Об утверждении Правил функционирования программы взаимодействия с исследователями информационной безопасности

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 1 апреля 2024 года № 185/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 2 апреля 2024 года № 34211

Примечание ИЗПИ!

Порядок введения в действие см. п. 4.

В соответствии с подпунктом 20-4) статьи 7-1 Закона Республики Казахстан "Об информатизации" ПРИКАЗЫВАЮ:

1. Утвердить прилагаемые Правила функционирования программы взаимодействия с исследователями информационной безопасности.

2. Комитету по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан в установленном законодательством 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;

3) 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) 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 шестидесяти календарных дней со дня его первого официального опубликования.

Министр цифрового развития, инноваций
и аэрокосмической промышленности
Республики Казахстан *Б. Мусин*

"СОГЛАСОВАН"
Комитет национальной безопасности
Республики Казахстан

Утверждены приказом

Министр цифрового развития,
инноваций и аэрокосмической
промышленности
Республики Казахстан
от 1 апреля 2024 года
№ 185/НҚ

Правила функционирования программы взаимодействия с исследователями информационной безопасности

Глава 1. Общие положения

1. Настоящие Правила функционирования программы взаимодействия с исследователями информационной безопасности (далее – Правила) разработаны в соответствии с подпунктом 20-4) статьи 7-1 Закона Республики Казахстан "Об информатизации" (далее – Закон) и определяют порядок функционирования программы взаимодействия с исследователями информационной безопасности по объектам информатизации государственных органов (далее – ПВ ИИБ по ОИ ГО).

2. В настоящих Правилах используются следующие основные понятия:

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

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

3) исследователь информационной безопасности (далее – исследователь ИБ) – специалист в сфере обеспечения информационной безопасности и (или) информационно-коммуникационных технологий, зарегистрированный в программе взаимодействия с исследователями информационной безопасности, исследующий объекты информатизации, подключенные к программе взаимодействия с исследователями информационной безопасности, для выявления уязвимостей;

4) программа взаимодействия с исследователями информационной безопасности (далее – ПВ ИИБ) – объект информатизации, предназначенный для регистрации исследователей информационной безопасности, регистрации выявленных уязвимостей, а также для обеспечения взаимодействия исследователей информационной безопасности с объектами информатизации;

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

6) государственная техническая служба – акционерное общество, созданное по решению Правительства Республики Казахстан;

7) оператор программы взаимодействия с исследователями информационной безопасности по объектам информатизации государственных органов (далее – оператор) – Государственный оперативный центр информационной безопасности, обеспечивающий функционирование программы взаимодействия по объектам информатизации государственных органов (далее – ОИ ГО);

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

9) отчет об уязвимости (далее – отчет) – сведения о выявленной исследователем ИБ уязвимости в объекте информатизации;

10) токен – уникальное строковое значение.

Глава 2. Порядок функционирования программы взаимодействия с исследователями информационной безопасности по объектам информатизации государственных органов

3. Задачи и функции Государственного оперативного центра информационной безопасности, как оператора, в соответствии с подпунктом 6) пункта 1 статьи 7-8, подпунктом 3) пункта 1 статьи 7-4 и подпунктом 15) пункта 1 статьи 14 Закона реализует государственная техническая служба (акционерное общество " Государственная техническая служба", далее – АО "ГТС"), обеспечивающая функционирование ПВ ИИБ по ОИ ГО на собственной информационно-коммуникационной инфраструктуре.

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

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

6. Собственники или владельцы ОИ ГО направляют уполномоченному органу сведения по ОИ ГО, имеющим доступ к Интернету, в виде наименований ОИ ГО и сроков 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 ОИ ГО формирует список ОИ ГО, подлежащих к подключению к ПВ ИИБ по ОИ ГО, и сроки поиска уязвимостей в ОИ 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 ОИ ГО согласно списку о необходимости подключения к ПВ ИИБ по ОИ ГО (далее – уведомление о подключении) в течение 3 (три) рабочих дней со дня получения списка.

10. Собственники или владельцы ОИ ГО обязаны принимать меры, обеспечивающие подключение ОИ к ПВ ИИБ по ОИ ГО, за исключением ОИ, не имеющих доступ к Интернету в соответствии с подпунктом 1) пункта 2-1 статьи 54 Закона.

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

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

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

13. Исследователь ИБ регистрируется в ПВ ИИБ по ОИ ГО и получает токен, которым исследователю ИБ необходимо маркировать трафик, запрос, параметр при поиске уязвимостей в ОИ ГО.

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

15. При исследовании ОИ ГО на наличие уязвимостей исследователь ИБ не может:

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

2) использовать инструменты для автоматического сканирования ОИ за исключением случаев, согласованных собственником или владельцем ОИ 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 ОИ 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 ОИ ГО или содержании информации, получаемой через эксплуатацию уязвимости, за исключением случая получения письменного разрешения от собственника или владельца ОИ ГО;

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

8) применять методы физического вмешательства в ОИ ГО;

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

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

17. Исследователь ИБ направляет отчет оператору посредством ПВ ИИБ по ОИ ГО в соответствии с формой, размещенной в ПВ ИИБ по ОИ 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 ОИ ГО.

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

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

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

1) уведомляет собственника или владельца ОИ ГО о наличии уязвимости в ОИ ГО (далее – уведомление об уязвимости) и направляет ему отчет;

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

3) информирует исследователя ИБ о результатах проверки.

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

1) не подтверждении оператором достоверности отчета;

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

23. Собственник или владелец ОИ ГО обязан принимать меры, обеспечивающие устранение выявленных уязвимостей, зарегистрированных в ПВ ИИБ по ОИ ГО в соответствии с подпунктом 2) пункта 2-1 статьи 54 Закона.

24. Собственник или владелец ОИ 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 ИИБ по ОИ ГО;

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

обоснование неустранения уязвимости и характер требуемых изменений в ОИ 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 ОИ ГО на устранение уязвимости в течение 5 (пять) рабочих дней.

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

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