О внесении изменений и дополнений в приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 года № 111/НҚ "Об утверждении методики и правил проведения испытаний объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры на соответствие требованиям информационной безопасности"

Приказ Заместителя Премьер-Министра – Министра искусственного интеллекта и цифрового развития Республики Казахстан от 27 ноября 2025 года № 602/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 28 ноября 2025 года № 37495

ПРИКАЗЫВАЮ:

1. Внести в приказ Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 года № 111/НҚ "Об утверждении методики и правил проведения испытаний объектов информатизации " электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры на соответствие требованиям информационной безопасности" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 18795) следующие изменения и дополнения:

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 5) статьи 7-1 Закона Республики Казахстан "Об информатизации" и подпунктом 52) пункта 15 Положения о Министерстве искусственного интеллекта и цифрового развития Республики Казахстан, утвержденного постановлением Правительства Республики Казахстан от 9 октября 2025 года № 846, **ПРИКАЗЫВАЮ**:".

в Методике проведения испытаний объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры на соответствие требованиям информационной безопасности, утвержденной указанным приказом:

пункт 1 изложить в следующей редакции:

"1. Настоящая Методика проведения испытаний объектов информатизации " электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры на соответствие требованиям информационной безопасности (далее – Методика) разработана в соответствии с подпунктом 5) статьи 7-1 Закона Республики Казахстан "Об информатизации" и

подпунктом 52) пункта 15 Положения о Министерстве искусственного интеллекта и цифрового развития Республики Казахстан, утвержденного постановлением Правительства Республики Казахстан от 9 октября 2025 года № 846.";

пункт 4 изложить в следующей редакции:

"4. Анализ исходных кодов объектов испытаний проводится с целью выявления уязвимостей ПО в соответствии с международными классификациями уязвимостей (Common Weakness Enumeration, Open Web Application Security Project Top 10, Open Web Application Security Project Mobile Top 10, Open Web Application Security Project Application Programming Interface Top 10), международными базами данных уязвимостей (Common Vulnerabilities and Exposures, National Institute of Standards and Technology) и стандартом Республики Казахстан 15408-3 "Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты".

Анализ исходных кодов объектов испытаний, собственником (владельцем) и (или) заказчиком которых является государственный орган проводится с целью выявления НДВ и уязвимостей ПО в соответствии с международными классификациями (Common Weakness Enumeration, Open Web Application Security Project Top 10, Open Web Application Security Project Mobile Top 10, Open Web Application Security Project Application Programming Interface Top 10), международными базами данных уязвимостей (Common Vulnerabilities and Exposures, National Institute of Standards and Technology) и стандартом Республики Казахстан 15408-3 "Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования к обеспечению защиты".";

пункт 7 изложить в следующей редакции:

"7. Выявление уязвимостей ПО проводится с использованием программного средства, предназначенного для анализа исходного кода, на основании исходных кодов, предоставленных заявителем.

Выявление уязвимостей ПО объектам испытаний, собственником (владельцем) и (или) заказчиком которых является государственный орган проводится ручным методом анализа исходного кода и с использованием программного средства, предназначенного для анализа исходного кода, на основании исходных кодов, предоставленных заявителем.";

подпункт 2) пункта 11 изложить в следующей редакции:

"2) проведение анализа исходного кода ручным методом объекта испытания:

изучение модульной и логической структуры ПО, а также отдельных модулей и сравнения этих структур с приведенными в технической документации;

изучение маршрута выполнения функциональных объектов и проверка обрабатывающих данных;

контроль полноты и отсутствия избыточности исходных кодов на уровне функциональных объектов;

фиксирование НДВ с помощью снимка экрана для последующего предоставления в отчете результатов выявления НДВ;";

пункт 14 изложить в следующей редакции:

"14. По окончанию анализа исходных кодов:

