О внесении изменений 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"

Приказ и.о. Министра искусственного интеллекта и цифрового развития Республики Казахстан от 8 июля 2026 года № 394/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 14 июля 2026 года № 39299

ПРИКАЗЫВАЮ:

1. 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:

заголовок изложить в следующей редакции:

"Об утверждении Правил проведения мониторинга обеспечения кибербезопасности цифровых объектов "цифрового правительства" и критически важных цифровых объектов";

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 7) статьи 7-1 Закона Республики Казахстан "О кибербезопасности" **ПРИКАЗЫВАЮ:**";

пункт 1 изложить в следующей редакции:

"1. Утвердить прилагаемые Правила проведения мониторинга обеспечения кибербезопасности цифровых объектов "цифрового правительства" и критически важных цифровых объектов.".

Правила проведения мониторинга обеспечения кибербезопасности цифровых объектов "цифрового правительства" и критически важных цифровых объектов, утвержденные указанным приказом, изложить в новой редакции согласно приложению к настоящему приказу.

2. Комитету по информационной безопасности Министерства искусственного интеллекта и цифрового развития Республики Казахстан в установленном законодательством Республики Казахстан порядке обеспечить:

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

2) размещение настоящего приказа на интернет-ресурсе Министерства искусственного интеллекта и цифрового развития 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 искусственного интеллекта и цифрового развития Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1) и 2) настоящего пункта.

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра искусственного интеллекта и цифрового развития Республики Казахстан.

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

Исполняющий обязанности
министра искусственного интеллекта
и цифрового развития Республики Казахстан *Р. Коняшкин*

"СОГЛАСОВАН"
Комитет национальной безопасности
Республики Казахстан

Приложение к приказу
Исполняющий обязанности
министра искусственного
интеллекта и цифрового
развития
Республики Казахстан
от 8 июля 2026 года № 394/НҚ

Правила проведения мониторинга обеспечения кибербезопасности цифровых объектов " цифрового правительства" и критически важных цифровых объектов

Глава 1. Общие положения

1. Настоящие Правила проведения мониторинга обеспечения кибербезопасности цифровых объектов "цифрового правительства" и критически важных цифровых объектов (далее – Правила) разработаны в соответствии с подпунктом 7) статьи 7-1 Закона Республики Казахстан "О кибербезопасности" (далее – Закон) и определяют порядок проведения мониторинга обеспечения кибербезопасности цифровых объектов "цифрового правительства" и критически важных цифровых объектов.

2. В настоящих Правилах используются следующие понятия:

1) критически важные цифровые объекты (далее – КВЦО) – цифровые объекты, 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, " цифрового правительства";

2) оперативный центр кибербезопасности (далее – ОЦКБ) – юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите цифровых ресурсов, цифровых систем, сетей телекоммуникаций и других цифровых объектов;

3) нормативно-техническая документация по кибербезопасности (далее – ТД по КБ) – документация, устанавливающая политику, защитные меры, касающиеся процессов обеспечения кибербезопасности (далее – КБ) цифровых объектов и (или) организации;

4) система мониторинга обеспечения КБ – организационные и технические мероприятия, направленные на проведение мониторинга безопасного использования цифровых технологий;

5) уполномоченный орган в сфере обеспечения КБ (далее – уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство и межотраслевую координацию в сфере обеспечения КБ;

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

7) система управления событиями КБ – программное обеспечение или аппаратно-программный комплекс, предназначенные для автоматизированного выявления событий КБ и инцидентов КБ путем сбора и анализа журналов регистрации событий цифрового объекта;

8) событие КБ – идентифицированное возникновение состояния цифрового объекта, указывающее на возможное нарушение КБ или ранее неизвестную ситуацию, которая может иметь отношение к обеспечению КБ;

9) инцидент КБ – событие или совокупность событий, негативно влияющих на КБ цифрового объекта;

10) государственная техническая служба (далее – АО "ГТС") - государственное юридическое лицо, созданное по решению Правительства Республики Казахстан;

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

12) уязвимость – недостаток цифрового объекта, создающий угрозу кибербезопасности;

