О внесении изменений в приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 1 апреля 2024 года № 185/НҚ "Об утверждении Правил функционирования программы взаимодействия с исследователями информационной безопасности"

Приказ Заместителя Премьер-Министра – Министра искусственного интеллекта и цифрового развития Республики Казахстан от 3 июля 2026 года № 378/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 7 июля 2026 года № 39234

ПРИКАЗЫВАЮ:

1. Внести в приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 1 апреля 2024 года № 185/НҚ "Об утверждении Правил функционирования программы взаимодействия с исследователями информационной безопасности" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 34211) следующие изменения:

заголовок изложить в следующей редакции:

"Об утверждении Правил функционирования программы взаимодействия с исследователями кибербезопасности";

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 24) статьи 7-1 Закона Республики Казахстан "О кибербезопасности" **ПРИКАЗЫВАЮ**:";

пункт 1 изложить в следующей редакции:

"1. Утвердить прилагаемые Правила функционирования программы взаимодействия с исследователями кибербезопасности."

Правила функционирования программы взаимодействия с исследователями кибербезопасности, 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.

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

"СОГЛАСОВАН"
Комитет национальной безопасности
Республики Казахстан

Приложение к приказу
Заместитель Премьер-Министра
–Министр искусственного
интеллекта и цифрового развития
Республики Казахстан
от 3 июля 2026 года № 378/НҚ

Правила функционирования программы взаимодействия с исследователями кибербезопасности

Глава 1. Общие положения

1. Настоящие Правила функционирования программы взаимодействия с исследователями кибербезопасности (далее – Правила) разработаны в соответствии с подпунктом 24) статьи 7-1 Закона Республики Казахстан "О кибербезопасности" (далее – Закон) и определяют порядок функционирования программы взаимодействия с исследователями кибербезопасности (далее – ПВ ИКБ).

2. В настоящих Правилах используются следующие понятия:

1) исследователь кибербезопасности – специалист в сфере обеспечения кибербезопасности, участвующий в программе взаимодействия с исследователями кибербезопасности;

2) программа взаимодействия с исследователями кибербезопасности – организационно-технические мероприятия, обеспечивающие взаимодействие исследователей кибербезопасности с цифровыми объектами для выявления в них уязвимостей;

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

4) оператор программы взаимодействия с исследователями кибербезопасности по цифровым объектам государственных органов (далее – оператор) – Государственный оперативный центр кибербезопасности, обеспечивающий функционирование программы взаимодействия по цифровым объектам государственных органов (далее – ЦО ГО);

5) государственная техническая служба – государственное юридическое лицо, созданное по решению Правительства Республики Казахстан;

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

7) отчет об уязвимости (далее – отчет) – сведения о выявленной исследователем КБ уязвимости в цифровом объекте;

8) токен – уникальное строковое значение;

9) цифровой объект (далее – ЦО) – 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;

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

Глава 2. Порядок функционирования программы взаимодействия с исследователями кибербезопасности

3. Задачи и функции Государственного оперативного центра кибербезопасности, как оператора, в соответствии с подпунктом 6) пункта 1 статьи 7-4, подпунктом 3) пункта 1 статьи 9 и подпунктом 5) пункта 1 статьи 14 Закона реализует Государственная техническая служба (акционерное общество "Государственная техническая служба", далее – АО "ГТС"), обеспечивающая функционирование ПВ ИКБ по ЦО ГО на собственной цифровой инфраструктуре.

4. Обеспечение функционирования ПВ ИКБ по ЦО ГО осуществляется на основании договорных отношений между Комитетом национальной безопасности Республики Казахстан (далее – КНБ РК) и АО "ГТС".

5. Уполномоченный орган для формирования списка ЦО ГО, подлежащих к подключению к ПВ ИКБ по ЦО ГО, направляет запрос собственникам или владельцам ЦО ГО для предоставления сведений по ЦО ГО, имеющим доступ к Интернету (далее – запрос).

6. Собственники или владельцы ЦО ГО направляют уполномоченному органу сведения по ЦО ГО, имеющим доступ к Интернету, информацию, содержащую наименования ЦО ГО и сроки поиска уязвимостей в нем в течение 10 (десять) рабочих дней со дня поступления запроса.

7. Уполномоченный орган на основе предоставленных сведений от собственников или владельцев ЦО ГО формирует список ЦО ГО, подлежащих к подключению к ПВ ИКБ по ЦО ГО, и сроки поиска уязвимостей в ЦО ГО (далее – список) в течение 10 (десять) рабочих дней.

8. Уполномоченный орган направляет список оператору в течение 3 (три) рабочих дней со дня формирования списка.

9. Оператор уведомляет собственников или владельцев ЦО ГО согласно списку о подключении к ПВ ИКБ по ЦО ГО в течение 3 (три) рабочих дней со дня получения списка.

10. Собственники или владельцы ЦО ГО принимают меры, обеспечивающие подключение ЦО к ПВ ИКБ по ЦО ГО, за исключением ЦО, не имеющих доступ к Интернету в соответствии с подпунктом 1) пункта 3 статьи 54 Закона.

11. Собственники или владельцы ЦО ГО, для подключения к ПВ ИКБ по ЦО ГО, в течение 10 (десять) рабочих дней со дня получения уведомления о подключении разрабатывают и утверждают порядок исследования, в котором определяют границы исследования ЦО ГО, предусматривающего минимальный объем тестирования, а также уровни критичности уязвимостей, перечень уязвимостей, которые не принимаются для рассмотрения, а также действия, недопустимые в отношении ЦО ГО при поиске уязвимостей.