1) исходные коды объекта испытаний (за исключением объектов информатизации, собственником (владельцем) и (или) заказчиком которых является государственный орган) маркируются и сдаются в опечатанном виде на ответственное хранение в архиве аккредитованной испытательной лаборатории;

2) исходные коды объекта испытаний (объекта информатизации, собственников (владельцем) и (или) заказчиком которых является государственный орган) получают уникальный идентификационный номер и хранятся в интернет-портале SYNAQ.";

в Правилах проведения испытаний объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры на соответствие требованиям информационной безопасности, утвержденных указанным приказом:

пункт 1 изложить в следующей редакции:

"1. Настоящие Правила проведения испытаний объектов информатизации " электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры на соответствие требованиям информационной безопасности (далее – Правила) разработаны в соответствии с подпунктом 5) статьи 7-1 Закона Республики Казахстан "Об информатизации" (далее – Закон), подпунктом 52) пункта 15 Положения о Министерстве искусственного интеллекта и цифрового развития Республики Казахстан, утвержденного постановлением Правительства Республики Казахстан от 9 октября 2025 года № 846 и определяют порядок проведения испытаний объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры на соответствие требованиям информационной безопасности.";

подпункт 8) пункта 2 изложить в следующей редакции:

"8) исходные коды – исходные тексты компьютерных программ компонентов и модулей объекта испытаний с библиотеками и файлами, необходимыми для успешной компиляции объекта испытаний;";

пункт 5 изложить в следующей редакции:

"5. При отсутствии исходного кода объекта испытания или невозможности проведения другого(их) вида(ов) испытаний (за исключением объектов информатизации, собственником (владельцем) и (или) заказчиком которых является

государственный орган), решение о необязательности проведения анализа исходного кода или другого(их) вида(ов) испытаний объекта испытаний устанавливается решением уполномоченного органа в сфере обеспечения информационной безопасности по запросу заявителя.

Уполномоченный орган в сфере обеспечения информационной безопасности направляет запрос поставщику о проверке обоснованности запроса заявителя об исключении анализа исходного кода или другого(их) вида(ов) испытаний объекта испытаний в период проведения испытаний по другим видам согласно пункту 4 настоящих Правил.";

пункт 7 изложить в следующей редакции:

"7. В испытания информационно-коммуникационной платформы "электронного правительства" входит:

1) анализ исходных кодов;

2) испытание функций информационной безопасности;

3) нагрузочное испытание;

4) обследование сетевой инфраструктуры;

5) обследование процессов обеспечения ИБ.";

пункт 8 исключить;

пункт 24 изложить в следующей редакции:

"24. Для расчета стоимости проведения испытаний заявитель направляет в государственную техническую службу анкету-вопросник о характеристиках объекта испытаний, удостоверенную ЭЦП собственника (владельца) объекта испытаний и техническое задание на создание (техническое задание на развитие, дополнение к техническому заданию при наличии) объекта информатизации на интернет-портале SYNAQ.";

пункт 28 исключить;

пункт 36 изложить в следующей редакции:

"36. Срок действия протоколов испытаний выдается сроком на 3 (три) года для всех объектов испытаний, за исключением информационно-коммуникационной платформы "электронного правительства", или после изменения условий функционирования и (или) функциональности, и (или) изменения прав собственности и (или) владения объекта испытаний.

При этом, срок действия протокола по отдельному виду испытания для ввода в промышленную эксплуатацию объекта информатизации не превышает одного года с даты выдачи протокола.

Собственник или владелец объекта информатизации за 3 (три) месяца до окончания срока действия протоколов испытаний подает заявку поставщику о прохождении испытаний в порядке, установленном главами 2 или 3 настоящих Правил.