13) цифровой объект – обособленный элемент цифровой среды, созданный, используемый или передаваемый посредством цифровых технологий, обладающий уникальными цифровыми характеристиками и позволяющий субъектам цифровой среды осуществлять правомочия владения, пользования либо распоряжения в объеме, установленном законодательством Республики Казахстан;

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

15) журналирование цифровых событий – процесс систематической записи, сбора и хранения цифровых записей о событиях, происходящих в цифровых объектах, с целью последующего анализа, выявления отклонений и исследования инцидентов КБ;

16) архитектурный портал цифровых объектов государства – цифровой объект, предназначенный для осуществления учета, хранения и систематизации сведений о цифровых объектах государства, цифровой архитектуре государства, платформенных программных продуктах в целях дальнейшего использования государственными органами для мониторинга, анализа и планирования в сфере цифровизации;

17) цифровые объекты "цифрового правительства" (далее – ЦО ЦП) – цифровые объекты государственных органов и иных лиц, предназначенные для осуществления деятельности государственных органов, выполнения государственных функций и оказания государственных услуг;

18) мониторинг обеспечения КБ цифровых объектов "цифрового правительства" (далее – МОКБ) – отслеживание полноты и качества реализации собственниками и (или) владельцами цифровых объектов "цифрового правительства" технических и организационных мероприятий по обеспечению КБ ЦО ЦП посредством выявления угроз и инцидентов КБ.

3. МОКБ проводится АО "ГТС", реализующим задачи и функции Национального координационного центра кибербезопасности (далее – НКЦКБ), в соответствии с подпунктом 5) пункта 1 статьи 14 Закона, посредством системы МОКБ НКЦКБ и включает в себя следующие виды работ:

мониторинг реагирования на инциденты КБ;

мониторинг обеспечения защиты;

мониторинг обеспечения безопасного функционирования.

4. Объектами МОКБ являются введенные в промышленную эксплуатацию ЦО ЦП, в том числе отнесенные к КВЦО, за исключением:

цифровых ресурсов, содержащих сведения, составляющие государственные секреты;

цифровых систем в защищенном исполнении, отнесенных к государственным секретам;

цифровых объектов Национального банка Республики Казахстан, не интегрируемых с ЦО ЦП.

5. МОКБ проводится по одному из следующих вариантов:

1) по одному виду работ;

2) по нескольким видам работ;

3) в полном составе видов работ.

6. МОКБ, отнесенных к КВЦО, осуществляется на основании договора, заключенного между Комитетом национальной безопасности Республики Казахстан (далее – КНБ РК) и АО "ГТС".

Глава 2. Порядок проведения мониторинга обеспечения кибербезопасности цифровых объектов "цифрового правительства"

7. АО "ГТС" для проведения МОКБ в качестве первичной информации использует сведения об объекте МОКБ из архитектурного портала цифровых объектов государства , а также сведения, полученные на этапах проведения испытаний сервисного программного продукта, цифровой платформы "цифрового правительства", интернет-ресурса государственного органа и цифровой системы на соответствие требованиям КБ, 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.

8. Собственник или владелец объекта МОКБ уведомляет АО "ГТС" о вводе объекта МОКБ 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 о ЦО ЦП по форме, согласно приложению 1 к настоящим Правилам (далее – Сведения).

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

10. АО "ГТС" при проведении МОКБ осуществляет:

1) в рамках мониторинга реагирования на инциденты КБ:

анализ объекта МОКБ на предмет определения перечня журналов регистрации событий, необходимых для передачи в систему управления событиями КБ НКЦКБ;

установку агентов системы управления событиями КБ на систему сбора журналов регистрации событий объекта МОКБ и, при необходимости, на иные объекты цифровой инфраструктуры собственника или владельца объекта МОКБ;

сбор в систему управления событиями КБ НКЦКБ журналов регистрации событий объекта МОКБ и относящихся к нему средств защиты информации, их обработку и анализ с целью выявления событий КБ и инцидентов КБ;

первичный анализ событий КБ или инцидентов КБ, выявленных на объекте МОКБ;

рассматривает уведомления ответственных лиц за обеспечение КБ объекта МОКБ в течение 30 минут с момента выявления события КБ или инцидента КБ с предоставлением перечня данных о выявленном событии КБ или инциденте КБ согласно приложению 2 к настоящим Правилам;