12. Собственники или владельцы ЦО ГО направляют оператору порядок исследования в течение 2 (два) рабочих дней со дня его утверждения.

Оператор размещает порядок исследования в ПВ ИКБ по ЦО ГО в течение 2 (два) рабочих дней со дня его получения.

13. Исследователь КБ регистрируется в ПВ ИКБ по ЦО ГО и получает токен, которым исследователю КБ необходимо маркировать трафик, запрос, параметр при поиске уязвимостей в ЦО ГО.

14. Исследователь КБ не может разглашать токен третьим лицам и использовать токены третьих лиц.

15. При исследовании ЦО ГО на наличие уязвимостей исследователь КБ не может:

1) исследовать IP-адреса и доменные имена, не указанные в ПВ ИКБ по ЦО ГО;

2) использовать инструменты для автоматического сканирования ЦО за исключением случаев, согласованных собственником или владельцем ЦО ГО;

3) осуществлять попытку эксплуатации уязвимости, за исключением минимального объема тестирования, указанного в порядке исследования и необходимого для

доказательства существования уязвимости или выявления индикатора, связанного с уязвимостью;

4) осуществлять преднамеренный доступ к содержимому любых сообщений, данных или информации, передаваемых или хранящихся в ЦО ГО, за исключением случаев, когда информация напрямую связана с уязвимостью и доступ необходим для доказательства существования уязвимости;

5) осуществлять выгрузку, хранение, раскрытие, передачу, модификацию, удаление каких-либо данных или информации, к которым получен доступ в ходе проведения исследования;

6) раскрывать какие-либо сведения об уязвимости ЦО ГО или содержании информации, получаемой через эксплуатацию уязвимости, за исключением случая получения письменного разрешения от собственника или владельца ЦО ГО;

7) совершать попытки получения доступа к учетным записям пользователей ЦО ГО, за исключением случая, когда они предоставлены исследователю КБ собственником или владельцем ЦО ГО для проведения исследования;

8) применять методы физического вмешательства в ЦО ГО;

9) использовать методы социальной инженерии в отношении работников или подрядчиков собственника, или владельца ЦО ГО или оператора.

16. Если эксплуатация найденной уязвимости может привести к нарушению целостности и доступности ЦО ГО, исследователю КБ необходимо воздержаться от действий по эксплуатации данной уязвимости и указать в отчете данные, необходимые для проверки найденной уязвимости.

17. Исследователь КБ направляет отчет оператору посредством ПВ ИКБ по ЦО ГО в соответствии с формой, размещенной в ПВ ИКБ по ЦО ГО.

18. Оператор в течение 15 (пятнадцать) рабочих дней со дня поступления отчета проверяет его на достоверность и готовит заключение о наличии или отсутствии уязвимости в ЦО ГО.

19. Оператор при проверке отчета, при необходимости, запрашивает у исследователя КБ дополнительные сведения, подтверждающие наличие уязвимости в ЦО ГО.

20. При не подтверждении достоверности отчета оператор в течение 5 (пять) рабочих дней после проверки отчета направляет исследователю КБ заключение об отсутствии уязвимости в ЦО ГО посредством ПВ ИКБ по ЦО ГО.

21. При подтверждении достоверности отчета оператор в течение 5 (пять) рабочих дней после проверки отчета посредством ПВ ИКБ по ЦО ГО:

1) направляет уведомление собственнику или владельцу ЦО ГО о наличии уязвимости в ЦО ГО (далее – уведомление об уязвимости) и направляет ему отчет;

2) уведомляет уполномоченный орган о наличии уязвимости в ЦО ГО;

3) информирует исследователя КБ о результатах проверки.

22. Оператор не направляет отчет собственнику или владельцу ЦО ГО и в уполномоченный орган при:

1) не подтверждении оператором достоверности отчета;

2) подтверждении оператором наличия идентичной уязвимости до направления отчета исследователем КБ.

23. Собственник или владелец ЦО ГО принимают меры, обеспечивающие устранение выявленных уязвимостей, зарегистрированных в ПВ ИКБ по ЦО ГО в соответствии с подпунктом 2) пункта 3 статьи 54 Закона.

24. Собственник или владелец ЦО ГО в течение 15 (пятнадцать) рабочих дней со дня получения уведомления об уязвимости:

1) устраняет уязвимость и направляет сведения об ее устранении оператору посредством ПВ ИКБ по ЦО ГО;

2) при невозможности устранения уязвимости направляет оператору и уполномоченному органу посредством ПВ ИКБ по ЦО ГО сведения о не устранении уязвимости в ЦО ГО, которые содержат:

обоснование не устранения уязвимости и характер требуемых изменений в ЦО ГО;

меры, направленные на минимизацию рисков эксплуатации выявленной уязвимости ;

сроки устранения уязвимости, не превышающие 6 (шесть) месяцев с момента первого обнаружения.

25. Оператор после истечения срока устранения уязвимости, определенного пунктом 24 настоящих Правил, проверяет ЦО ГО на устранение уязвимости в течение 5 (пять) рабочих дней.

При не устранении собственником или владельцем ЦО ГО уязвимости в ЦО ГО оператор уведомляет об этом посредством ПВ ИКБ по ЦО ГО уполномоченный орган и КНБ РК в течение 1 (один) рабочего дня после завершения срока проверки.

26. При нарушении исследователем КБ пунктов 13, 14, 15, 16 и 17 настоящих Правил и порядка исследования оператор блокирует учетную запись исследователя КБ в ПВ ИКБ по ЦО ГО.