Об утверждении Правил проведения мониторинга событий информационной безопасности объектов информатизации государственных органов

Приказ и.о. Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 16 августа 2019 года № 199/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 23 августа 2019 года № 19286.

В соответствии с подпунктом 5-1) 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 событий информационной безопасности объектов информатизации государственных органов.

2. Комитету по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности 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 настоящего приказа направление его на казахском и русском языках в Республиканское государственное предприятие на праве хозяйственного ведения "Институт законодательства и правовой информации Республики Казахстан" для официального опубликования и включения в Эталонный контрольный банк нормативных правовых актов Республики Казахстан;

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

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

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

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

и.о. Министра цифрового развития,
инноваций и аэрокосмической промышленности
Республики Казахстан

"СОГЛАСОВАН"
Комитет национальной безопасности
Республики Казахстан

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

Правила проведения мониторинга событий информационной безопасности объектов информатизации государственных органов

Сноска. Правила - 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).

Глава 1. Общие положения

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

2. В настоящих Правилах используются следующие понятия и определения:

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

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

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

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

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

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

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

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

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

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

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

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

5. К объектам МСИБ не относятся:

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

2) информационные системы в защищенном исполнении, отнесенные к государственным секретам в соответствии с законодательством Республики Казахстан

о государственных секретах, а также сети телекоммуникаций специального назначения и/или правительственной, засекреченной, шифрованной и кодированной связи;

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

6. В рамках МСИБ источниками событий ИБ являются:

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

система управления событиями ИБ НКЦИБ.

7. МСИБ включает в себя следующие виды работ:

1) установку источников событий ИБ в ИКИ объектов МСИБ;

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

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

8. МСИБ проводится по одному из следующих вариантов:

1) по одному виду работ;

2) по нескольким видам работ.

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

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

10. При проведении МСИБ АО "ГТС" осуществляет:

1) в рамках установки источников событий ИБ:

изучение ИКИ объектов МСИБ;

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

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

2) в рамках технического сопровождения источников событий ИБ:

установку обновлений источников событий ИБ по мере их выпуска производителем ;

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

отработку заявок от ГО по вопросам функционирования источников событий ИБ;

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

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

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

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

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

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

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

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

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

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

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

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

11. Координатор информационной безопасности осуществляет:

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

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

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

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

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

12. ГО или уполномоченное им лицо при проведении МСИБ:

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

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

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

осуществляют обновление до актуальных версий пользовательских и серверных операционных систем;

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

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

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

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

Сведения об объекте МСИБ

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