выдачу первичных рекомендаций по приостановлению распространения инцидента КБ собственнику или владельцу объекта МОКБ;

направление, к месту размещения объекта МОКБ работника АО "ГТС" в рамках реагирования на инцидент КБ (по согласованию с КНБ РК и АО "ГТС");

уведомление КНБ РК при не устранении собственником или владельцем объекта МОКБ или уполномоченным им лицом причин и последствий инцидента КБ в течение 72 часов с момента подтверждения инцидента КБ;

2) в рамках мониторинга обеспечения защиты:

обследование объектов МОКБ на предмет наличия уязвимостей (далее – обследование на уязвимости) согласно графику проведения работ по МОКБ:

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

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

по запросу собственника или владельца объектов МОКБ консультирование по вопросам устранения уязвимостей объектов МОКБ, выявленных в рамках обследования на уязвимости;

3) в рамках мониторинга обеспечения безопасного функционирования:

обследование объекта МОКБ на предмет исполнения положений ТД по КБ, проводит в соответствие в приложением 3 к настоящим Правилам, согласно графику проведения работ по МОКБ;

предоставление собственникам или владельцам объектов МОКБ результатов обследования объекта МОКБ на предмет исполнения положений ТД по КБ и

устранения выявленных нарушений в течение 10 рабочих дней со дня завершения обследования.

11. Собственник или владелец объекта МОКБ обеспечивает условия для проведения АО "ГТС" работ по МОКБ, включая:

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

два рабочих места для работников АО "ГТС" с предоставлением круглосуточного сетевого доступа к объекту МОКБ на безвозмездной основе;

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

доступ к ТД по КБ, утвержденной собственником или владельцем объекта МОКБ, заверенной его подписью и печатью (при наличии);

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

12. При проведении АО "ГТС" мониторинга реагирования на инциденты КБ собственник или владелец объекта МОКБ или лицо, оказывающее ему услуги ОЦКБ:

организует журналирование событий объекта МОКБ и относящихся к нему средств защиты информации, в соответствии с форматами и типами записей журналов регистрации событий ЦО ЦП, приведенными в приложении 4 к настоящим Правилам;

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

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

уведомляет АО "ГТС" о планируемых работах по внесению изменений в журналирование событий объекта МОКБ 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 МОКБ из системы сбора журналов регистрации событий объекта МОКБ в систему управления событиями КБ НКЦКБ;

при самостоятельном обнаружении инцидента КБ на объекте МОКБ, уведомляет АО "ГТС" в течение 15 минут с момента подтверждения инцидента КБ и направляет в АО "ГТС" данные о принятых мерах по устранению инцидента КБ в течение 72 часов с момента его подтверждения, в соответствии с приложением 5 к настоящим Правилам;

при уведомлении АО "ГТС" о событии КБ или инциденте КБ, в течение 72 часов с момента уведомления направляет в АО "ГТС":

при подтверждении события КБ - результаты анализа события КБ ;

при подтверждении инцидента КБ - данные о принятых мерах по устранению инцидента КБ в соответствии с приложением 5 к настоящим Правилам.

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

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 МОКБ;

при самостоятельном обнаружении уязвимости объекта МОКБ, предоставляет в АО "ГТС" перечень данных об уязвимости ЦО ЦП по форме согласно приложению 6 к настоящим Правилам в течение 24 часов с момента выявления уязвимости;

при неустранении уязвимости объекта МОКБ 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 7 к настоящим Правилам.

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

в течение 10 рабочих дней со дня получения уведомления о проведении работ по обследованию объекта МОКБ на предмет исполнения положений ТД по КБ предоставляет в АО "ГТС" копии ТД по КБ, утвержденной собственником или владельцем объекта МОКБ, заверенной его подписью и печатью (при наличии);

в течение одного месяца со дня получения результатов обследования объекта МОКБ на предмет исполнения положений ТД по КБ предоставляет в АО "ГТС" информацию о мерах, принятых по выявленным нарушениям положений ТД по КБ.

