Об утверждении методики и правил проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы " электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности

Утративший силу

Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 14 марта 2018 года № 40/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 30 марта 2018 года № 16694. Утратил силу приказом Министра цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан от 3 июня 2019 года № 111/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования)

Сноска. Утратил силу приказом Министра цифрового развития, оборонной и аэрокосмической промышленности РК от 03.06.2019 № 111/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

В соответствие с подпунктом 5) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" ПРИКАЗЫВАЮ:

1. Утвердить:

1) Методику проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности согласно приложению 1 к настоящему приказу;

2) Правила проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности согласно приложению 2 к настоящему приказу.

2. Признать утратившим силу приказ исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 63 " Об утверждении методики и правил проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы " электронного правительства", интернет-ресурса государственного органа и

информационной системы на соответствие требованиям информационной безопасности" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 13207, опубликован 1 марта 2016 года в информационно-правовой системе "Әділет").

3. Комитету по информационной безопасности Министерства оборонной и аэрокосмической промышленности Республики Казахстан в установленном законодательством порядке обеспечить:

1) государственную регистрацию настоящего приказа в Министерстве юстиции Республики Казахстан;

2) в течение десяти календарных дней со дня государственной регистрации настоящего приказа направление его копии в бумажном и электронном виде на казахском и русском языках в Республиканское государственное предприятие на праве хозяйственного ведения "Республиканский центр правовой информации" для официального опубликования и включения в Эталонный контрольный банк нормативных правовых актов Республики Казахстан;

3) в течение десяти календарных дней после государственной регистрации настоящего приказа направление его копии на официальное опубликование в периодические печатные издания;

4) размещение настоящего приказа на официальном интернет-ресурсе Министерства оборонной и аэрокосмической промышленности Республики Казахстан после его официального опубликования;

5) в течение десяти рабочих дней после государственной регистрации настоящего приказа в Министерстве юстиции Республики Казахстан представление в Юридический департамент Министерства оборонной и аэрокосмической промышленности Республики Казахстан сведений об исполнении мероприятий, предусмотренных подпунктами 1), 2) 3) и 4) настоящего пункта.

4. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра оборонной и аэрокосмической промышленности Республики Казахстан.

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

Министр оборонной и аэрокосмической промышленности Республики Казахстан *Б. Атамкулов*

Приложение 1
к приказу Министра
оборонной и аэрокосмической
промышленности

Республики Казахстан
от 14 марта 2018 года № 40/НҚ

Методика
проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности

Глава 1. Общие положения

1. Настоящая Методика проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности (далее – Методика) разработана в соответствие с подпунктом 5) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации.

2. В настоящей Методике используются следующие основные понятия и сокращения:

1) уязвимость – недостаток в программном обеспечении, обуславливающий возможность нарушения его работоспособности, либо выполнения каких-либо несанкционированных действий в обход разрешений, установленных в программном обеспечении;

2) экспертный метод – метод поиска и результат его применения, полученный на основании использования персонального мнения эксперта или коллективного мнения группы экспертов;

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

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

3. Проведение испытания включает:

1) анализ исходных кодов;

2) испытание функций информационной безопасности;

3) нагрузочное испытание;

4) обследование сетевой инфраструктуры.

Глава 2. Анализ исходных кодов

4. Анализ исходных кодов объектов испытаний проводится с целью выявления недостатков (программных закладок и уязвимостей) программного обеспечения (далее – ПО).

5. Анализ исходных кодов проводится для ПО, перечисленного в акте приема-передачи исходных кодов объектов испытаний, согласно Правилам проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности (далее- Правила).

6. Если при проведении испытания выявится необходимость проведения повторного анализ исходных кодов до окончания срока испытания, заявитель обращается с запросом в ГТС и заключается дополнительное соглашение о проведении повторного анализа исходных кодов в соответствии с пунктом 25 Правил.

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

8. Анализ исходных кодов включает:

1) выявление недостатков ПО;

2) фиксацию результатов анализа исходного кода.