Протоколы испытаний информационно-коммуникационной платформы " электронного правительства" выдаются со сроком действия 1 (один) год.";

пункт 37 изложить в следующей редакции:

"37. Поставщик на постоянной основе предоставляет в уполномоченный орган в сфере обеспечения информационной безопасности следующие данные:

1) заявка на проведение испытаний;

2) информацию о договоре на проведение испытаний в испытательных лабораториях (дата, номер);

3) наименование объекта испытаний;

4) наименование собственника и (или) владельца объекта испытаний;

5) реестровый номер, дата выдачи и протокол испытаний на соответствие требованиям информационной безопасности по каждому виду работ с указанием результата;

6) фактическое местоположение сетевого и серверного оборудования объекта испытаний;

7) анкета-вопросник о характеристиках объекта испытаний, утвержденная собственником или владельцем объекта испытаний.

Аккредитованная испытательная лаборатория обеспечивает внесение вышеуказанных данных в интернет-портал уполномоченного органа в сфере обеспечения информационной безопасности или при наличии собственного интернет-портала предоставляет доступ в личный кабинет уполномоченному органу в сфере обеспечения информационной безопасности.

Информация в виде отчета формируется с использованием ЭЦП аккредитованной испытательной лаборатории.

Государственная техническая служба для передачи вышеуказанных данных, обеспечивает интеграцию интернет-портала SYNAQ с интернет-порталом уполномоченного органа в сфере обеспечения информационной безопасности или предоставляет доступ в личный кабинет на интернет-портале SYNAQ уполномоченному органу в сфере обеспечения информационной безопасности.

Поставщик предоставляет ежеквартальный отчет о проведенных и планируемых испытаниях в уполномоченный орган в сфере обеспечения информационной безопасности с предоставлением данных указанных в подпунктах 3), 4) и 5) пункта 37 настоящих Правил по системе электронного документооборота.";

пункт 38 изложить в следующей редакции:

"38. При изменении условий функционирования и (или) функциональности, и (или) изменении прав собственности объекта информатизации, собственник или владелец объекта информатизации после завершения работ, приведших к изменениям,

направляет поставщику уведомление с приложением описания всех произведенных изменений, прежней и обновленной анкеты-вопросника о характеристиках объекта испытаний, утвержденной собственником или владельцем объекта испытаний.

При принятии решений о проведении по одному (нескольким) виду испытаний, ранее выданный соответствующий протокол (протоколы) испытаний или акт испытаний прекращают свое действие.";

пункт 41 изложить в следующей редакции:

"41. При отзыве протоколов испытаний, собственник или владелец в трехмесячный срок подает заявку поставщикам о прохождении испытаний в порядке, установленном главами 2 или 3 настоящих Правил.";

подпункт 5) пункта 1 приложения 1 изложить в следующей редакции:

"5) _____

(перечень видов работ согласно пунктов 4,6,7 настоящих Правил

(указать нужный пункт)";

приложение 2 изложить в новой редакции согласно приложению 1 к настоящему приказу;

приложение 3 изложить в новой редакции согласно приложению 2 к настоящему приказу;

в приложении 4:

в Перечне изменений функционирования и (или) функциональности объекта информатизации:

строку, порядковый номер 10, изложить в следующей редакции:

"

10.	Изменение класса объекта информатизации	-	+	-	+	+

";

дополнить строкой, с порядковым номером 11, следующего содержания:

"

11.	Изменение прав собственности и (или) владения объекта информатизации (изменение собственника и/или владельца)	-	-	-	-	+

".

2. Комитету по информационной безопасности Министерства искусственного интеллекта и цифрового развития 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 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"
Агентство по регулированию и развитию
финансового рынка

"СОГЛАСОВАН"
Комитет национальной безопасности
Республики Казахстан

Приложение 1 к приказу
Заместитель Премьер-Министра –
Министр искусственного
интеллекта и цифрового развития
Республики Казахстан
от 27 ноября 2025 года
№ 602/НҚ

Приложение 2
к Правилам проведения
испытаний объектов
информатизации
"электронного правительства"
и критически важных объектов
информационно- коммуникационной
инфраструктуры на соответствие
требованиям информационной
безопасности

