О внесении изменений 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 и.о. Министра искусственного интеллекта и цифрового развития Республики Казахстан от 22 июня 2026 года № 345/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 24 июня 2026 года № 39054.

Примечание ИЗПИ

Вводится в действие с 12.07.2026 года

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:

заголовок изложить в следующей редакции:

"Об утверждении методики и правил проведения испытаний цифровых объектов " цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности";

преамбулу изложить в следующей редакции:

"В соответствии с подпунктом 5) статьи 7-1 Закона Республики Казахстан "О кибербезопасности" 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**:";

пункт 1 изложить в следующей редакции:

"1. Утвердить:

1) Методику проведения испытаний цифровых объектов "цифрового правительства " и критически важных цифровых объектов на соответствие требованиям кибербезопасности согласно приложению 1 к настоящему приказу;

2) Правила проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности согласно приложению 2 к настоящему приказу.";

Методику проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности, утвержденную указанным приказом, изложить в новой редакции согласно приложению 1 к настоящему приказу;

Правила проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности, утвержденные указанным приказом, изложить в новой редакции согласно приложению 2 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 с 12 июля 2026 года и подлежит официальному опубликованию.

Исполняющий обязанности
министра искусственного интеллекта и цифрового развития
Республики Казахстан *Д. Мусалиев*

"СОГЛАСОВАН"
Комитет национальной безопасности
Республики Казахстан

Приложение 1 к приказу
Исполняющий обязанности
министра искусственного
интеллекта и цифрового развития
Республики Казахстан
от 22 июня 2026 года № 345/НҚ

Приложение 1 к приказу
Министра цифрового
развития, оборонной
и аэрокосмической
промышленности
Республики Казахстан
от 3 июня 2019 года № 111/НҚ

Методика проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности

Глава 1. Общие положения

1. Настоящая Методика проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности (далее – Методика) разработана в соответствии с подпунктом 5) статьи 7-1 Закона Республики Казахстан "О кибербезопасности" 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.

2. В настоящей Методике используются следующие понятия и сокращения:

1) программная закладка – скрытно внесенный в программное обеспечение (далее – ПО) функциональный объект, осуществляющий несанкционированный доступ и (или) воздействие на цифровой объект;

2) бэкдор – вредоносное ПО для получения несанкционированного доступа к программному обеспечению путем обхода аутентификации, а также других стандартных методов и технологий безопасности;

3) недекларированные возможности (далее – НДВ) – функциональные возможности ПО, не отраженные или не соответствующие описанным в нормативно-технической документации;

4) ручное тестирование на проникновение – легитимная оценка защищенности цифровых объектов с применением безопасных и контролируемых атак, выявлением уязвимостей и попытками их эксплуатации без реального ущерба деятельности заявителя;

5) прикладное программное обеспечение – комплекс программного обеспечения для решения прикладной задачи определенного класса предметной области;

6) поставщик – государственная техническая служба или аккредитованная испытательная лаборатория;

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

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

9) заявитель – собственник или владелец объекта испытаний, а также физическое или юридическое лицо, уполномоченное собственником или владельцем объекта испытаний, подавший(ее) заявку на проведение испытаний цифрового объекта на соответствие требованиям кибербезопасности;

10) доверенный канал – средство взаимодействия между функциями безопасности объектов испытаний (далее – ФБО) и удаленным доверенным продуктом цифровых технологий, обеспечивающее необходимую степень уверенности в поддержании политики безопасности объектов испытаний;

11) доверенный маршрут – средство взаимодействия между пользователем и ФБО, обеспечивающее уверенность в поддержании политики безопасности объектов испытаний;

12) интернет-портал SYNAQ – интернет-портал государственной технической службы, предназначенный для автоматизации процесса оказания услуги по испытаниям цифровых объектов на соответствие требованиям кибербезопасности;

13) объект испытаний – цифровой объект, в отношении которого проводятся работы по испытанию на соответствие требованиям кибербезопасности;

14) сегмент сети (подсеть) объекта испытаний – логически выделенный сегмент сети объекта испытаний;

15) функциональный объект – элемент (процедура, функция, ветвь или иная компонента) ПО, выполняющий действия по реализации законченного фрагмента алгоритма программы;

16) маршрут выполнения функциональных объектов – определенная алгоритмом последовательность выполняемых функциональных объектов;

17) среда штатной эксплуатации – целевой набор серверного оборудования, сетевой инфраструктуры, системного программного обеспечения, используемый на этапе опытной эксплуатации (пилотного проекта) и предназначенный для применения на этапе промышленной эксплуатации цифрового объекта.

3. Проведение испытаний включает:

1) анализ исходных кодов;

2) испытание функций кибербезопасности;

3) нагрузочное испытание;

4) обследование сетевой инфраструктуры;

5) обследование процессов обеспечения кибербезопасности.

Глава 2. Анализ исходных кодов

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, отнесенных к цифровым объектам " цифрового правительства" 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".

5. Анализ исходных кодов проводится для ПО, перечисленного в таблицах подпункта 11) и подпункта 12) пункта 5 анкеты-вопросника о характеристиках объекта испытаний приложения 2 к Правилам проведения испытаний цифровых объектов " цифрового правительства" и критически важных цифровых объектов, на соответствие требованиям кибербезопасности (далее – Правила).

6. При выявлении необходимости проведения повторного анализа исходных кодов до окончания срока испытания, заявитель обращается с запросом к поставщику и заключает дополнительное соглашение о проведении повторного анализа исходных кодов в соответствии с пунктом 21 Правил.

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

Выявление уязвимостей ПО объектов испытаний, отнесенных к цифровым объектам "цифрового правительства", проводится ручным методом анализа исходного кода и с использованием программного средства, предназначенного для анализа исходного кода, на основании исходных кодов, предоставленных заявителем.

8. Выявление НДВ ПО объектов испытаний, отнесенных к цифровым объектам " цифрового правительства", проводится ручным методом анализа исходного кода с детальным просмотром исходного кода и проведением поиска бэкдоров в библиотеках с открытым исходным кодом.

9. Анализ исходных кодов включает:

1) выявление уязвимостей ПО;

2) выявление НДВ для объектов испытаний, отнесенных к цифровым объектам " цифрового правительства";

3) фиксацию результатов анализа исходного кода.

10. Выявление уязвимостей ПО осуществляется в следующем порядке:

1) проводится подготовка исходных данных (загрузка исходных кодов цифровых объектов "цифрового правительства" и критически важных цифровых объектов, выбор режима сканирования (динамический и/или статический), настройка характеристик режимов сканирования);

2) проводится ручной метод анализа исходного кода и подготовка исходных данных (загрузка исходных кодов объектов испытаний собственником (владельцем) и (или) заказчиком которых является государственный орган), выбор режима сканирования (статический, анализ зависимостей и/или динамический), настройка характеристик режимов сканирования);

3) запускается ПО, предназначенное для выявления уязвимостей ПО;

4) проводится анализ программных отчетов на наличие ложных срабатываний;

5) формируется отчет, включающий в себя перечень выявленных уязвимостей ПО с указанием их описания, маршрута (пути к файлу) и степени риска (высокая, средняя, низкая).

11. Выявление НДВ осуществляется в следующем порядке:

1) анализ нормативно-технической документации на объект испытания, в том числе технического задания на создание (развитие) цифрового объекта, в части сведений о его назначении, области применения, применяемых методах, классе решаемых задач, ограничениях при применении, минимальной конфигурации технических средств, среде функционирования и порядке работы;

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 нормативно-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.

3) формирование отчета, включающего в себя перечень выявленных НДВ с приведением их описания, маршрута (пути к файлу) и снимка экрана;

4) проведение поиска бэкдоров в библиотеках с открытым исходным кодом, в том числе с помощью автоматизированного анализатора;

5) формирование отчета, включающего в себя описание уязвимостей с приведением идентификатора из международных баз данных уязвимостей.

12. Объем работ по анализу исходного кода определяется размером исходного кода.

13. Результаты анализа исходных кодов фиксируются ответственным исполнителем данного вида работ поставщика, в протоколе анализа исходных кодов (произвольная форма) с приложением копии анкеты-вопросника о характеристиках объекта испытаний согласно приложению 2 к Правилам.

Протокол анализа исходных кодов с приложениями и отчетом, выдаваемый:

1) аккредитованной лабораторией, прошивается со сквозной нумерацией страниц и опечатывается печатью (при наличии);

2) государственной технической службой, размещается в электронном виде в личном кабинете заявителя на интернет-портале SYNAQ.

14. По окончанию анализа исходных кодов:

1) исходные коды объекта испытаний (за исключением цифровых объектов " цифрового правительства") маркируются и сдаются в опечатанном виде на ответственное хранение в архив аккредитованной испытательной лаборатории;

2) исходные коды объекта испытаний (цифрового объекта "цифрового правительства") получают уникальный идентификационный номер и хранятся в интернет-портале SYNAQ.

15. Поставщик обеспечивает сохранение полученных исходных кодов с соблюдением их конфиденциальности сроком не менее трех лет после завершения испытаний.

Глава 3. Испытание функций кибербезопасности

16. Оценка функций цифровых объектов на соответствие требованиям кибербезопасности (далее – испытание функций кибербезопасности) осуществляется с целью оценки их соответствия требованиям нормативно-технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов по кибербезопасности.