15. АО "ГТС" направляет запрос собственникам или владельцам объектов МОКБ о предоставлении Сведений с целью формирования перечня объектов МОКБ. Собственник или владелец объекта МОКБ в течение 10 рабочих дней с момента получения запроса от АО "ГТС" предоставляет в АО "ГТС" Сведения в электронной форме.

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

17. АО "ГТС" ежеквартально направляет в КНБ РК сводную информацию по выявленным событиям КБ, инцидентам КБ, уязвимостям ЦО ЦП, изменениям ЦО ЦП и выявленным нарушениям положений ТД по КБ, а также сведения о принятых собственниками или владельцами объектов МОКБ мерах.

18. КНБ РК ежеквартально направляет в уполномоченный орган сводную информацию по выявленным инцидентам КБ, уязвимостям ЦО ЦП, изменениям ЦО ЦП и выявленным нарушениям положений ТД по КБ, а также сведения о принятых собственниками или владельцами объектов МОКБ мерах.

Глава 3. Порядок проведения мониторинга обеспечения кибербезопасности критически важных цифровых объектов

19. Мониторинг обеспечения КБ КВЦО, не относящихся к ЦО ЦП, осуществляется собственным подразделением по КБ владельца КВЦО или путем приобретения услуг третьих лиц в соответствии со статьей 683 Гражданского кодекса Республики Казахстан.

20. Собственник и (или) владелец КВЦО обеспечивает подключение системы мониторинга обеспечения КБ (далее – СМО КБ) КВЦО к техническим средствам ОЦКБ , а также определяет ответственного по КБ КВЦО в течение девяноста календарных дней со дня включения в перечень КВЦО, утверждаемого согласно подпункту 385) пункта 15 Положения о Министерстве искусственного интеллекта и цифрового развития Республики Казахстан, утвержденного постановлением Правительства Республики Казахстан от 9 октября 2025 года № 846.

21. После подключения СМО КБ КВЦО к техническим средствам ОЦКБ, при выявлении СМО КБ КВЦО инцидента КБ, ОЦКБ в течение 15 минут с момента подтверждения инцидента КБ уведомляет путем письменного (электронного) сообщения АО "ГТС" и собственника и (или) владельца КВЦО, оповещает путем письменного (электронного) сообщения ответственного по КБ КВЦО. ОЦКБ в течение 72 часов с момента подтверждения инцидента КБ направляет в АО "ГТС" данные о принятых мерах по устранению инцидента КБ.

22. При самостоятельном выявлении инцидента КБ подразделением по КБ КВЦО, ответственный по КБ КВЦО в течение 15 минут с момента подтверждения инцидента КБ уведомляет АО "ГТС" и ОЦКБ. ОЦКБ в течение 72 часов с момента подтверждения инцидента КБ направляет в АО "ГТС" данные о принятых мерах по устранению инцидента КБ. При отсутствии лица, оказывающего услуги ОЦКБ, информацию о принятых мерах по устранению инцидента КБ в АО "ГТС" направляет подразделение по КБ КВЦО.

Приложение 1
к Правилам проведения
мониторинга обеспечения
кибербезопасности
цифровых объектов
"цифрового правительства"
и критически важных
цифровых объектов
Форма

Сведения о цифровом объекте "цифрового правительства"

1. Официальное наименование ЦО ЦП.

2. Собственник ЦО ЦП.

3. Владелец ЦО ЦП (при наличии).

4. Физическое месторасположение ЦО ЦП (улица, город, область).

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

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

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

8. Информация о наличии подключения ЦО ЦП к Интернету и пропускной способности канала связи.

9. Логическая и физическая архитектурные схемы ЦО ЦП , 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 ОЦКБ или лица, ответственного за обеспечение КБ ЦО ЦП .

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

Приложение 2
к Правилам проведения
мониторинга обеспечения
кибербезопасности
цифровых объектов
"цифрового правительства"
и критически важных
цифровых объектов
Форма

Перечень данных о выявленном событии кибербезопасности или инциденте кибербезопасности

Дата регистрации события КБ/инцидента КБ	
	Дата и время обнаружения;

Детали	IP-адрес источника; IP-адрес назначения (при наличии информации в ЖРС); Наименование устройства/Имя компьютера; Наименование события КБ/инцидента КБ; 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 КБ/инцидента КБ	В случае наличия дополнительной информации в ЖРС
Собственник или владелец ЦО ЦП	
Объект, на котором выявлено событие КБ/инцидент КБ	
Примечание	

Приложение 3
к Правилам проведения
мониторинга обеспечения
кибербезопасности
цифровых объектов
"цифрового правительства"
и критически важных
цифровых объектов
Форма

Нормативно-техническая документация по кибербезопасности

1. Документы первого уровня:

1) политика КБ.

