О внесении изменений и дополнений 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 цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 23 апреля 2025 года № 175/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 24 апреля 2025 года № 36014

ПРИКАЗЫВАЮ:

1. Внести в приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан 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 за № 17019), следующие изменения и дополнение:

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

в пункте 2:

подпункт 3) изложить в следующей редакции:

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

подпункт 13) изложить в следующей редакции:

"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";";

пункты 4, 5 и 6 изложить в следующей редакции:

"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.

5. МОИБ проводится по одному из следующих вариантов:

1) по одному виду работ;

2) по нескольким видам работ;

3) в полном составе видов работ.

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

пункты 8 и 9 изложить в следующей редакции:

"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).

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

пункты 10, 11, 12, 13, 14, 15, 16 и 17 изложить в следующей редакции:

"10. АО "ГТС" при проведении МОИБ осуществляет:

1) в рамках мониторинга реагирования на инциденты ИБ:

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

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

сбор 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.

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.

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.

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.

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.

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.

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.

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.";

пункты 19 и 20 изложить в следующей редакции:

"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.

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";

пункт 22 изложить в следующей редакции:

"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.";

пункт 24 изложить в следующей редакции:

"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.";

приложение 1 к указанному приказу изложить в новой редакции согласно приложению 1 к настоящему приказу;

приложения 1 и 2 к Сведениям об объекте информатизации "электронного правительства" исключить;

приложение 2 к указанному приказу изложить в новой редакции согласно приложению 2 к настоящему приказу;

дополнить приложением 7 согласно приложению 3 к настоящему приказу.

2. Комитету по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности 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 цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан после его официального опубликования;

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

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

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

исполняющий обязанности
Министра цифрового развития, инноваций
и аэрокосмической промышленности
Республики Казахстан *К. Тулеушин*

Приложение 1 к приказу
исполняющий обязанности
Министра цифрового развития,
инноваций и аэрокосмической
промышленности
Республики Казахстан
от 23 апреля 2025 года
№ 175/НҚ

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"

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 2 к приказу
исполняющий обязанности
Министра цифрового развития,
инноваций и аэрокосмической
промышленности
Республики Казахстан
от 23 апреля 2025 года
№ 175/НҚ

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

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 приказу
исполняющий обязанности
Министра цифрового развития,
инноваций и аэрокосмической
промышленности
Республики Казахстан
от 23 апреля 2025 года
№ 175/НҚ

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

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	