17. Испытание функций кибербезопасности включает:

1) оценку соответствия функций безопасности требованиям нормативно-технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов по кибербезопасности, в том числе с применением программных средств (при необходимости);

2) ручное тестирование на проникновение объектов испытаний, отнесенных к цифровым объектам "цифрового правительства";

3) сканирование программным обеспечением на наличие обновлений и анализ конфигурации;

4) фиксацию результатов испытания в отчете с указанием результатов наблюдения, оценки соответствия или несоответствия и рекомендации по исправлению выявленных несоответствий (при необходимости).

18. Перечень функций кибербезопасности приведен в приложении 1, перечень функций ручного тестирования приведен в приложении 2 к Методике.

19. Испытание функций кибербезопасности проводятся по уровням реализации:

среды виртуализации операционных систем – гипервизоры;

операционные системы;

системы управления базами данных (СУБД);

прикладное программное обеспечение и их совокупность в составе цифровых объектов "цифрового правительства", перечисленных в таблицах подпункта 1) и подпункта 4) пункта 5 анкеты-вопросника о характеристиках объекта испытаний приложения 2 к Правилам.

20. Ручное тестирование на проникновение объектов испытаний, отнесенных к цифровым объектам "цифрового правительства", включает:

1) выявление уязвимостей в объекте испытаний;

2) формирование рекомендаций по устранению выявленных уязвимостей.

21. Результаты испытаний функций кибербезопасности фиксируются ответственным исполнителем данного вида работ поставщика в протоколе испытаний функций кибербезопасности (произвольная форма) с приложением копии анкеты-вопросника о характеристиках объекта испытаний.

Протокол испытаний функций кибербезопасности с приложениями и отчетом, выдаваемый:

1) аккредитованной лабораторией, прошивается со сквозной нумерацией страниц и опечатывается печатью (при наличии);

2) государственной технической службой, размещается в электронном виде в личном кабинете заявителя на интернет-портале SYNAQ.

Глава 4. Нагрузочное испытание

22. Нагрузочное испытание проводится с целью оценки соблюдения доступности, целостности и конфиденциальности объекта испытаний.

23. Нагрузочное испытание проводится с использованием специализированного программного средства на основании автоматических сценариев, в среде штатной эксплуатации объекта испытаний, в которой персональные данные заменены на фиктивные.

24. Параметры нагрузочного испытания предоставляются заявителем таблицах подпункта 9) и подпункта 10) пункта 5 анкеты-вопросника о характеристиках объекта испытаний приложения 2 к Правилам.

При проведении нагрузочного испытания выявляется параметры фактической нагрузочной способности объекта испытаний.

25. Нагрузочное испытание осуществляется в следующем порядке:

1) проводится подготовка к испытанию;

2) проводится испытание;

3) фиксируются результаты испытания.

26. Подготовка к испытанию включает:

1) определение сценария испытания;

2) определение временных и количественных характеристик испытания;

3) согласование времени проведения испытания с заказчиком.

27. Проведение испытания включает:

1) настройка конфигурации и сценария испытания в специализированное программное средство;

2) запуск специализированного программного средства;

3) регистрация нагрузки на объект испытаний;

4) формирование и выдача отчета нагрузочного испытания с указанием рекомендаций по увеличению или снижению реальной пропускной способности объекта испытаний.

28. Работы по проведению нагрузочного тестирования проводятся для одного объекта испытаний по количеству вариантов точек подключений пользователей и вариантов точек подключения интеграционного взаимодействия объекта испытаний, указанных в таблицах подпункта 9) и подпункта 10) пункта 5 анкеты-вопросника о характеристиках объекта испытаний приложения 2 к Правилам.

29. Результаты нагрузочного испытания фиксируются ответственным исполнителем данного вида работ поставщика в протоколе нагрузочного испытания (произвольная форма) с приложением копии анкеты-вопросника о характеристиках объекта испытаний.

Протокол нагрузочного испытания с приложениями и отчетом, выдаваемый:

1) аккредитованной лабораторией, прошивается со сквозной нумерацией страниц и опечатывается печатью (при наличии);

2) государственной технической службой, размещается в электронном виде в личном кабинете заявителя на интернет-портале SYNAQ.

Глава 5. Обследование сетевой инфраструктуры

30. Обследование сетевой инфраструктуры проводится с целью оценки безопасности сетевой инфраструктуры.

31. Обследование сетевой инфраструктуры включает:

1) оценку соответствия функций защиты сетевой инфраструктуры требованиям нормативно-технической документации, нормативных правовых актов Республики

Казахстан и действующих на территории Республики Казахстан стандартов по кибербезопасности;

2) обследование сетевой инфраструктуры заявителя, в том числе с применением программных средств (при необходимости);

3) сканирование программным средством на наличие известных уязвимостей программного обеспечения из базы общих уязвимостей и рисков;

4) фиксацию полученных результатов испытания в отчете с указанием результатов наблюдения, оценки соответствия или несоответствия и рекомендации по исправлению выявленных несоответствий (при необходимости).

32. Перечень функций защиты сетевой инфраструктуры приведен в приложении 3 к настоящей Методике.

33. Работы по обследованию сетевой инфраструктуры, проводятся для каждого сегмента сети (подсети) объекта испытаний, указанного в таблице подпункта 7) пункта 5 анкеты-вопросника о характеристиках объекта испытаний приложения 2 к Правилам.

34. Результаты обследования сетевой инфраструктуры фиксируются ответственным исполнителем данного вида работ поставщика в протоколе обследования сетевой инфраструктуры (произвольная форма) с приложением копии анкеты-вопросника о характеристиках объекта испытаний.

Протокол обследования сетевой инфраструктуры с приложениями и отчетом, выдаваемый:

1) аккредитованной лабораторией, прошивается со сквозной нумерацией страниц и опечатывается печатью (при наличии);

2) государственной технической службой, размещается в электронном виде в личном кабинете заявителя на интернет-портале SYNAQ.

Глава 6. Обследование процессов обеспечения кибербезопасности

35. Обследование процессов обеспечения кибербезопасности осуществляется с целью определения их соответствия требованиям нормативных правовых актов и стандартов по обеспечения кибербезопасности.

36. Обследование процессов обеспечения кибербезопасности включает:

1) оценку соответствия процессов обеспечения кибербезопасности требованиям нормативных правовых актов и стандартов в сфере обеспечения кибербезопасности;

2) фиксацию результатов оценки испытания с указанием результатов наблюдения, оценки соответствия или несоответствия и рекомендации по исправлению выявленных несоответствий (при необходимости).

37. Перечень процессов обеспечения кибербезопасности и их содержание приведено в приложении 4 к Методике.

38. Работы по обследованию процессов обеспечения кибербезопасности проводятся для объекта испытания.

39. Результаты обследования процессов обеспечения кибербезопасности фиксируются ответственным исполнителем данного вида работ поставщика в протоколе обследования процессов обеспечения кибербезопасности (произвольная форма) с приложением копии анкеты-вопросника о характеристиках объекта испытаний.

Протокол обследования процессов обеспечения кибербезопасности с приложениями и отчетом, выдаваемый:

1) аккредитованной лабораторией, прошивается со сквозной нумерацией страниц и опечатывается печатью (при наличии);

2) государственной технической службой, размещается в электронном виде в личном кабинете заявителя на интернет-портале SYNAQ.

Результаты сканирования программным средством на соответствие стандартам в сфере обеспечения кибербезопасности не включаются в Протокол обследования процессов обеспечения кибербезопасности и носят рекомендательный характер.

Приложение 1
к Методике проведения
испытаний цифровых объектов
"цифрового правительства" и
критически важных цифровых
объектов на соответствие
требованиям кибербезопасности
Форма

Перечень функций кибербезопасности

№ п/п	Наименование функций	Содержание функций
1	2	3
Аудит безопасности		
1	Автоматическая реакция аудита безопасности	Обеспечение мониторинга кибербезопасности средствами сбора и анализа событий кибербезопасности. Осуществление генерации записи в регистрационном журнале, локальная или удаленная сигнализация администратору об обнаружении нарушения безопасности.
2	Генерация данных аудита безопасности	Наличие протоколирования, по крайней мере, запуска и завершения регистрационных функций, а также всех событий базового уровня аудита, то есть в каждой регистрационной записи присутствие даты и времени события, типа события, идентификатора субъекта и

		результата (успех или неудача) события.
3	Анализ аудита безопасности	Осуществление (с целью выявления вероятных нарушений), по крайней мере, путем накопления и/или объединения неуспешных результатов использования механизмов аутентификации, а также неуспешных результатов выполнения криптографических операций.
4	Просмотр аудита безопасности	Обеспечение и предоставление администратору возможности просмотра (чтения) всей регистрационной информации. Прочим пользователям доступ к регистрационной информации закрыт, за исключением явно специфицированных случаев.
5	Выбор событий аудита безопасности	Наличие избирательности регистрации событий, основывающейся, по крайней мере, на следующих атрибутах: 1) идентификатор объекта; 2) идентификатор субъекта; 3) адрес узла сети; 4) тип события; 5) дата и время события.
6	Хранение данных аудита безопасности	Наличие регистрационной информации о надежности защиты от несанкционированной модификации.
Криптографическая поддержка		
7	Управление криптографическими ключами	Наличие поддержки: 1) генерации криптографических ключей; 2) распределения криптографических ключей; 3) управления доступом к криптографическим ключам; 4) уничтожения криптографических ключей.
		1. Наличие для всей информации, передаваемой по доверенному каналу, шифрования и контроля целостности в соответствии с требованиями нормативно-технической документации, нормативных правовых актов Республики