Форма

Анкета-вопросник о характеристиках объекта испытаний

1. Наименование объекта испытаний: _____
_____
2. Краткая аннотация на объект испытаний _____
_____
(назначение и область применения)
3. Классификация объекта испытаний:
1) класс прикладного программного обеспечения _____.
2) схема классификации по форме приложения 2 к Правилам классификации объектов информатизации, утвержденным приказом исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135 (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 13349).
4. Архитектура объекта испытаний:
1) функциональная схема объекта испытаний (при необходимости) с указанием:
компонентов, модулей объекта испытаний и их IP-адресов;
связей между компонентами или модулями и направления информационных потоков;
точки подключения интеграционного взаимодействия с другими объектами информатизации;
точки подключения пользователей;
мест и технологий хранения данных;
применяемого резервного оборудования;
разъяснения применяемых терминов и аббревиатур;
2) схема сети передачи данных объекта испытаний (при необходимости) с указанием:
архитектуры и характеристик сети;
серверного сетевого и коммуникационного оборудования;
адресации и применяемых сетевых технологий;
используемых локальных, ведомственных (корпоративных) и глобальных сетей;
решения(й) по обеспечению отказоустойчивости и резервированию;
разъяснения применяемых терминов и аббревиатур;
5. Информация об объекте испытаний:
1) информация о серверном оборудовании:

					Операционная система (далее - ОС), система	

№ п/п	Наименование сервера или виртуального ресурса (доменное имя, сетевое имя или логическое имя сервера)	Назначение (выполняемые функциональные задачи)	Количество	Характеристики сервера или используемых заявленных виртуальных ресурсов	управления базами данных (далее – СУБД), программное обеспечение (далее – ПО), приложения, библиотеки и средства защиты, установленные на серверах или используемые виртуальные сервисы (состав программной среды с указание номеров версий)	Применяемые IP-адреса
1	2	3	4	5	6	7

2) информация о сетевом оборудовании:

№ п/п	Наименование сетевого оборудования (марка/модель)	Назначение (выполняемые функциональные задачи)	Количество	Применяемые сетевые технологии	Применяемые технологии защиты сети	Используемые IP-адреса, в том числе, порт управления
1	2	3	4	5	6	7

3) местонахождение серверного и сетевого оборудования:

№ п/п	Владелец серверного помещения	Юридический адрес владельца серверного помещения	Фактическое местоположение – адрес серверного помещения	Ответственные лица за организацию доступа (фамилия, имя, отчество (при наличии)	Телефоны ответственных лиц (рабочие, сотовые)
1	2	3	4	5	6

4) характеристики резервного серверного оборудования:

	Наименование сервера или виртуальног	Назначение (		Характеристики	ОС, СУБД, ПО, приложения, библиотеки и средства защиты, установленные на		

№ п/п	о ресурса (доменное имя, сетевое имя или логическое имя сервера)	выполняемы е функциональные задачи)	Количество	сервера или используемы х заявленных виртуальных ресурсов	серверах и л и используемы е виртуальные сервисы (состав программной среды с указание номеров версий)	Применяемы е IP-адреса	Метод резервирования
1	2	3	4	5	6	7	8

5) характеристики резервного сетевого оборудования:

№ п/п	Наименование сетевого оборудования (марка/ модель)	Назначение (выполняемы е функциональные задачи)	Количество	Применяемые сетевые технологии	Применяемы е технологии защиты сети	Используемы е IP-адреса, в том числе порт управления	Метод резервирования
1	2	3	4	5	6	7	8

6) местонахождение резервного серверного и сетевого оборудования:

№ п/п	Владелец серверного помещения	Юридический адрес владельца серверного помещения	Фактическое местоположение – адрес серверного помещения	Ответственные лица за организацию доступа (фамилия, имя, отчество (при наличии)	Телефоны ответственных лиц (рабочие, сотовые)
1	2	3	4	5	6

7) структура сети объекта испытаний (при необходимости):