9. Выявление недостатков ПО осуществляется в следующем порядке:

1) проводится подготовка исходных данных (загрузка исходных кодов сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа, информационная система (далее-ОИ), выбор режима сканирования (динамический и/или статический), настройка характеристик режимов сканирования);

2) запускается программное средство, предназначенное для выявления недостатков ПО;

3) проводится анализ программных отчетов на наличие ложных срабатываний;

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

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

11. Результаты анализа исходных кодов фиксируются ответственным исполнителем данного вида работ, в Протоколе анализа исходных кодов (Произвольная форма).

12. По окончанию проведенного анализа исходных кодов при условии его положительного результата, исходные коды объекта испытаний маркируются и сдаются в опечатанном виде на ответственное хранение в архив ГТС.

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

Глава 3. Испытание функций информационной безопасности

14. Оценка функций сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности (далее - испытание функций информационной безопасности) осуществляется с целью оценки их соответствия требованиям технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов в сфере информатизации.

15. Испытание функций информационной безопасности включает:

1) оценку соответствия функций безопасности требованиям технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов в сфере информатизации;

2) фиксацию результатов оценки.

16. Перечень функций информационной безопасности приведены в приложении 1 настоящей Методики.

17. Испытание функций информационной безопасности проводятся в разрезе серверов и виртуальных ресурсов.

18. Результаты испытаний функций информационной безопасности фиксируются ответственным исполнителем данного вида работ в Протоколе испытаний функций информационной безопасности (Произвольная форма).

Глава 4. Нагрузочное испытание

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

20. 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.

21. Параметры нагрузочного испытания предоставляются заявителем в Анкете-вопроснике о характеристиках объекта испытаний согласно приложению 2 Правил.

22. Нагрузочное испытание осуществляется в следующем порядке:

1) проводится подготовка к испытанию;

2) проводится испытание;

3) фиксируются результаты испытания.

23. Подготовка к испытанию включает:

1) определение сценария испытания;

2) определение временных и количественных характеристик испытания;

3) согласование времени проведения испытания с заказчиком.

24. 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.

25. Работы по проведению нагрузочного тестирования проводятся для одного объекта испытаний по количеству вариантов подключений пользователей и вариантов интеграционного взаимодействия объекта испытаний.

26. Результаты нагрузочного испытания фиксируются ответственным исполнителем данного вида работ в Протоколе нагрузочного испытания (произвольная форма).

Глава 5. Обследование сетевой инфраструктуры

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

28. Обследование сетевой инфраструктуры включает:

1) оценку соответствия функций защиты сетевой инфраструктуры требованиям технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов в сфере информатизации;

2) обследование сетевой инфраструктуры заявителя;

3) фиксацию полученных результатов.

29. Перечень функций защиты сетевой инфраструктуры приведены в приложении 2 настоящей Методики.

30. Работы по обследованию сетевой инфраструктуры, проводятся для каждой подсети (сегмента сети) объекта испытаний.

31. Результаты обследования сетевой инфраструктуры фиксируются ответственным исполнителем данного вида работ в Протоколе обследования сетевой инфраструктуры (произвольная форма).

Приложение 1
к Методике проведения испытаний
сервисного программного продукта,
информационно-коммуникационной
платформы "электронного
правительства", интернет-ресурса
государственного органа и
информационной системы на
соответствие требованиям
информационной безопасности

Перечень функций информационной безопасности

№ п/п	Наименование функций	Содержание функций
1	2	3
Аудит безопасности		
1	Автоматическая реакция аудита безопасности	Осуществление генерации записи в регистрационном журнале, локальной или удаленной 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, т.е. 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 должен быть закрыт, за исключением явно специфицированных случаев
5	Выбор событий аудита безопасности	Наличие избирательности регистрации событий, основывающейся, по крайней мере, на следующих атрибутах: идентификатор объекта; идентификатор субъекта; адрес узла сети; тип события; дата и время события
6	Хранение данных аудита безопасности	Наличие регистрационной информации о надежности защиты от несанкционированной модификации
Организация связи		