8	Криптографические операции	Казахстан и действующих на территории Республики Казахстан стандартов в сфере кибербезопасности. 2. Применение средств криптографической защиты информации для объектов испытаний (далее – ОИ), содержащих конфиденциальные данные, персональные данные ограниченного доступа или служебную информацию ограниченного распространения.
Защита данных пользователя		
9	Политика управления доступом	Осуществление разграничения доступа для пользователей, прямо или косвенно выполняющих операции с сервисом безопасности .
10	Функции управления доступом	Применение функций разграничения доступа основывается, по крайней мере, на следующих атрибутах безопасности: 1) идентификаторы субъектов доступа; 2) идентификаторы объектов доступа; 3) адреса субъектов доступа; 4) адреса объектов доступа; 5) права доступа субъектов.
11	Аутентификация данных	Поддержка гарантии правильности специфического набора данных, который впоследствии используется для верификации того, что содержание информации не было подделано или модифицировано мошенническим путем.
12	Экспорт данных за пределы действия функций безопасности ОИ (далее – ФБО)	Обеспечение при экспорте данных пользователя из ОИ защиты и сохранности или игнорирования их атрибутов безопасности.
13	Политика управления информационными потоками	Обеспечение предотвращения раскрытия, модификации и/или недоступности данных пользователя при их передаче между физически разделенными частями сервиса безопасности.
		Организация и обеспечение контроля доступа к хранилищам данным с целью исключения

14	Функции управления информационными потоками	бесконтрольного распространения информации, содержащейся в них (управление информационными потоками для реализации надежной защиты от раскрытия или модификации в условиях недоверенного программного обеспечения (далее - ПО).
15	Импорт данных из-за пределов действия ФБО	Наличие механизмов для передачи данных пользователя в ОИ таким образом, чтобы эти данные имели требуемые атрибуты безопасности и защиту.
16	Передача в пределах ОИ	Наличие защиты данных пользователя при их передаче между различными частями ОИ по внутреннему каналу.
17	Защита остаточной информации	Обеспечение полной защиты остаточной информации, то есть недоступности предыдущего состояния при освобождении ресурса.
18	Откат текущего состояния	Наличие возможности отмены последней операции или ряда операций, ограниченных некоторым пределом (например, периодом времени), и возврат к предшествующему известному состоянию. Откат предоставляет возможность отменить результаты операции или ряда операций, чтобы сохранить целостность данных пользователя.
19	Целостность хранимых данных	Обеспечение защиты данных пользователя во время их хранения в пределах ФБО.
20	Защита конфиденциальности данных пользователя при передаче между ФБО	Обеспечение конфиденциальности данных пользователя при их передаче по внешнему каналу между ОИ и другим доверенным продуктом IT. Конфиденциальность осуществляется путем предотвращения несанкционированного раскрытия данных при их передаче между двумя оконечными точками. Оконечными точками могут быть ФБО или пользователь.
		Обеспечивается целостность данных пользователя при их передаче между ФБО и другим

21	Защита целостности данных пользователя при передаче между ФБО	доверенным продуктом ИТ, а также возможность их восстановления при обнаруживаемых ошибках.
Идентификация и аутентификация		
22	Отказы аутентификации	Наличие возможности при достижении определенного администратором числа неуспешных попыток аутентификации отказать субъекту в доступе, сгенерировать запись регистрационного журнала и сигнализировать администратору о вероятном нарушении безопасности.
23	Определение атрибутов пользователя	Для каждого пользователя необходимо поддерживать, по крайней мере, следующие атрибуты безопасности: идентификатор; аутентификационная информация (например, пароль); права доступа (роль).
24	Спецификация секретов	1) наличие автоматической блокировки учетной записи при превышении срока действия пароля; 2) наличие процедуры смены пароля пользователя; 3) при смене пароля ставятся ограничения на минимальную длину и сложность пароля. Должны быть реализованы меры по защищенному хранению аутентификационной информации и иных секретов, используемых компонентами системы и сервисными учетными записями, с использованием специализированных механизмов или средств управления секретами, обеспечивающих их конфиденциальность и защиту от несанкционированного доступа.
25	Аутентификация пользователя	Наличие механизмов аутентификации пользователя, предоставляемых ФБО.
		Обеспечение: 1) успешности идентификации и аутентификации каждого пользователя до разрешения любого действия, выполняемого

26	Идентификация пользователя	сервисом безопасности от имени этого пользователя; 2) возможностей по предотвращению применения аутентификационных данных, которые были подделаны или скопированы у другого пользователя; 3) аутентификации любого представленного идентификатора пользователя; 4) повторной аутентификации пользователя по истечении определенного администратором интервала времени; 5) предоставления пользователю функций безопасности только со скрытой обратной связью во время выполнения аутентификации.
27	Связывание пользователь-субъект	Следует ассоциировать соответствующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя.
Управление безопасностью		
28	Управление отдельными функциями ФБО	Наличие единоличного права администратора на определение режима функционирования, отключения, подключения, модификации режимов идентификации и аутентификации, управления правами доступа, протоколирования и аудита.
29	Управление атрибутами безопасности	Наличие единоличного права администратора на изменения подразумеваемых значений, опрос, изменения, удаления, создания атрибутов безопасности, правил управления потоками информации. При этом необходимо обеспечить присваивание атрибутам безопасности только безопасных значений.
30	Управление данными ФБО	Наличие единоличного права администратора на изменения подразумеваемых значений, опрос, изменения, удаления, очистки, определения типов регистрируемых событий, размеров регистрационных журналов, прав доступа субъектов

		, сроков действия учетных записей субъектов доступа, паролей, криптографических ключей.
31	Отмена атрибутов безопасности	Наличие осуществления отмены атрибутов безопасности в некоторый момент времени. Только у уполномоченных администраторов имеется возможность отмены атрибутов безопасности, ассоциированных с пользователями. Важные для безопасности полномочия отменяются немедленно.
32	Срок действия атрибута безопасности	Обеспечение возможности установления срока действия атрибутов безопасности.
33	Роли управления безопасностью	1) Обеспечение поддержки, по крайней мере, следующих ролей: уполномоченный пользователь, удаленный пользователь, администратор; 2) Обеспечение получения ролей удаленного пользователя и администратора только по запросу .
Защита ФБО		
34	Безопасность при сбое	Сохранение сервисом безопасного состояния при аппаратных сбоях (вызванных, например, перебоями электропитания).
35	Доступность экспортируемых данных ФБО	Сервис обеспечивает верификацию доступности всех данных при их передаче между ним и удалҰнным доверенным продуктом цифровых технологий, а также повторную передачу информации и генерацию записи регистрационного журнала при обнаружении модификаций.
36	Конфиденциальность экспортируемых данных ФБО	Предоставление сервисом возможности верифицировать конфиденциальность всех данных при их передаче между ним и удаленным доверенным продуктом цифровых технологий и выполнять повторную передачу информации, а также генерировать запись регистрационного журнала, если модификации обнаружены.
		Предоставление сервисом возможности верифицировать

37	Целостность экспортируемых данных ФБО	целостность всех данных при их передаче между ним и удаленным доверенным продуктом цифровых технологий и выполнять повторную передачу информации, а также генерировать запись регистрационного журнала, если модификации обнаружены.
38	Передача данных ФБО в пределах ОИ	Сервис предоставляет возможность верифицировать доступность, Предоставление сервисом возможности конфиденциальность и целостность всех данных при их передаче между ним и удаленным доверенным продуктом цифровых технологий и выполнять повторную передачу информации, а также генерировать запись регистрационного журнала, если модификации обнаружены.
39	Надежное восстановление	Когда автоматическое восстановление после сбоя или прерывания обслуживания невозможно, сервис переходит в режим аварийной поддержки, позволяющей вернуться к безопасному состоянию. После аппаратных сбоев обеспечивается возврат к безопасному состоянию с использованием автоматических процедур.
40	Обнаружение повторного использования	Обеспечение обнаружения сервисом повторного использования аутентификационных данных, отказа в доступе, генерирования записи регистрационного журнала и сигнализирования администратору о вероятном нарушении безопасности.
41	Посредничество при обращениях	Обеспечение вызова и успешного выполнения функций, осуществляющих политику безопасности сервиса прежде, чем разрешается выполнение любой другой функции сервиса.
42	Разделение домена	Поддержка отдельного домена для собственного выполнения функций безопасности, который защищает их от вмешательства и искажения недоверенными субъектами.

43	Протокол синхронизации состояний	Обеспечение синхронизации состояний при выполнении идентичных функций на серверах.
44	Метки времени	Предоставление для использования функциями безопасности надежных меток времени.
45	Согласованность данных между ФБО	Обеспечение согласованной интерпретации регистрационной информации, а также параметров используемых криптографических операций.
46	Согласованность данных ФБО при дублировании в пределах ОИ	Обеспечение согласованности данных функций безопасности при дублировании их в различных частях объекта испытаний. Когда части, содержащие дублируемые данные, разъединены, согласованность обеспечивается после восстановления соединения перед обработкой любых запросов к заданным функциям безопасности.
47	Использование сценариев (скриптов)	Отсутствие в ОИ возможных сценариев (скриптов) с правами на модификацию, применение которых влечет возникновение инцидентов кибербезопасности.
Использование ресурсов		
48	Отказоустойчивость	Обеспечение доступности функциональных возможностей объекта испытаний даже при сбоях. Примеры таких сбоев: отключение питания, отказ аппаратуры, сбой ПО.
49	Распределение ресурсов	1. Обеспечение управления использованием ресурсов пользователями и субъектами таким образом, чтобы не допустить несанкционированные отказы в обслуживании из-за монополизации ресурсов другими пользователями или субъектами. 2. Использование в рамках цифрового объекта только обеспечивающих его функционирование программных продуктов.
Доступ к ОИ		
		Ограничение как атрибутов безопасности сеанса, которые

50	Ограничение области выбираемых атрибутов	выбирает пользователь, так и атрибутов субъектов, с которыми пользователь связан, на основе метода или места доступа, порта доступа, а также времени (например, времени суток, дня недели).
51	Ограничение на параллельные сеансы	Ограничение максимального числа параллельных сеансов, предоставляемых одному пользователю. У этой величины подразумеваемое значение устанавливается администратором .
52	Блокирование сеанса	Принудительное завершение сеанса работы по истечении установленного администратором значения длительности бездействия пользователя.
53	Предупреждения перед предоставлением доступа к ОИ	Обеспечение возможности еще до идентификации и аутентификации отображения для потенциальных пользователей предупреждающего сообщения относительно характера использования объекта испытаний.
54	История доступа к ОИ	Обеспечение возможности отображения для пользователя, при успешном открытии сеанса, истории неуспешных попыток получить доступ от имени этого пользователя. Эта история содержит дату, время, IP -адрес источника откуда идет подключение, средства доступа и порт последнего успешного доступа к объекту испытаний, а также число неуспешных попыток доступа к объекту испытаний после последнего успешного доступа идентифицированного пользователя.
55	Открытие сеанса с ОИ	Обеспечение сервисом способности отказать в открытии сеанса, основываясь на идентификаторе субъекта, пароле субъекта, правах доступа субъекта .
Функции защиты от вредоносного кода		
		Применение для защиты от вредоносного кода средств мониторинга, обнаружения и

56	Наличие средств антивирусной защиты	блокирования или удаления вредоносного кода на серверах и при необходимости, на рабочих станциях объекта испытаний.
57	Лицензии для средств антивирусной защиты	Наличие у средств антивирусной защиты лицензии (приобретенной, ограниченной, свободно распространяемой) на сервера и рабочие станции.
58	Обновление баз сигнатур и программного обеспечения средств антивирусной защиты	Обеспечение регулярного обновления и поддержания в актуальном состоянии средств антивирусной защиты.
59	Управление доступом к средствам антивирусной защиты	Осуществление централизованного управления и конфигурирования средств антивирусной защиты.
60	Управление защитой от вредоносного кода на внешних электронных носителях информации средствами антивирусной защиты	Обеспечение управлением защитой от вредоносного кода на внешних электронных носителях информации проверки и блокировки файлов и при необходимости носителей информации.
Безопасность при обновлении ПО		
61	Регулярное обновления ПО	Обеспечение регулярного обновления общесистемного и прикладного ПО серверов и рабочих станций.
62	Обновление ПО в сетевых средах без доступа к серверам обновления в Интернете	Обеспечение обновления ПО в сетевых средах без доступа к серверам обновления в Интернете от специализированного сервера обновлений.
Безопасность при внесении изменений в прикладное ПО		
63	Среда разработки и тестирования прикладного ПО	Обеспечение наличия среды для разработки и тестирования прикладного ПО, изолированной от среды промышленной эксплуатации прикладного ПО.
64	Разграничение доступа в средах разработки и тестирования прикладного ПО	Обеспечение управления доступом к средам разработки и тестирования прикладного ПО для программистов и администраторов.
65	Система развертывания прикладного ПО	Наличие системы развертывания (распространения) прикладного ПО на серверах и рабочих станциях среды промышленной эксплуатации.

66	Разграничение доступа к системе развертывания прикладного ПО	Обеспечение управления доступом к системе развертывания (распространения) прикладного ПО на серверах и рабочих станциях среды промышленной эксплуатации.
"Защита от утечек конфиденциальной информации" на цифровых объектах государственных органов, местных исполнительных органах и критически важных цифровых объектов		
67	Политика управления доступом	Управление системой защиты от утечек конфиденциальной информации
68	Обновление компонентов системы	Обеспечение регулярного обновления и поддержания в актуальном состоянии системы защиты от утечек информации.
69	Атрибут безопасности раздела	Обеспечение применения парольной политики в соответствии Едиными требованиями в сферах цифровизации и обеспечения кибербезопасности утверждаемыми Правительством Республики Казахстан в соответствии с подпунктом 3) статьи 6 Закона Республики Казахстан "О кибербезопасности" (далее – ЕТ).
70	Хранение данных	Хранение журналов событий системы защиты от утечки конфиденциальной информации не менее трех лет и в оперативном доступе не менее двух месяцев.

Приложение 2
к Методике проведения
испытаний цифровых объектов
"цифрового правительства" и
критически важных цифровых
объектов на соответствие
требованиям кибербезопасности

Перечень функций ручного тестирования

№	Наименование функций	Содержание функций
1	Архитектура, дизайн и модель угроз (Architecture, Design and Threat Modeling)	Обеспечение безопасности дизайна приложения и архитектуры объекта испытаний и отсутствия уязвимостей.
2	Аутентификация (Authentication)	Обеспечение корректного функционирования аутентификации пользователей в объекте испытаний (логин/пароль, многофакторная авторизация,

		хэширование и другие криптографические методы).
3	Управление сессией (Session Management)	Обеспечение генерации уникальной сессии для каждого пользователя и технического запрета (блокировки) совместного использования сессии. Блокировка сессии пользователя по истечению времени бездействия (Timeout session).
4	Контроль доступа (Access Control)	Обеспечение разграничения прав пользователей и исключение несанкционированного доступа к объекту испытаний.
5	Проверка, фильтрация и кодирование (Validation, Sanitation and Encoding)	Обеспечение фильтрации входных пользовательских данных для предотвращения атак путем внедрения, а также обеспечение правильной кодировки выходных данных, при котором гарантируется защита их контекста от злоумышленников.
6	Хранимая криптография (Stored Cryptography)	Применение надежных алгоритмов шифрования и обеспечение безопасного управления и хранения криптографических ключей.
7	Обработка ошибок и логирование (Error Handling and Logging)	Обеспечение журналирования действий пользователей объекта испытаний и событий кибербезопасности с учетом их защиты в соответствии с требованиями безопасности. Собранные журналы с конфиденциальными данными не хранятся долго локально на серверах объекта испытаний и удаляются по истечении определенного промежутка времени.
8	Защита данных (Data Protection)	Обеспечение конфиденциальности при передаче и хранении данных в объекте испытаний с использованием средств криптографической защиты информации в соответствии с классификатором.
9	Связь (Communication)	Обеспечение безопасности объекта испытаний при передаче данных с использованием безопасных протоколов связи и алгоритмов шифрования.

10	Вредоносный код (Malicious Code)	Применение средств защиты для предотвращения выполнения вредоносного кода в объекте испытаний.
11	Бизнес-логика (Business Logic)	Обеспечение корректной работы логического функционирования объекта испытания согласно техническому заданию.
12	Файлы и ресурсы (Files and Resources)	Обеспечение хранения данных, полученных из сторонних и ненадежных источников вне серверов приложений.
13	Программный интерфейс приложения (API)	Обеспечение соответствия API следующим требованиям: - API имеет корректную авторизацию, основные параметры управления сеансом и аутентификацию для доступа ко всем веб-сервисам; API имеет надлежащую проверку вводимых данных при переходе их параметров с более низкого на более высокий уровень доверия; различные API, такие как облачные и бессерверные, имеет все необходимые элементы управления безопасностью.
14	Конфигурация (Configuration)	Обеспечение использования безопасных параметров конфигурации, сторонних библиотек, а также фильтрации небезопасных компонентов и надежной защиты конфиденциальных данных в файлах конфигураций при эксплуатации объекта испытаний.

Приложение 3
к Методике проведения
испытаний цифровых объектов
"цифрового правительства" и
критически важных цифровых
объектов на соответствие
требованиям кибербезопасности

Перечень функций защиты сетевой инфраструктуры

№ п/п	Наименование функций	Содержание функций
1	2	3
		1. Использование уникальных идентификаторов учетных записей

1	Идентификация и аутентификация	для установления связи пользователя с осуществленными действиями. 2. Привилегированные права доступа предназначены учетным записям на основе потребности в их использовании. 3. Регистрация неудачных и успешных попыток аутентификации. 4. Ограничение времени сеанса. 5. Отказы аутентификации (наличие возможности при достижении определенного числа неуспешных попыток аутентификации отказать субъекту в доступе). 6. Использование и выбор надежных паролей. 7. Проведение регулярной смены пароля, а также – по мере необходимости.
2	Отметки аудитов (формирование и наличие отчетов о событиях, связанных с безопасностью сетевых соединений)	1. Регистрация событий, связанных с состоянием кибербезопасности, при этом журналы событий включают: идентификаторы пользователей; системные действия; дату, время и детали ключевых событий, например, вход и выход из системы; отчеты об успешных и отклоненных попытках доступа; изменения системной конфигурации; использование привилегий; сетевые адреса и протоколы. 2. Проведение мониторинга событий, связанных с нарушением кибербезопасности, и анализ результатов мониторинга. 3. Хранение журналов регистрации событий в течение срока, указанного в нормативно-технической документации по кибербезопасности, но не менее трех лет и нахождение их в оперативном доступе не менее двух месяцев. 4. Обеспечение защиты журналов регистрации событий от вмешательства и

		неавторизованного доступа, при этом: не допускается наличие у системных администраторов полномочий на изменение, удаление и отключение журналов; для конфиденциальных цифровых объектов требуется создание и ведение резервного хранилища журналов. 5. Наличие оповещения о критичных видах событий кибербезопасности. 6. Обеспечение синхронизации времени журналов регистрации событий с эталоном времени и частоты, воспроизводящим национальную шкалу всемирного координированного времени UTC (kz).
3	Обнаружение вторжения	1. Обеспечение наличия средств, позволяющих прогнозировать вторжения (потенциальные вторжения в сетевую инфраструктуру), выявлять их в реальном масштабе времени и поднимать соответствующую тревогу. 2. Возможность автоматизированного обновления базы правил.
4	Управление сетевой безопасностью	1. Неиспользуемые интерфейсы кабельной системы локальной сети физически отключаются от активного оборудования. 2. Исключение подключения локальной сети внутреннего контура государственных органов и местных исполнительных органов к Интернету, а также исключение сопряжения локальной сети внутреннего контура и локальной сети внешнего контура государственных органов и местных исполнительных органов между собой. 3. Защита конфиденциальности целостности данных, передаваемых по сетям цифрового объекта государственных органов и местных исполнительных органов осуществляются из

		внутренней локальной сети владельца цифрового объекта. 4. Применение средств логического и/или физического сегментирования локальной сети. 5. Обеспечение синхронизации по времени между компонентами цифрового объекта, а также между цифровым объектом и средой его функционирования.
5	Межсетевые экраны	1. Обеспечение фильтрации входящих и исходящих пакетов на каждом интерфейсе. 2. В настройках оборудования неиспользуемые порты блокируются. 3. Преобразование сетевых адресов.
6	Защита конфиденциальности целостности данных, передаваемых по сетям	При организации выделенного канала связи, объединяющего локальные сети, применяются программно-технические средства защиты информации, в том числе криптографического шифрования, с использованием средств криптографической защиты информации.
7	Неотказуемость от совершенных действий по обмену информацией	Применение средств мониторинга и анализа сетевого трафика.
8	Обеспечение непрерывной работы и восстановления	Для обеспечения доступности и отказоустойчивости используется резервирование аппаратно-программных средств обработки данных, систем хранения данных, компонентов сетей хранения данных и каналов передачи данных.
9	Доверенный канал	Предоставление для связи с удаленным доверенным продуктом канала, который логически отличим от других и обеспечивает надежную аутентификацию его сторон, а также защиту данных от модификации и раскрытия. Обеспечение у обеих сторон возможности инициировать связь через доверенный канал.
		Предоставление для связи с удаленным пользователем маршрута, который логически отличим от других и обеспечивает

10	Доверенный маршрут	надежную аутентификацию его сторон, а также защиту данных от модификации и раскрытия. Обеспечение у пользователя возможности инициировать связь через доверенный маршрут. Для начальной аутентификации удаленного пользователя и удаленного управления использование доверенного маршрута является обязательным.

Приложение 4
к Методике проведения
испытаний цифровых объектов
"цифрового правительства" и
критически важных цифровых
объектов на соответствие
требованиям кибербезопасности

Перечень процессов обеспечения кибербезопасности и их содержание

№ п/п	Наименование процессов	Требование к содержанию процессов обеспечения кибербезопасности
1	2	3
1	Управление активами, связанными с цифровыми технологиями	1. Идентификация активов в соответствии с ЕТ. 2. Классификация информации в соответствии с ЕТ. 3. Проверка класса, определенного для объекта испытаний на соответствие требованиям правил классификации цифровых объектов. 4. Маркировка активов в соответствии с ЕТ. 5. Закрепление ответственных лиц за идентифицированными активами. 6. Ведение и актуализация реестра активов в соответствии с принятой формой реестра. 7. Определение, документирование и реализация процедур обращения с активами (выдача, использование, хранение, внос/вынос и возврат) в соответствии с ЕТ. 8. Паспортизация средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения.

		9. Безопасная организация работ при приеме/отгрузке активов, связанных с цифровыми технологиями. 10. Безопасная утилизация (повторное использование) серверного и телекоммуникационного оборудования, систем хранения данных, рабочих станций, носителей информации.
2	Организация кибербезопасности	1. Наличие подразделения кибербезопасности или сотрудника, ответственного за кибербезопасность, обособленного от подразделения цифровых технологий, подчиняющегося непосредственно высшему руководству. 2. Функционирование рабочих групп и проведение совещаний по вопросам координации работ и обеспечения кибербезопасности. 3. Разработка (актуализация), утверждение, одобрение руководством нормативно-технической документации по кибербезопасности, доведение их содержимого до сотрудников и привлекаемых со стороны исполнителей. 4. Поддержание контактов с полномочными органами, профессиональными сообществами, профессиональными ассоциациями или форумами специалистов по кибербезопасности. 5. Определение и документирование процедур обеспечения кибербезопасности, в том числе, при привлечении сторонних организаций. 6. Разработка (пересмотр) соглашения о конфиденциальности или неразглашении, отражающие потребности в защите информации. 7. Определение и включение в соглашения со сторонними

		организациями требований по кибербезопасности и уровня обслуживания. Контроль за реализации положений соглашения.
3	Безопасность, связанная с персоналом	1. Предварительная проверка кандидатов при приеме на работу. 2. Определение, назначение и отражение в должностных инструкциях и (или) условиях трудового договора сотрудников и привлекаемых со стороны исполнителей ролей, обязанностей и ответственности, связанных с кибербезопасностью в период занятости, изменения или прекращения трудовых отношений и обязательств владельца объекта испытаний. 3. Определение и документирование процедур увольнения сотрудников, имеющих обязательства в области обеспечения кибербезопасности. 4. Определение и регламентирование действий, которые будут предприняты к нарушителям правил кибербезопасности. 5. Извещение сотрудников об изменениях в политиках, правилах и процедурах обеспечения кибербезопасности, затрагивающих исполнение их служебных обязанностей. 6. Осведомленность и исполнение сотрудниками и привлекаемыми со стороны исполнителями об обязанностях и ответственности, связанными с обеспечением кибербезопасности в период занятости, изменения или прекращения трудовых отношений. 7. Обучение и подготовка сотрудников в сфере кибербезопасности. 8. Ответственность руководства за обеспечение возможности выполнения сотрудниками и привлекаемыми со стороны исполнителями обязательств в отношении кибербезопасности.

4	Мониторинг событий КБ и управление инцидентами КБ	1. Регистрация действий пользователей, операторов, администратор и событий операционных систем, систем управления базой данных, антивирусного программного обеспечения (далее – ПО), прикладного ПО, телекоммуникационного оборудования, систем обнаружения и предотвращения атак, системы управления контентом. 2. Ведение, хранение и защита журналов регистрации событий. 3. Осуществление анализа журналов регистрации событий. 4. Мониторинг зарегистрированных событий и оповещение о событиях высокой и критичной степени важности для кибербезопасности. 5. Оценка и принятие решения по событию кибербезопасности. 6. Разработка, документирование, доведение до сведения сотрудников и привлекаемых со стороны исполнителей, выполнение процедур реагирования на инциденты кибербезопасности. 7. Проведение анализа инцидентов кибербезопасности.
5	Управление непрерывностью КБ	1. Планирование непрерывности кибербезопасности. 2. Идентификация событий, которые являются возможной причиной нарушения непрерывности процесса обеспечения кибербезопасности или бизнес-процессов. 3. Разработка (актуализация), внедрение процессов и процедур поддержания необходимого уровня непрерывности кибербезопасности во внештатных (кризисных) ситуациях. 4. Определение, документирование, доведение до сведений сотрудников и привлекаемых со стороны

		исполнителей, выполнение процедур во внештатных (кризисных ситуациях). 5. Проверка (тестирование), анализ и оценка процессов и процедур обеспечения непрерывности кибербезопасности. 6. Резервирование средств обработки информации, цифрового объекта с учетом требований законодательства.
6	Управление сетевой безопасностью	1. Определение, документирование и доведение до сведений сотрудников и привлекаемых со стороны исполнителей, выполнение процедур управления сетевым оборудованием. 2. Определение и включение в соглашения по обслуживанию сетей и передаче информации механизмов обеспечения безопасности, уровней доступности для всех сетевых услуг и сервисов. 3. Определение, документирование, доведение до сведений сотрудников и привлекаемых со стороны исполнителей, выполнение политик и процедур использования сетей и сетевых услуг, передачи информации, подключения к Интернету, сетям телекоммуникаций и связи и использования беспроводного доступа к сетевым ресурсам. 4. Определение, документирование и выполнение процедур по применению средств защиты информации, передаваемой по сети и электронных сообщений. 5. Способы подключения и взаимодействия сетей, учитывающие требования законодательства.
		1. Регламентация управления криптографическими ключами, включающая вопросы изготовления, учета, хранения, передачи, использования, возврата

7	Криптографические методы защиты	(уничтожения), защиты криптографических ключей, учитывающая требования законодательства. 2. Применение криптографических средств при хранении и передаче информации, включая аутентификационные данные.
8	Управление рисками кибербезопасности	1. Выбор методики оценки рисков. 2. Идентификация угроз (рисков) для идентифицированных и классифицированных активов и формирование (актуализация) каталога угроз (рисков) кибербезопасности. Отражение в каталоге угроз (рисков), рисков, связанных с процессами обеспечения кибербезопасности. 3. Оценка (переоценка) идентифицированных рисков. 4. Обработка рисков, формирование и утверждение (актуализация) плана обработки рисков. 5. Мониторинг и пересмотр рисков.
9	Управление доступом	1. Разработка (актуализация), документирование, ознакомление пользователей с правилами разграничения прав доступа к информации, функциям прикладных систем, услугам, системному ПО, сетям и сетевым сервисам в соответствии с ЕТ. 2. Применяемые методы и процедуры идентификации, аутентификации и авторизации пользователей. 3. Реализация правил разграничения прав доступа в соответствии с ЕТ. 4. Процедуры регистрации и отмены регистрации (блокировки) пользователей. 5. Управление учетными записями с привилегированными правами доступа. 6. Использование и управление криптографическими методами в процедурах аутентификации пользователей.