№ п/п	Наименование сегмента сети	IP-адрес сети/маска сети
1	2	3

8) информация по рабочим станциям администраторов:

№ п/п	Роль администратора	Количество учетных записей администраторов	Наличие доступа к Интернет	Наличие удаленного доступа к оборудованию	IP-адрес рабочей станции администратора	Фактическое местоположение – адрес рабочего места
1	2	3	4	5	6	7

9) информация о пользователях прикладного программного обеспечения, в том числе с применением мобильных и интернет приложений:

		Перечень типовых	Адрес и порт точки подключени	Протокол подключени	Количество пользователей согласно технической	Максимальное количество,	Максимальное время

№ п/п	Роль пользователя	действий пользователя	я пользователей к объекту испытаний	я пользователей к объекту испытаний	документации на создание или развитие объекта испытаний	обрабатываемых запросов (пакетов) в секунду	ожидания между запросами
1	2	3	4	5	6	7	8

10) Информация об интеграционном взаимодействии объекта испытаний, в том числе, планируемые:

№ п/п	Наименование интеграционной связи (объекта информатизации)	Собственник или владелец интегрируемого объекта	Действующая/планируемая	Наличие модуля интеграции	Адрес точки подключения	Протокол подключения	Максимальное количество запросов (пакетов) в секунду	Максимальное время ожидания между запросами
1	2	3	4	5	6	7	8	9

11) Исходные коды прикладного ПО (при необходимости):

№ п/п	Маркировка диска (при необходимости)	Наименование каталога/ Наименование каталога на диске	Наименование файла	Размер файла, Мбайт	Применяемый язык программирования (при необходимости)	Версия языка программирования	Применяемый фреймворк, версия фреймворка	Версия среды разработки	Дата модификации файла
1	2	3	4	5	6	7	8	9	10

12) Исходные коды и исполняемые файлы используемых библиотек и программных (ой) платформ(ы) (при необходимости):

№ п/п	Маркировка диска (при необходимости)	Наименование каталога/ Наименование каталога на диске	Наименование библиотеки/ программной платформы/ файла	Размер, Мбайт	Язык программирования (при необходимости)	Версия библиотеки
1	2	3	4	5	6	7

6. Документирование испытываемого объекта (при необходимости):

№ п/п	Наименование документа	Наличие	Количество страниц	Дата утверждения	Стандарт или нормативный документ, в соответствии с которым был разработан документ
1	2	3	4	5	6

1.	Политика информационной безопасности				
2.	Методика оценки рисков информационной безопасности				
3.	Правила идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации				
4.	Правила проведения внутреннего аудита информационной безопасности				
5.	Правила использования средств криптографической защиты информации				
6.	Правила организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам				
7.	Правила организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты				

8.	Правила организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации				
9.	Руководство администратора по сопровождению объекта информатизации, резервному копированию и восстановлению информации				
10.	Инструкцию о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях				

Приложение 2 к приказу
Заместитель Премьер-Министра –
Министр искусственного
интеллекта и цифрового развития
Республики Казахстан
от 27 ноября 2025 года
№ 602/НҚ

Приложение 3
к Правилам проведения
испытаний объектов
информатизации
"электронного правительства"
и критически важных объектов
информационно-коммуникационной

инфраструктуры на соответствие
требованиям информационной
безопасности
Форма

Перечень технической документации по информационной безопасности объекта испытаний

1. Политика информационной безопасности;
2. Методика оценки рисков информационной безопасности;
3. Правила идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации;
4. Правила проведения внутреннего аудита информационной безопасности;
5. Правила использования средств криптографической защиты информации;
6. Правила организации процедуры аутентификации и разграничения прав доступа к электронным информационным ресурсам;
7. Правила организации антивирусного контроля, использования мобильных устройств, носителей информации, Интернета и электронной почты;
8. Правила организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации;
9. Руководство администратора по сопровождению объекта информатизации, резервному копированию и восстановлению информации;
10. Инструкция о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях.