщик; Эксплуатация уязвимости; Компрометация средств аутентификации/авторизации; Фишинг; Спам; Другой.
Масштабность	Единичный; Массовый.
Детали	Дата и время возникновения; Дата и время подтверждения; Повторный/новый; Индикатор компрометации (IOC).
Признак	Действительный; Попытка; Подозрение;
Контур	Локальная сеть внутреннего контура; Локальная сеть внешнего контура.
Описание инцидента ИБ	
Последствие	Без последствий; Нарушение работоспособности; Нарушение целостности; Нарушение режима конфиденциальности информации.
Объект, которому нанесен ущерб	
Действия, предпринятые для устранения инцидента ИБ	
Примечание	

Уровни критичности инцидента информационной безопасности

Уровень критичности	Признаки	Примеры инцидентов ИБ
Высокий (4)	Инциденты ИБ, которые приводят к невозможности предоставления услуг/выполнения работ, и (или) потере/модификации критичных* данных, и (или) нарушению конфиденциальности объекта	- Несанкционированный доступ - Эксплуатация уязвимости - Шифровальщик - Вредоносное ПО - Отказ в обслуживании

	информатизации, обрабатывающего критичные* данные.	(DoS/DDoS-атака) И т.д.
Средний (3)	Инциденты ИБ, которые приводят к существенному ограничению предоставления услуг/выполнения работ, и (или) потере/ модификации данных, не являющихся критичными*, и (или) нарушению конфиденциальности объекта информатизации, обрабатывающего данные, не являющихся критичными*.	- Несанкционированный доступ - Шифровальщик - Вредоносное ПО - Отказ в обслуживании (DoS/DDoS-атака) - Эксплуатация уязвимости И т.д.
Низкий (2)	Инциденты ИБ, не влияющие на предоставление услуги/ выполнение работ.	- Вредоносное ПО - Отказ в обслуживании (DoS/ DdoS-атака) - Эксплуатация уязвимости - Спам - Фишинговая атака И т.д.
Не определено (1)**	Влияние инцидента ИБ на предоставление услуг не определено	Нехарактерная/подозрительная активность

Примечание:

* К критичным данным относятся данные, защищаемые законодательством Республики Казахстан и/или отнесенные к критичным владельцем/собственником объекта информатизации.

**Уровень необходимо пересмотреть в течение 48 часов с момента подтверждения инцидента ИБ.

Приложение 3
к Правилам проведения
мониторинга обеспечения
информационной безопасности
объектов информатизации
"электронного правительства"
и критически важных объектов
информационно-коммуникационной
инфраструктуры
Форма

Техническая документации по информационной безопасности

1. Документы первого уровня:

1) политика информационной безопасности.

2. Документы второго уровня:

1) методика оценки рисков информационной безопасности;

2) правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации;

3) правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации;

4) правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения;

5) правила проведения внутреннего аудита ИБ;

6) правила использования средств криптографической защиты информации;

7) правила разграничения прав доступа к электронным информационным ресурсам;

8) правила использования Интернет и электронной почты;

9) правила организации процедуры аутентификации;

10) правила организации антивирусного контроля;

11) правила использования мобильных устройств и носителей информации;

12) правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов.

3. Документы третьего уровня:

1) каталог угроз (рисков) ИБ;

2) план обработки угроз (рисков) ИБ;

3) регламент резервного копирования и восстановления информации;

4) план мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации;

5) руководство администратора по сопровождению объекта информатизации;

6) инструкцию о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях.

4. Документы четвертого уровня:

1) журнал регистрации инцидентов ИБ и учета внештатных ситуаций;

2) журнал посещения серверных помещений;

3) отчет о проведении оценки уязвимости сетевых ресурсов;

4) журнал учета кабельных соединений;

5) журнал учета резервных копий (резервного копирования, восстановления), тестирования резервных копий;

6) журнал учета изменений конфигурации оборудования, тестирования и учета изменений свободного программного обеспечения и прикладного программного обеспечения информационной системы, регистрации и устранения уязвимостей программного обеспечения;

7) журнал тестирования дизель-генераторных установок и источников бесперебойного питания для серверного помещения;

8) журнал тестирования систем обеспечения микроклимата, видеонаблюдения, пожаротушения серверных помещений.

Приложение 4
к Правилам проведения

мониторинга обеспечения
информационной безопасности
объектов информатизации
"электронного правительства"
и критически важных объектов
информационно-коммуникационной
инфраструктуры
Форма

Форматы и типы записей журналов регистрации событий объектов информатизации " электронного правительства"

Глава 1. Форматы и типы записей журналов регистрации событий операционной системы

1. Типы событий операционной системы (далее – ОС), подлежащие журналированию:

1) запуск/остановка системы;

2) работа с объектами ОС (открытие, сохранение, переименование, удаление, создание, копирование);

3) установка и удаление программного обеспечения (далее – ПО);

4) авторизация (вход и выход) пользователей в ОС, успешные и неуспешные попытки авторизации;

5) изменение системной конфигурации;

6) создание, удаление, модификация учетных записей;

7) активация/дезактивация систем защиты, таких как антивирусные системы и системы обнаружения вторжения, и средств ведения журнала регистрации событий;

8) изменение или попытки изменения настроек и средств управления защитой системы;

9) использование привилегированных учетных записей;

10) подключение/отключение устройства ввода/вывода;

11) неудавшиеся или отвергнутые действия пользователя;

12) неудавшиеся или отвергнутые действия, затрагивающие данные и другие ресурсы;

13) запуск, остановка процессов в ОС.

2. Журнал регистрации событий ОС содержит следующие поля:

1) дата и время (формат даты: ДД:ММ:ГГГГ, формат времени: ЧЧ:ММ:СС);

2) наименование хоста;

3) описание события.

3. Для серверных ОС семейства Unix-подобных систем (Unix, Linux, AIX, HPUX и др.) дополнительно к событиям из пункта 1, необходима фиксация следующих событий :

1) подключение идентичной учетной записи с разных IP-адресов на один и тот же сервер;

2) открытие новых портов в системе;

3) всех событий в ключевых логах: /var/log/secure, /var/log/messages, /var/log/audit.

4. Для серверных ОС семейства Windows, дополнительно к событиям из пункта 1, необходима фиксация следующих событий:

1) присвоение специальных привилегий новому сеансу (logon) – Windows EID 4672;

2) Сетевой вход (Network logon) – Windows EID 4624;

3) Доступ к сетевой папке администратора (administrative share access) и доступ к SMB каналам (pipes) – Windows EID 5140/5145;

4) доступ к объекту "Файл" с правами "Запись данных" или "Добавление файла–Windows" EID 4663;

5) запуск потенциально опасных процессов (WmiPrvSE.exe, WinrsHost.exe, wsmprovhost.exe, mmc.exe, psexe*.exe, paexe*.exe) – Sysmon EID 1;

6) установка и запуск службы (сервиса) – Windows EID 7045/7036/4697;

7) создание или изменение параметров заданий в планировщике задач (scheduled tasks) – Windows EID 4698/4702;

8) достигнут таймаут службы– Windows EID 7009;

9) ошибка при запуске службы – Windows EID 7000;

10) изменено значение реестра – Windows EID 4657;

11) запись в пространство имен WMI – Windows EID 4662.

5. Записи в журналах регистрации событий хранятся в текстовом формате.

6. Значения полей журналов регистрации событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей.

7. Для журналов регистрации событий используется кодировка UTF-8.

8. В один файл журнала регистрации событий не допускается запись событий, имеющих разные форматы данных.

Глава 2. Форматы и типы записей журналов регистрации событий системы управления базами данных

9. Типы событий системы управления базами данных, подлежащие журналированию:

1) контроль сессий (успешная/неуспешная авторизация, регистрация использования незарегистрированных учетных записей);

2) все действия пользователей базы данных (далее – БД) имеющих административные привилегии (включая команды select, create, alter, drop, truncate, rename, insert, update, delete, call (execute), lock);

3) все действия пользователей имеющих права на присвоение привилегий другим пользователям БД (grant, revoke, deny).

10. Журнал регистрации событий БД содержит следующие поля:

1) дата и время (формат даты: ДД:ММ:ГГГГ, формат времени: ЧЧ:ММ:СС);

2) имя учетной записи/ID пользователя;

3) IP-адрес хоста или наименование хоста;

4) описание события;

5) наименование объекта (таблицы, процедуры, функции, при возможности реализации).

11. Записи в журналах регистрации событий хранятся в текстовом формате.

12. Значения полей журналов регистрации событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей.

13. Для журналов регистрации событий используется кодировка UTF-8.

14. В один файл журнала регистрации событий не допускается запись событий, имеющих разные форматы данных.

Глава 3. Форматы и типы записей журналов регистрации событий телекоммуникационного оборудования

15. Типы событий телекоммуникационного оборудования, подлежащие журналированию:

1) запуск/остановка системы;

2) изменение системной конфигурации;

3) создание, удаление, модификация локальных учетных записей;

4) использование привилегированных учетных записей;

5) подключение/отключение устройства ввода/вывода;

6) неудавшиеся или отвергнутые действия пользователя;

7) запуск, падение, остановка сетевых линков (коннектов).

16. С межсетевых экранов при наличии технической возможности ведется запись логов всего трафика (входящего и исходящего), а также запись всех событий на устройстве.

17. Журнал регистрации событий телекоммуникационного оборудования содержит следующие поля:

1) дата и время (формат даты: ДД:ММ:ГГГГ, формат времени: ЧЧ:ММ:СС);

2) наименование устройства;

3) имя учетной записи/ID пользователя;

4) IP-адрес хоста;

5) IP-адрес источника;

6) IP-адрес назначения;

7) описание события.

18. Записи в журналах регистрации событий хранятся в текстовом формате.

19. Значения полей журналов регистрации событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей.

20. Для журналов регистрации событий используется кодировка UTF-8.