		7. Управление изменениями правами доступа. 8. Управление паролями. 9. Использование привилегированных утилит. 10. Управление доступом к исходному коду объекта испытаний.
10	Физическая безопасность и защита от природных угроз	1. Размещение серверного, телекоммуникационного оборудования, систем хранения данных с учетом требования законодательства. 2. Физическая защита периметра безопасности помещений, в которых размещены активы, связанные с цифровыми технологиями. 3. Организация основного и резервного серверных помещений, учитывающая требования законодательства. 4. Оснащение основного и резервных серверных помещений системами обеспечения, учитывающее требования законодательства. 5. Организация контролируемого доступа в серверные помещения. 6. Организация работ в серверном помещении. 7. Организация работ по техническому сопровождению и обслуживанию серверного и телекоммуникационного оборудования, систем хранения данных и систем обеспечения. 8. Способы защиты оборудования от отказов в системе электроснабжения и других нарушений, вызываемых сбоями в работе коммунальных служб. 9. Обеспечение безопасности кабельной системы. 10. Обеспечение безопасности кроссовых помещений.
		1. Разработка (актуализация), документирование, ознакомление пользователей с инструкциями, регламентирующими эксплуатационные процедуры обеспечения кибербезопасности.

11	Эксплуатационные процедуры обеспечения кибербезопасности	2. Применение средств и систем обеспечения кибербезопасности. 3. Процедуры резервного копирования информации и тестирование результатов копирования. Безопасность мест хранения резервных копий. 4. Синхронизация времени журналов регистрации событий с единым источником времени. 5. Процедуры управления изменениями при установке новых версий прикладного и системного ПО в эксплуатируемых системах. 6. Контроль и управление уязвимостями ПО. 7. Ознакомление сотрудников и реализация положений ЕТ. 8. Разработка (актуализация), ознакомление сотрудников, реализация положений инструкции по организации удаленной работы. 9. Мониторинг работоспособности объекта испытаний. 10. Разделение сред разработки, тестирования и эксплуатации. 11. Обеспечение конфиденциальности при передаче сообщений электронной почты и информации посредством Интернет. 12. Способа предоставления Интернета и взаимодействия с внешними электронными почтовыми системами в соответствии с требованиями законодательства. 13. Ограничения и порядок фильтрации при доступе к ресурсам Интернета.
		1. Определение (актуализация), документирование законодательных, нормативных, иных обязательных, договорных требований для объекта испытаний. 2. Внедрение процедур, реализующих соответствие законодательным, нормативным и договорным требованиям, связанным с правами на интеллектуальную собственность.

12	Соответствие законодательным и договорным требованиям	3. Разработка и реализация политик защиты конфиденциальных и персональных данных, соответствующих нормам законодательства. 4. Соответствие применяемых криптографических методов и средств требованиям законодательства и соглашениям (договорам). 5. Проведение аудита кибербезопасности. 6. Проведение анализа объекта испытаний на предмет соответствия требованиям законодательства, стандартов и нормативно-технической документации по кибербезопасности. 7. Защита записей от потери, повреждения, фальсификации, несанкционированного доступа и несанкционированного выпуска в соответствии с законодательными, нормативными, договорными требованиями.
13	Приобретение, разработка и обслуживание систем	1. Включение (актуализация) требований, связанных с кибербезопасностью и соответствующих действующему законодательству и стандартам в состав нормативно-технической документации на объект испытаний. 2. Определение и применение безопасных процедур управления изменениями ПО (системного и прикладного) для эксплуатируемых систем. 3. Контроль процесса разработки ПО объекта испытаний, в том числе, осуществляемой сторонней организацией. 4. Контроль процесса технического сопровождения системы, осуществляемого сторонней организацией. 5. Тестирование функций безопасности системы.

Приложение 2 к приказу
Исполняющий
обязанности министра

искусственного интеллекта
и цифрового развития
Республики Казахстан
от 22 июня 2026 года № 345/НҚ
Приложение 2 к приказу
Министра цифрового
развития, оборонной
и аэрокосмической
промышленности
Республики Казахстан
от 3 июня 2019 года № 111/НҚ

Правила проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности

Глава 1. Общие положения

1. Настоящие Правила проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности (далее – Правила) разработаны в соответствии с подпунктом 5) статьи 7-1 Закона Республики Казахстан "О кибербезопасности" (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 цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности.

2. В настоящих Правилах используются следующие понятия и сокращения:

1) программное обеспечение – цифровой объект, представляющий собой подготовленную для использования совокупность кодов, реализующих алгоритмы, обеспечивающих выполнение определенных функций, обработку, хранение, воспроизведение и (или) передачу цифровых данных.

2) исходный код – тексты программ, выраженные на языке программирования, предназначенные для создания, модификации и поддержки программного обеспечения;

3) кибербезопасность – состояние защищенности цифровых объектов от нарушения их конфиденциальности, целостности или доступности;

4) нормативно-техническая документация по кибербезопасности – документация, устанавливающая политику, защитные меры, касающиеся процессов обеспечения кибербезопасности цифровых объектов и (или) организации;

5) интернет-портал уполномоченного органа в сфере обеспечения кибербезопасности – интернет-портал, предназначенный для мониторинга состояния кибербезопасности цифровых объектов;

6) поставщик – государственная техническая служба или аккредитованная испытательная лаборатория;

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

8) заявитель – собственник или владелец объекта испытаний, а также физическое или юридическое лицо, уполномоченное собственником или владельцем объекта испытаний, подавший(ее) заявку на проведение испытаний цифрового объекта на соответствие требованиям кибербезопасности;

9) испытательная лаборатория – юридическое лицо или структурное подразделение юридического лица, действующее от его имени, уполномоченное проводить испытания на соответствие требованиям кибербезопасности и аккредитованное в соответствии с законодательством о техническом регулировании;

10) интернет-портал SYNAQ – интернет-портал государственной технической службы, предназначенный для автоматизации процесса оказания услуги по испытаниям цифровых объектов на соответствие требованиям кибербезопасности;

11) объекты испытаний – цифровые объекты "цифрового правительства" и критически важные цифровые объекты, в отношении которых проводятся работы по испытанию на соответствие требованиям кибербезопасности;

12) цифровая система – функционально связанный комплекс цифровых ресурсов, использующий объекты цифровой инфраструктуры с целью обеспечения создания, сбора, обработки, хранения и распространения цифровых данных, а также автоматизирующий взаимодействие субъектов цифровой среды и (или) обеспечивающий оказание услуг в цифровой среде;

13) подсистема цифровой системы – совокупная часть (компонент или модуль) цифровой системы, реализующая ее определенные функции, необходимые для достижения назначения цифровой системы;

14) платформа "цифрового правительства" – цифровая платформа оператора, предназначенная для разработки, развития, размещения, интеграции платформенных программных продуктов и (или) размещения цифровых объектов;

15) программный продукт платформы "цифрового правительства" (далее – платформенный программный продукт) – программное обеспечение, разработанное и размещенное на платформе "цифрового правительства";

16) среда штатной эксплуатации – целевой набор серверного оборудования, сетевой инфраструктуры, системного программного обеспечения, используемый на этапе опытной эксплуатации (пилотного проекта) и предназначенный для применения на этапе промышленной эксплуатации цифрового объекта.

Глава 2. Порядок проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности

3. Испытания объектов на соответствие требованиям кибербезопасности (далее – испытания) включают в себя работы по оценке соответствия объектов испытаний требованиям нормативно-технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов по кибербезопасности и проводятся в среде штатной эксплуатации объекта испытаний.

4. В состав испытаний объекта испытаний, за исключением программного обеспечения (программного продукта) созданного и (или) размещенного на платформе "цифрового правительства" и платформы "цифрового правительства" входят следующие виды работ:

1) анализ исходных кодов;

2) испытание функций кибербезопасности;

3) нагрузочное испытание;

4) обследование сетевой инфраструктуры;

5) обследование процессов обеспечения кибербезопасности.

5. При отсутствии исходного кода объекта испытания или невозможности проведения другого(их) вида(ов) испытаний (за исключением цифровых объектов " цифрового правительства"), решение о необязательности проведения анализа исходного кода или другого(их) вида(ов) испытаний объекта испытаний устанавливается решением уполномоченного органа в сфере обеспечения кибербезопасности по запросу заявителя.

Уполномоченный орган в сфере обеспечения кибербезопасности 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.