2. Документы второго уровня:

1) методика оценки рисков КБ;

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 КБ;

6) правила использования средств криптографической защиты информации;

7) правила разграничения прав доступа к цифровым 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 цифровых ресурсов.

3. Документы третьего уровня:

1) каталог угроз (рисков) КБ;

2) план обработки угроз (рисков) КБ ;

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 цифрового объекта;

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

4. Документы четвертого уровня:

1) журнал регистрации инцидентов КБ и учета внештатных ситуаций;

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 цифровой
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
кибербезопасности
цифровых объектов

"цифрового правительства"
и критически важных
цифровых объектов
Форма

Форматы и типы записей журналов регистрации событий цифровых объектов "цифрового 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, при содержании поля присутствует символ-разделитель и поле имеет длинный формат, 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, при содержании поля присутствует символ-разделитель и поле имеет длинный формат, 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, при содержании поля присутствует символ-разделитель и поле имеет длинный формат, 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
кибербезопасности
цифровых объектов
"цифрового правительства"
и критически важных
цифровых объектов
Форма

Перечень данных об инциденте кибербезопасности

Дата регистрации инцидента КБ	
Уровень критичности инцидента КБ *	Высокий (4); Средний (3); Низкий (2); Не определено (1).
Тип инцидента КБ	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 КБ	
Последствие	Без последствий; Нарушение работоспособности; Нарушение целостности; Нарушение режима конфиденциальности информации.
Объект, которому нанесен ущерб	
Действия, предпринятые для устранения инцидента КБ	
Примечание	

Уровни критичности инцидента кибербезопасности

Уровень критичности	**Признаки**	**Примеры инцидентов КБ**
Высокий (4)	Инциденты КБ, которые приводят к невозможности предоставления услуг/выполнения работ, и (или) потере/модификации критичных* данных, и (или) нарушению конфиденциальности цифрового объекта, обрабатывающего критичные* данные.	- Несанкционированный доступ - Эксплуатация уязвимости - Шифровальщик - Вредоносное ПО - Отказ в обслуживании (DoS/ DDoS-атака) и так далее.
Средний (3)	Инциденты КБ, которые приводят к существенному ограничению предоставления услуг/выполнения работ, и (или) потере/ модификации данных, не являющихся критичными*, и (или) нарушению конфиденциальности цифрового объекта, обрабатывающего данные, не являющихся критичными*.	- Несанкционированный доступ - Шифровальщик - Вредоносное ПО - Отказ в обслуживании (DoS/ DDoS-атака) - Эксплуатация уязвимости и так далее.
Низкий (2)	Инциденты КБ , не влияющие на предоставлениеуслуги/ выполнение работ.	- Вредоносное ПО - Отказ в обслуживании (DoS/DdoS-атака) - Эксплуатация уязвимости - Спам - Фишинговая атака и так далее.
Не определено (1)**	Влияние инцидента КБ 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 цифрового объекта.

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

Приложение 6
к Правилам проведения
мониторинга обеспечения
кибербезопасности

цифровых объектов
"цифрового правительства"
и критически важных
цифровых объектов
Форма

Перечень данных об уязвимости цифровых объекта "цифрового правительства"

Дата и время обнаружения уязвимости	Контур	Название цифрового объекта	Компонент цифрового объекта (название, IP, hostname и так далее)	Порт	Описание уязвимости	Дополнительная информация
1	2	3	4	5	6	7
	Внешний/ Внутренний контур					

Приложение 7
к Правилам проведения
мониторинга обеспечения
кибербезопасности цифровых объектов

"цифрового правительства"
и критически важных цифровых
объектов
Форма

Категории причин неустранения уязвимости и обоснование причины неустранения

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