21. В один файл журнала регистрации событий не допускается запись событий, имеющих разные форматы данных.

Глава 4. Форматы и типы записей журналов регистрации событий прикладного программного обеспечения

22. Типы событий ПО, подлежащие журналированию:

1) авторизация (вход и выход) пользователей, успешные и неуспешные попытки авторизации;

2) создание, копирование, перемещение, удаление, модификация локальных учетных записей и конфигурационных файлов;

3) неудавшиеся или отвергнутые действия пользователя;

4) получение пользователем доступа к объектам доступа;

5) действия пользователей прикладного ПО (доступ к объекту (данным), изменения объекта (данных), удаления объекта (данных)).

23. Журнал регистрации событий ПО содержит следующие поля:

1) дата и время (формат даты: ДД:ММ:ГГГГ, формат времени: ЧЧ:ММ:СС);

2) наименование источника события (сервис/служба);

3) имя учетной записи/ID пользователя;

4) IP-адрес пользователя;

5) время начала операции;

6) время окончания операции;

7) описание события.

24. Записи в журналах регистрации событий хранятся в текстовом формате.

25. Значения полей журналов регистрации событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей.

26. Для журналов регистрации событий используется кодировка UTF-8.

27. В один файл журнала регистрации событий не допускается запись событий, имеющих разные форматы данных.

Глава 5. Форматы и типы записей журналов регистрации событий, выявляемые средствами защиты информации

28. Типы событий, выявляемые средствами защиты информации, подлежащие журналированию:

1) создание, копирование, перемещение, удаление, модификация локальных учетных записей и конфигурационных файлов;

2) запуск/остановка службы;

3) изменение системной конфигурации;

4) создание, удаление, модификация локальных учетных записей.

29. Журнал регистрации событий средств защиты информации содержит следующие поля:

1) дата и время (формат даты: ДД:ММ:ГГГГ, формат времени: ЧЧ:ММ:СС);

2) наименование источника события (сервис/служба);

3) имя учетной записи/ID пользователя;

4) IP-адрес клиента;

5) время начала операции;

6) время окончания операции;

7) описание события.

30. Записи в журналах регистрации событий хранятся в текстовом формате.

31. Значения полей журналов регистрации событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей.

32. Для журналов регистрации событий используется кодировка UTF-8.

33. В один файл журнала регистрации событий не допускается запись событий, имеющих разные форматы данных.

Приложение 5
к Правилам проведения
мониторинга обеспечения
информационной безопасности
объектов информатизации
"электронного правительства"
и критически важных объектов
информационно-коммуникационной
инфраструктуры
Форма

Перечень данных об уязвимости объекта информатизации "электронного правительства"

Дата и время обнаружения уязвимости	Контур	Название объекта информатизации	Компонент объекта информатизации (название, IP, hostname и т.д.)	Порт	Описание уязвимости	Дополнительная информация
1	2	3	4	5	6	7

	Внешний/ Внутренний контур					

Приложение 6
к Правилам проведения
мониторинга обеспечения
информационной безопасности
объектов информатизации
"электронного правительства"
и критически важных объектов
информационно-коммуникационной
инфраструктуры
Форма

Категории причин неустранения уязвимости и обоснование причины неустранения

Категории причин неустранения уязвимости	Обоснование причины неустранения уязвимости
Производственная необходимость	Описание уязвимости и состояние объекта информатизации "электронного правительства"; предпринятые меры по устранению уязвимости; причины и характер требуемых изменений в объекте информатизации; сроки устранения уязвимости, не превышающие шести месяцев с момента первого обнаружения.
Уязвимость нулевого дня	Описание уязвимости и состояние объекта информатизации "электронного правительства", а также проведенные мероприятия по снижению вероятности эксплуатации уязвимости.
Ложное срабатывание	Описание характеристики или состояние объекта информатизации "электронного правительства", определенного как уязвимость.

Приложение 7
к Правилам проведения
мониторинга обеспечения
информационной безопасности
объектов информатизации
"электронного правительства"
и критически важных объектов
информационно-коммуникационной
инфраструктуры
Форма

Перечень данных о выявленном событии информационной безопасности или инциденте информационной безопасности

Сноска. Правила дополнены приложением 7 в соответствии с приказом и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 23.04.2025 № 175/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

Дата регистрации события ИБ/инцидента ИБ	
Детали	Дата и время обнаружения; IP-адрес источника; IP-адрес назначения (при наличии информации в ЖРС); Наименование устройства/Имя компьютера; Наименование события ИБ/инцидента ИБ; Путь файла/Запрос (при наличии информации в ЖРС); Код ответа от сервера (при наличии информации в ЖРС); Количество сработок на СЗИ (при наличии информации в ЖРС); Организация-источник (при наличии информации в ЖРС); Первичное фиксирование/повторное фиксирование;
Описание события ИБ/инцидента ИБ	В случае наличия дополнительной информации в ЖРС
Собственник или владелец ОИ ЭП	
Объект, на котором выявлено событие ИБ/инцидент ИБ	
Примечание	