6. В испытания программного обеспечения (платформенного программного продукта) созданного и (или) размещенного на цифровой платформе "цифрового правительства" входит:

1) анализ исходных кодов, включая статический и динамический анализ, анализ зависимостей;

2) испытания функций кибербезопасности;

3) нагрузочное испытание.

7. В испытания платформы "цифрового правительства" входит:

1) анализ исходных кодов;

2) испытание функций кибербезопасности;

3) нагрузочное испытание;

4) обследование сетевой инфраструктуры;

5) обследование процессов обеспечения кибербезопасности.

8. В случае интеграции (действующей или планируемой) объекта испытаний с другим цифровым объектом, испытания проводятся с включением в состав объекта испытаний компонентов, обеспечивающих интеграции (модуль интеграции, подсистема интеграции, интеграционная шина или другое).

9. Испытания проводятся согласно Методике проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности.

10. Собственники и (или) владельцы объектов испытаний передают исходные коды цифровых объектов, получивших положительные протоколы испытаний в соответствии с Правилами функционирования Национального репозитория исходных кодов, утвержденными приказом Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 29 февраля 2024 года № 110/НҚ (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 34101).

Глава 3. Порядок проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности в государственной технической службе

11. Для проведения испытаний заявителем на интернет-портале SYNAQ заполняется, подписывается электронной цифровой подписью (далее – ЭЦП) и подается заявка на проведение испытаний (далее – заявка) в государственную техническую службу по форме, согласно приложению 1 к настоящим Правилам, с приложением следующих документов:

1) анкета-вопросник о характеристиках объекта испытаний согласно приложению 2 к настоящим Правилам, удостоверенная ЭЦП собственника (владельца) объекта испытаний на интернет-портале SYNAQ;

2) электронная копия доверенности на лицо, уполномоченное на подписание договоров или документа о назначении руководителя юридического лица (для юридических лиц);

3) электронная копия согласованного с уполномоченным органом в сфере цифровизации и уполномоченным органом в сфере обеспечения кибербезопасности технического задания на цифровой объект;

4) исходные коды компонентов и модулей объекта испытаний с библиотеками и файлами, необходимыми для успешной компиляции (при необходимости);

5) электронные копии утвержденной нормативно-технической документации по кибербезопасности объекта испытаний, согласно приложению 3 к настоящим Правилам в электронном виде (при необходимости);

6) электронная копия документа, уполномочивающего заявителя владельцем (собственником) подать заявку на проведение испытаний (при необходимости).

12. При осуществлении заявителем закупки посредством веб-портала государственных закупок, заявка на проведение испытаний принимается не позднее 1 (первого) ноября текущего года.

13. Государственная техническая служба в течение 3 (трех) рабочих дней со дня получения заявки осуществляет проверку полноты документов, указанных в пункте 11 настоящих Правил.

14. В случае несоответствия заявки и приложенных документов в соответствии с требованиями, указанными в пункте 11 настоящих Правил, в течение 10 (десяти) рабочих дней заявка возвращается заявителю с указанием причин возврата.

15. Государственная техническая служба после проверки заявки на наличие полного пакета документов согласно пункту 11 настоящих Правил в течение 3 (трех) рабочих дней направляет заявителю:

1) проект технической спецификации к договору на проведение испытаний при осуществлении закупки посредством веб-портала государственных закупок. Заявитель в течение 3 (трех) рабочих дней со дня получения проекта технической спецификации размещает на веб-портале государственных закупок проект договора о государственных закупках способом из одного источника путем прямого заключения договора о государственных закупках;

2) два экземпляра договора на проведение испытаний при осуществлении закупки без применения веб-портала государственных закупок.

Заявитель в течение 5 (пяти) рабочих дней со дня получения двух экземпляров вышеуказанного договора подписывает их и возвращает один экземпляр договора в государственную техническую службу.

16. При отсутствии договора о государственных закупках, направленного посредством веб-портала государственных закупок в адрес государственной технической службы позднее 15 ноября текущего года, заявка аннулируется и возвращается заявителю.

17. Срок испытаний согласовывается с заявителем и зависит от объема работ по испытаниям и классификационных характеристик объекта испытаний.

При отсутствии согласования сроков проведения испытания, заявка возвращается заявителю без удовлетворения с указанием возможности обратиться в уполномоченный орган в сфере обеспечения кибербезопасности для определения сроков испытаний.

18. Для проведения испытаний заявитель обеспечивает:

1) рабочее место, физический доступ к рабочему месту пользователя, серверному и сетевому оборудованию, сети телекоммуникаций объекта испытаний с проведением фото и видео фиксации и к документации на объект испытания и сопутствующей документации, в том числе к договорам на сопровождение и техническую поддержку объекта испытаний и компонентов, входящих в состав объекта испытаний;

2) демонстрацию функций объекта испытаний, согласно требованиям нормативно-технической документации.

19. При невозможности обеспечения заявителем требований пункта 18 настоящих Правил, испытания приостанавливаются на время, необходимое Заявителю для их обеспечения с учетом подписания дополнительного соглашения к договору на продление его срока исполнения.

20. При выявлении расхождений между данными анкеты-вопросника о характеристиках объекта испытаний, поданной в соответствии с подпунктом 1) пункта 11 настоящих Правил и фактическим состоянием объекта испытаний, заявитель направляет в государственную техническую службу обновленную анкету-вопросник о характеристиках объекта испытаний, удостоверенную ЭЦП собственника (владельца) объекта испытаний на интернет-портале SYNAQ. Обновленная анкета-вопросник о характеристиках объекта испытаний (при необходимости) будет основанием для заключения дополнительного соглашения на продление срока испытаний и изменение стоимости проведения испытаний.

21. При выявлении необходимости проведения повторного испытания по одному или по нескольким видам испытаний до окончания срока испытания, заявитель обращается с запросом в государственную техническую службу и заключается дополнительное соглашение о проведении повторного испытания на безвозмездной основе по этим видам работ.

22. Результаты работ, входящих в испытания, и рекомендации по устранению выявленных несоответствий вносятся в отдельные протоколы, размещаемые на интернет-портале SYNAQ в личном кабинете заявителя по завершению всех видов работ.

23. Цены на проведение государственной технической службой каждого вида работ, входящих в испытания, устанавливаются согласно пункту 2 статьи 14 Закона.

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) цифрового объекта на интернет-портале SYNAQ.

25. При устранении заявителем выявленных при испытаниях несоответствия в течение 60 (шестидесяти) рабочих дней со дня размещения на интернет-портале SYNAQ протоколов испытаний по проведенным работам и направления в государственную техническую службу запроса на проведение повторных испытаний с приложением сравнительной таблицы с результатами исправления выявленных несоответствий посредством интернет-портала SYNAQ, государственная техническая

служба на безвозмездной основе в течение 20 (двадцати) рабочих дней со дня получения от заявителя запроса проводит повторные испытания по данным видам работ с оформлением соответствующих документов.

26. Заявитель подает заявку на повторные испытания не более двух раз, в установленный срок.

При необходимости, заявитель единожды увеличивает срок устранения выявленных при испытаниях несоответствий путем подачи дополнительной заявки на увеличение срока устранения выявленных несоответствий, но не более 20 (двадцати) рабочих дней.

Пропуск установленного срока является основанием для проведения испытаний в общем порядке, установленном настоящими Правилами.

27. При проведении повторных испытаний после исправления несоответствий, связанных с внесением изменений в ПО объекта, проводится анализ исходного кода.

При этом заявитель к запросу на проведение повторных испытаний прикладывает исходные коды компонентов и модулей объекта испытаний с библиотеками и файлами, необходимыми для успешной компиляции объекта испытаний.

28. При выявлении несоответствий во время проведения повторных испытаний государственная техническая служба оформляет протокол с отрицательным заключением, после чего испытания проводятся в порядке, установленном в главе 3 настоящих Правил.

Глава 4. Порядок проведения испытаний цифровых объектов "цифрового правительства" и критически важных цифровых объектов на соответствие требованиям кибербезопасности в испытательных лабораториях

29. Порядок заключения договоров на проведение испытаний в испытательных лабораториях определяется в соответствии с Гражданским кодексом Республики Казахстан.

30. Для проведения испытаний заявителем направляется заявка на бумажном носителе поставщику согласно приложению 1 к настоящим Правилам, с предоставлением следующих документов:

1) копия доверенности на лицо, уполномоченное на подписание договоров или документа о назначении руководителя юридического лица (для юридических лиц);

2) анкета-вопросник о характеристиках объекта испытаний согласно приложению 2 к настоящим Правилам, утвержденный собственником или владельцем объекта испытаний на бумажном носителе;

3) утвержденные собственником или владельцем техническое задание или техническая спецификация на цифровой объект, за исключением цифрового объекта " цифрового правительства", на компакт-диске (при необходимости);

4) исходные коды компонентов и модулей объекта испытаний с библиотеками и файлами, необходимыми для успешной компиляции, на компакт-диске (при необходимости);

5) копии утвержденного перечня нормативно-технической документации по кибербезопасности объекта испытаний, согласно приложению 3 к настоящим Правилам в электронном виде на компакт-диске (при необходимости);

6) документ, уполномочивающий заявителя собственником или владельцем подать заявку на проведение испытаний (при необходимости).

31. После устранения заявителем выявленных при испытаниях несоответствий в течение 20 (двадцати) рабочих дней со дня получения протоколов испытаний, заявитель направляет поставщику заявку на проведение повторных испытаний с приложением сравнительной таблицы. Поставщик обязуется провести повторные испытания в течение 20 (двадцати) рабочих дней со дня получения уведомления на безвозмездной основе и оформить соответствующие документы.

