О внесении изменений в приказ исполняющего обязанности 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"

Приказ Заместителя Премьер-Министра – Министра искусственного интеллекта и цифрового развития Республики Казахстан от 30 апреля 2026 года № 229/НҚ

Вводится в действие с 12 июля 2026 года.

ПРИКАЗЫВАЮ:

1. Внести в приказ исполняющего обязанности 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 Реестре нормативных правовых актов № 19286) следующие изменения:

заголовок приказа изложить в следующей редакции:

"Об утверждении Правил проведения мониторинга событий кибербезопасности цифровых объектов государственных органов";

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 6) статьи 7-1 Закона Республики Казахстан "О кибербезопасности" **ПРИКАЗЫВАЮ**:";

Правила проведения мониторинга событий информационной безопасности объектов информатизации государственных органов, утвержденных настоящим 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 порядке обеспечить:

1) направление настоящего приказа в электронном виде на казахском и русском языках в течение пяти рабочих дней со дня его подписания в Республиканское государственное предприятие на праве хозяйственного ведения "Институт законодательства и правовой информации Республики Казахстан" Министерства юстиции Республики Казахстан для включения в Эталонный контрольный банк нормативных правовых актов Республики Казахстан;

2) размещение настоящего приказа на интернет-ресурсе Министерства искусственного интеллекта и цифрового развития Республики Казахстан.

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

4. Настоящий приказ вводится в действие с 12 июля 2026 года и подлежит официальному опубликованию.

Заместитель Премьер Министра –
Министр искусственного интеллекта и
цифрового развития Республики Казахстан *Ж. Мадиев*

"СОГЛАСОВАН"
Комитет национальной безопасности
Республики Казахстан

Приложение к приказу

Правила проведения мониторинга событий кибербезопасности цифровых объектов государственных органов

Глава 1. Общие положения

1. Настоящие Правила проведения мониторинга событий кибербезопасности цифровых объектов государственных органов (далее - Правила) разработаны в соответствии с подпунктом 6) статьи 7-1 Закона Республики Казахстан "О кибербезопасности" (далее – Закон) и определяют порядок проведения мониторинга событий кибербезопасности цифровых объектов государственных органов.

2. В настоящих Правилах используются следующие понятия и определения:

1) государственная техническая служба (далее – АО "ГТС") – акционерное общество, созданное по решению Правительства Республики Казахстан;

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

3) инцидент кибербезопасности (далее – инцидент КБ) - отдельно или серийно возникающие сбои в работе цифровой инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования цифровых ресурсов;

4) кибербезопасность в сфере цифровизации (далее - кибербезопасность) - состояние защищенности цифровых ресурсов, цифровых систем и цифровой инфраструктуры от внешних и внутренних угроз;

5) координатор кибербезопасности – работник АО "ГТС", располагающийся на постоянной основе в государственном органе и осуществляющий координацию мероприятий, направленных на поддержание состояния защищенности цифровых объектов государственных органов;

6) мониторинг событий кибербезопасности - постоянное наблюдение за цифровым объектом с целью выявления и идентификации событий кибербезопасности;

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

8) 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;

9) цифровые объекты - цифровые ресурсы, программное обеспечение, интернет-ресурс и цифровая инфраструктура;

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

3. Мониторинг событий кибербезопасности цифровых объектов государственных органов (далее – МСКБ) проводится АО "ГТС", реализующим задачи и функции Национального координационного центра кибербезопасности (далее – НКЦКБ).

4. Объектами МСКБ являются цифровые объекты государственного органа (далее – ГО).

5. К объектам МСКБ не относятся:

1) цифровые ресурсы, содержащие сведения, составляющие государственные секреты;

2) цифровые 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) цифровые объекты Национального Банка Республики Казахстан, не интегрируемые с объектами цифровой инфраструктуры "цифрового правительства".

6. В рамках МСКБ источниками событий КБ являются:

1) средства защиты информации в цифровой инфраструктуре (далее – ЦИ) объектов МСКБ, в том числе, устанавливаемые и сопровождаемые АО "ГТС" (далее – источники событий КБ);

2) система управления событиями КБ НКЦКБ.

7. МСКБ включает в себя следующие виды работ:

1) установку источников событий КБ в ЦИ объектов МСКБ;

2) техническое сопровождение источников событий КБ в ЦИ объектов МСКБ;

3) отслеживание событий КБ объектов МСКБ с целью обнаружения инцидентов КБ и последующего на них реагирования.

8. МСКБ проводится по одному из следующих вариантов:

1) по одному виду работ;

2) по нескольким видам работ.

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

Глава 2. Порядок проведения мониторинга событий кибербезопасности цифровых объектов государственных органов

10. При проведении МСКБ АО "ГТС" осуществляет:

1) в рамках установки источников событий КБ:

изучение ЦИ объектов МСКБ;

развертывание аппаратно-программного комплекса источников событий КБ в ЦИ объектов МСКБ;

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

2) в рамках технического сопровождения источников событий КБ:

установку обновлений источников событий КБ по мере их выпуска производителем ;

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

отработку заявок от ГО по вопросам функционирования источников событий КБ;

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

определение перечня журналов регистрации событий, необходимых для передачи в систему управления событиями КБ НКЦКБ;

организацию журналирования событий источников событий КБ, сопровождаемых АО "ГТС";

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

организацию сбора журналов регистрации событий объектов МСКБ и источников событий КБ в систему сбора журналов регистрации событий НКЦК;

организацию передачи журналов регистрации событий объектов МСКБ и источников событий КБ в систему управления событиями КБ НКЦКБ, их обработку и анализ с целью выявления событий КБ и инцидентов КБ;

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

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

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

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

направление, при необходимости, к месту размещения объектов МСКБ работника АО "ГТС" в рамках реагирования на инцидент КБ (необходимость определяется КНБ РК или АО "ГТС" самостоятельно);

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

11. Координатор кибербезопасности осуществляет:

изучение цифровой инфраструктуры ГО в целях формирования рекомендаций по повышению уровня защищенности ЦО ГО;

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

координирование мероприятий по реагированию на инциденты КБ, выявленных в цифровой инфраструктуре ГО;

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

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

12. ГО или уполномоченное им лицо при проведении МСКБ:

предоставляют физический и сетевой доступ сотрудникам АО "ГТС" к цифровой 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 МСКБ и источников событий КБ в систему управления событиями КБ НКЦКБ;

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 КБ и (или) о мерах, принятых по устранению инцидента КБ, в течение 48 часов с момента получения уведомления от АО "ГТС" о выявлении события КБ или инцидента КБ соответственно.

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

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

Приложение
к Правилам проведения
мониторинга событий
кибербезопасности
цифровых объектов
государственных органов

Сведения об объекте МСКБ

№	Наименование государственного органа	Структурное подразделение (департамент)	Физическое месторасположение (этаж, кабинет)	Ф И О 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							