7	Неотказуемость отправления	Предоставление пользователям/субъектам свидетельства идентичности отправителя некоторой информации, чтобы отправитель не смог отрицать факт передачи информации, поскольку свидетельство отправления (например, цифровая подпись) доказывает связь между отправителем и переданной информацией
8	Неотказуемость получения	Обеспечение невозможности отрицания получателем информации факта ее получения
Криптографическая поддержка		
9	Управление криптографическими ключами	Наличие поддержки: 1) генерации криптографических ключей; 2) распределения криптографических ключей; 3) управления доступом к криптографическим ключам; 4) уничтожения криптографических ключей
10	Криптографические операции	Наличие для всей информации, передаваемой по доверенному каналу, шифрования и контроля целостности в соответствии с требованиями технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов в сфере информатизации.
Защита данных пользователя		
11	Политика управления доступом	Осуществление разграничения доступа для пользователей, прямо или косвенно выполняющих операции с сервисом безопасности
12	Функции управления доступом	Применение функций разграничения доступа основывается, по крайней мере, на следующих атрибутах безопасности: идентификаторы субъектов доступа; идентификаторы объектов доступа; адреса субъектов доступа; адреса объектов доступа; права доступа субъектов
13	Аутентификация данных	Поддержка гарантии правильности специфического набора данных, который впоследствии используется для верификации того, что содержание информации не было подделано или модифицировано мошенническим путем
14	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
15	Политика управления информационными потоками	Обеспечение предотвращения раскрытия, модификации и/или недоступности данных пользователя при их передаче между физически разделенными частями сервиса безопасности
16	Функции управления информационными потоками	Организация и обеспечение контроля доступа к хранилищам данным с целью исключения бесконтрольного распространения информации, содержащейся в них (управление информационными потоками для реализации надежной защиты от раскрытия или модификации в условиях недоверенного ПО)
17	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
18	Передача в пределах ОИ	Наличие защиты данных пользователя при их передаче между различными частями ОИ по внутреннему каналу

19	Защита остаточной информации	Обеспечение полной защиты остаточной информации, то есть недоступности предыдущего состояния при освобождении ресурса
20	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
21	Целостность хранимых данных	Обеспечение защиты данных пользователя во время их хранения в пределах ФБО
22	Защита конфиденциальности данных пользователя при передаче между ФБО	Обеспечение конфиденциальности данных пользователя при их передаче по внешнему каналу между ОИ и другим доверенным продуктом ИТ. Конфиденциальность осуществляется путем предотвращения несанкционированного раскрытия данных при их передаче между двумя оконечными точками. Оконечными точками могут быть ФБО или пользователь
23	Защита целостности данных пользователя при передаче между ФБО	обеспечивается целостность данных пользователя при их передаче между ФБО и другим доверенным продуктом ИТ, а также возможность их восстановления при обнаруживаемых ошибках
Идентификация и аутентификация		
24	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
25	Определение атрибутов пользователя	Для каждого пользователя необходимо поддерживать, по крайней мере, следующие атрибуты безопасности: идентификатор; аутентификационная информация (например, пароль); права доступа (роль)
26	Спецификация секретов	Если аутентификационная информация обеспечивается криптографическими операциями, поддерживается также открытые и секретные ключи
27	Аутентификация пользователя	Наличие механизмов аутентификации пользователя, предоставляемых ФБО
28	Идентификация пользователя	Обеспечение: 1) успешности идентификации и аутентификации каждого пользователя до разрешения любого действия, выполняемого 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
29	Связывание пользователь-субъект	Следует ассоциировать соответствующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя
Управление безопасностью		
30	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