32. Заявитель подает заявку на проведение повторных испытаний не более двух раз, в установленный срок.

33. Заявитель вправе однократно увеличить срок устранения выявленных при проведении испытаний несоответствий, подав дополнительную заявку на увеличение срока их устранения, но не более чем на 20 (двадцать) рабочих дней.

Несвоевременная подача заявки на проведение повторных испытаний является основанием для проведения испытаний в общем порядке, установленном настоящими Правилами.

34. При выявлении несоответствий в ходе повторных испытаний поставщик оформляет протокол с отрицательным заключением, после чего испытания проводятся в порядке, установленном в главе 3 настоящих Правил.

35. При утере, порче или повреждении протоколов испытаний собственник или владелец объекта испытаний направляет поставщику уведомление с указанием причин.

Поставщик в течение 5 (пяти) рабочих дней со дня получения уведомления выдает дубликат протоколов испытаний.

Глава 5. Порядок выдачи и отзыва протоколов испытаний

36. Протоколы испытаний выдаются поставщиком.

37. Срок действия протоколов испытаний выдается сроком на 3 (три) года для всех объектов испытаний, за исключением платформы "цифрового 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 цифрового объекта не превышает одного года с даты выдачи протокола.

Собственник или владелец цифрового объекта за 3 (три) месяца до окончания срока действия протоколов испытаний подает заявку поставщику о прохождении испытаний в порядке, установленном главами 3 или 4 настоящих Правил.

Протоколы испытаний платформы "цифрового правительства" выдаются со сроком действия 1 (один) год.

38. Поставщик на постоянной основе предоставляет в уполномоченный орган в сфере обеспечения кибербезопасности следующие данные:

1) заявку 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 кибербезопасности 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 кибербезопасности.

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 кибербезопасности.

39. При изменении условий функционирования и (или) функциональности, и (или) изменении прав собственности цифрового объекта, собственник или владелец цифрового объекта 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.

40. Уполномоченный орган в сфере обеспечения кибербезопасности при выявлении несоответствий требованиям настоящих Правил, направляет поставщику информацию с приложением выявленных несоответствий.

41. Поставщик в срок не более 10 (десяти) рабочих дней рассматривает внесенные изменения в цифровой объект и (или) информацию о выявленных несоответствиях, и (или) информацию об изменениях исходного кода по результатам анализа неизменности и принимает решение об отзыве протоколов испытаний и необходимости проведения того вида испытаний функции которого были нарушены при изменении условий функционирования и (или) функциональности цифрового объекта.

Решение принимается с учетом Перечня изменений функционирования и (или) функциональности цифрового объекта согласно приложению 4 к настоящим Правилам.

42. При отзыве протоколов испытаний, собственник или владелец в трехмесячный срок подает заявку поставщикам о прохождении испытаний в порядке, установленном главами 3 или 4 настоящих Правил.

43. В случае несогласия заявителя с результатами протоколов испытаний, обжалование административного действия (бездействия), осуществляется в соответствии со статьей 91 Административного процедурно-процессуального кодекса Республики Казахстан.

Приложение 1
к Правилам проведения
испытаний цифровых объектов
"цифрового правительства" и
критически важных цифровых
объектов на соответствие
требованиям кибербезопасности
Форма

_____

__

(наименование поставщика)

Заявка на проведение испытаний

_____

(наименование объекта испытаний)

на соответствие требованиям кибербезопасности (далее – испытания)

1. _____

(наименование организации-заявителя, фамилия, имя, отчество (при наличии), бизнес-идентификационный номер, банковские реквизиты заявителя)

_____

_____

(почтовый адрес, эл. почта и телефон заявителя, область, город, район) просит провести испытания

_____

(наименование объекта испытаний, номер версии, дата разработки) в составе следующих видов работ:

1) _____

2) _____
3) _____
4) _____
5) _____

(перечень видов работ согласно пунктов 4,6,7 настоящих Правил (указать нужный пункт)

2. Сведения о владельце (собственнике) испытываемого объекта испытаний

_____

(наименование или фамилия, имя, отчество (при наличии)

_____

_____

(область, город, район, почтовый адрес, телефон)

3. Сведения о разработчике испытываемого объекта испытаний

_____

(информация о разработчике, наименование или фамилия, имя, отчество (при наличии) авторов)

_____

(область, город, район, почтовый адрес, телефон)

4. Данные лица, ответственного за связь с поставщиком:

1) фамилия, имя, отчество: _____;
2) должность: _____;
3) телефон рабочий: _____, телефон сотовый: _____;
4) адрес электронной почты: _____@_____.

Руководитель организации – заявителя (фамилия, имя, отчество (при наличии), заявителя _____ (подпись, дата)

(место печати) при наличии

Приложение 2
к Правилам проведения
испытаний цифровых объектов
"цифрового правительства" и
критически важных цифровых
объектов на соответствие
требованиям кибербезопасности
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 согласно классификатору цифровых объектов, утверждаемому в соответствии с пунктом 3 статьи 20 Цифрового Кодекса Республики Казахстан.

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 цифровыми объектами;

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:

№ п/п	Наименование сервера или виртуального ресурса (доменное имя, сетевое имя или	Назначение (выполняемые функциональные задачи)	Количество	Характеристики сервера или используемых	Операционная система (далее – ОС), система управления базами данных (далее – СУБД), программное обеспечение (далее – ПО), приложения, библиотеки и средства защиты, установленны	

	логическое имя сервера)			заявленных виртуальных ресурсов	е на серверах и л и 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, п о р т 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 л и ц а за организацию доступа (фамилия, имя, отчество (при наличии)	Телефоны ответственных лиц (рабочие, сотовые)
1	2	3	4	5	6

4) характеристики резервного серверного оборудования:

№ п/п	Наименование сервера и л и виртуального ресурса (доменное имя, сетевое имя или логическое имя сервера)	Назначение (выполняемы е функциональные задачи)	Количество	Характеристики сервера или используемы х заявленных виртуальных ресурсов	ОС, СУБД, П О , приложения , библиотеки и средства защиты, установленные на 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 (выполняемые функциональные задачи)	Количество	Применяемые сетевые технологии	Применяемые технологии защиты сети	Используемые 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:

№ п/п	Роль пользователя	Перечень типовых действий пользователя	Адрес и порт точки подключения пользователей к объекту испытаний	Протокол подключения пользователей к объекту испытаний	Количество пользователей согласно нормативно-технической документации на создание или развитие объекта испытаний	Максимальное количество, обрабатываемых запросов (пакетов) в секунду	Максимальное время 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 (цифрового объекта)	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 кибербезопасности				
2.	Методика оценки рисков кибербезопасности				
	Правила идентификации, классификации, маркировки,				

3.	паспортизации активов, связанных со средствами обработки информации и их инвентаризации				
4.	Правила проведения внутреннего аудита кибербезопасности				
5.	Правила использования средств криптографической защиты информации				
6.	Правила организации процедуры аутентификации и разграничения прав доступа к цифровым 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 цифрового объекта, резервному копированию и восстановлению информации				
10.	Инструкцию о порядке действий пользователей по реагированию на инциденты кибербезопасности и во внештатных (кризисных) ситуациях				

Приложение 3
к Правилам проведения
испытаний цифровых объектов
"цифрового правительства" и
критически важных цифровых
объектов на соответствие
требованиям кибербезопасности
Форма

Перечень нормативно-технической документации по кибербезопасности объекта испытаний

1. Политика кибербезопасности;
2. Методика оценки рисков кибербезопасности;
3. Правила идентификации, классификации, маркировки, паспортизации активов, связанных со средствами обработки информации и их инвентаризации;
4. Правила проведения внутреннего аудита кибербезопасности;
5. Правила использования средств криптографической защиты информации;
6. Правила организации процедуры аутентификации и разграничения прав доступа к цифровым 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 цифрового объекта, резервному копированию и восстановлению информации;

10. Инструкция о порядке действий пользователей по реагированию на инциденты кибербезопасности и во внештатных (кризисных) ситуациях.

Приложение 4
к Правилам проведения
испытаний цифровых объектов
"цифрового правительства" и
критически важных цифровых
объектов на соответствие
требованиям кибербезопасности
Форма

Перечень изменений функционирования и (или) функциональности цифрового объекта

№ п/п	Произведенные изменения	Анализ исходных кодов	Функции кибербезопасности	Нагрузочное испытание	Обследование сетевой инфраструктуры	Обследование процессов обеспечения кибербезопасности
1	2	3	4	5	6	7
1.	Изменение среды разработки (язык программирования)	+	-	-	-	-
2.	Изменение функции прикладного программного обеспечения	+	+	+	-	-
3.	Замена серверного оборудования	-	+	+	+	+
4.	Замена сетевого оборудования	-	-	+	+	-
5.	Изменение типа операционной системы, системы управления базами данных	-	+	+	-	-
6.	Изменение место	-	+	-		+

	расположения объекта испытаний				+	
7.	Миграция объекта испытаний из внутреннего контура на внешний контур или на оборот	-	+	+	+	+
8.	Добавление нового компонента (сервера)	-	+	-	+	+
9.	Новая интеграция с другими цифровыми системами	+	+	+	+	+
10.	Изменение класса цифрового объекта	-	+	-	+	+
11.	Изменение прав собственности и (или) владения цифрового объекта (изменение собственника и/или владельца)	-	-	-	-	+