31	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
32	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
33	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
34	Срок действия атрибута безопасности	Обеспечение возможности установления срока действия атрибутов безопасности
35	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		
36	Безопасность при сбое	Сохранение сервисом безопасного состояния при аппаратных сбоях (вызванных , например, перебоями электропитания)
37	Доступность экспортируемых данных ФБО	Предоставление сервисом возможности верифицировать доступность, всех данных при их передаче между ним и удаленным доверенным продуктом ИТ и выполнять повторную передачу информации, а также генерировать запись регистрационного журнала, если модификации обнаружены
38	Конфиденциальность экспортируемых данных ФБО	Предоставление сервисом возможности верифицировать конфиденциальность всех данных при их передаче между ним и удаленным доверенным продуктом ИТ и выполнять повторную передачу информации, а также генерировать запись регистрационного журнала, если модификации обнаружены
39	Целостность экспортируемых данных ФБО	Предоставление сервисом возможности верифицировать целостность всех данных при их передаче между ним и удаленным доверенным продуктом ИТ и выполнять повторную передачу информации, а также генерировать запись регистрационного журнала, если модификации обнаружены
40	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 изделием ИТ и выполнять повторную передачу информации, а также генерировать запись регистрационного журнала, если модификации обнаружены
41	Физическая защита ФБО	Осуществление физической защиты ФБО
42	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
		Обеспечение обнаружения сервисом повторного использования аутентификационных данных, отказа в доступе, генеририрования записи

43	Обнаружение повторного использования	регистрационного журнала и сигнализирования администратору о вероятном нарушении безопасности
44	Посредничество при обращениях	Обеспечение вызова и успешного выполнения функций, осуществляющих политику безопасности сервиса, прежде, чем разрешается выполнение любой другой функции сервиса
45	Разделение домена	Поддержка отдельного домена для собственного выполнения функций безопасности, который защищает их от вмешательства и искажения недоверенными субъектами
46	Протокол синхронизации состояний	Обеспечение синхронизации состояний при выполнении идентичных функций на серверах
47	Метки времени	Предоставление для использования функциями безопасности надежных меток времени
48	Согласованность данных между ФБО	Обеспечение согласованной интерпретации регистрационной информации, а также параметров используемых криптографических операций
49	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
50	Самотестирование ФБО	Для демонстрации правильности работы функций безопасности при запуске, периодически в процессе нормального функционирования и/или по запросу администратора выполнение пакета программ самотестирования. У администратора наличие возможности верифицировать целостность данных и выполняемого кода функций безопасности
Использование ресурсов		
51	Отказоустойчивость	Обеспечение доступности функциональных возможностей объекта испытаний даже в случае сбоев. Примеры таких сбоев: отключение питания, отказ аппаратуры, сбой ПО
52	Приоритет обслуживания	Обеспечение управления использованием ресурсов пользователями и субъектами в пределах своей области действия так, что высокоприоритетные операции в пределах объекта испытаний всегда будут выполняться без препятствий или задержек со стороны операций с более низким приоритетом
53	Распределение ресурсов	Обеспечение управления использованием ресурсов пользователями и субъектами таким образом, чтобы не допустить несанкционированные отказы в обслуживании из-за монополизации ресурсов другими пользователями или субъектами
	Доступ к ОИ	
54	Ограничение области выбираемых атрибутов	Ограничение как атрибутов безопасности сеанса, которые может выбирать пользователь, так и атрибутов субъектов, с которыми пользователь может быть связан, на основе метода или места доступа, порта, с которого осуществляется доступ, и/или времени (например, времени суток, дня недели)
55	Ограничение на параллельные сеансы	Ограничение максимального числа параллельных сеансов, предоставляемых одному пользователю. У этой величины подразумеваемое значение устанавливается администратором
56	Блокирование сеанса	Принудительное завершение сеанса работы по истечении установленного администратором значения длительности бездействия пользователя

57	Предупреждения перед предоставлением доступа к ОИ	Обеспечение возможности еще до идентификации и аутентификации отображения для потенциальных пользователей предупреждающего сообщения относительно характера использования объекта испытаний
58	История доступа к ОИ	Обеспечение возможности отображения для пользователя, при успешном открытии сеанса, истории неуспешных попыток получить доступ от имени этого пользователя. Эта история может содержать дату, время, 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
59	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		
60	Наличие средств антивирусной защиты	Применение для защиты от вредоносного кода средств мониторинга, обнаружения и блокирования или удаления вредоносного кода на серверах и при необходимости, на рабочих станциях объекта испытаний
61	Лицензии для средств антивирусной защиты	Наличие у средств антивирусной защиты лицензии (приобретенной, ограниченной, свободно распространяемой) на сервера и рабочие станции
62	Обновление баз сигнатур и программного обеспечения средств антивирусной защиты	Обеспечение регулярного обновления и поддержания в актуальном состоянии средств антивирусной защиты
63	Управление доступом к средствам антивирусной защиты	Осуществление централизованного управления и конфигурирования средств антивирусной защиты
64	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		
65	Регулярное обновления ПО	Обеспечение регулярного обновления общесистемного и прикладного ПО серверов и рабочих станций
66	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		

67	Среда разработки и тестирования прикладного ПО	Обеспечение наличия среды для разработки и тестирования прикладного ПО, изолированной от среды промышленной эксплуатации прикладного ПО
67	Разграничение доступа в средам разработки и тестирования прикладного ПО	Обеспечение управления доступом к средам разработки и тестирования прикладного ПО для программистов и администраторов
69	Система развертывания прикладного ПО	Наличие системы развертывания (распространения) прикладного ПО на серверах и рабочих станциях среды промышленной эксплуатации
70	Разграничение доступа к системе развертывания прикладного ПО	Обеспечение управления доступом к системе развертывания (распространения) прикладного ПО на серверах и рабочих станциях среды промышленной эксплуатации

Приложение 2
к Методике проведения испытаний
сервисного программного продукта,
информационно-коммуникационной
платформы "электронного
правительства", интернет-ресурса
государственного органа и
информационной системы на
соответствие требованиям
информационной безопасности

Перечень функций защиты сетевой инфраструктуры

№ п/п	Наименование функций	Содержание функций
1	2	3
1	Идентификация и аутентификация	Обеспечение безопасности сервисов, предоставляемых сетевой инфраструктурой и предохранения соответствующих данных путем ограничения доступа через соединения к уполномоченному персоналу (внутри или за пределами организации)
2	Отметки аудитов (формирование и наличие отчетов о событиях, связанных с безопасностью сетевых соединений)	Достаточную информацию по следам аудита сбойных ситуаций и действительных событий следует фиксировать, чтобы иметь возможность тщательного критического обзора подозреваемых и действительных происшествий
3	Обнаружение вторжения	Обеспечение наличия средств, позволяющих прогнозировать вторжения (потенциальные вторжения в сетевую инфраструктуру), выявлять их в реальном масштабе времени и поднимать соответствующую тревогу
4	Управление сетевой безопасностью	Наличие мер по управлению защитой сетевых ресурсов, обеспечивающих предохранение от несанкционированного доступа ко всем портам дистанционной диагностики (виртуальным или физическим). Наличие шлюзов безопасности для связи между сетями.
		Для каждого межсетевого экрана необходимо наличие отдельного документа, определяющего политику (безопасность) доступа к сервисам

5	Межсетевые экраны	, и реализацию его для каждого соединения, обеспечивающих гарантию прохождения через это соединение только разрешенного трафика
6	Защита конфиденциальности целостности данных, передаваемых по сетям	В обстоятельствах, когда важно сохранить конфиденциальность и целостность данных, следует предусматривать криптографические меры защиты, чтобы шифровать информацию, проходящую через сетевые соединения
7	Неотказуемость от совершенных действий по обмену информацией	В случае, когда требуется представить свидетельство передачи информации по сети, используются следующие защитные меры: 1) протоколы связи, которые дают подтверждение факта отправки документа; 2) протоколы приложения, которые требуют представления исходного адреса или идентификатора и проверки на присутствие данной информации; 3) межсетевые экраны, где проверяются форматы адресов отправителя и получателя на достоверность синтаксиса и согласованность с информацией в соответствующих директориях; 4) протоколы, которые подтверждают факты доставки информации в рамках межсетевых взаимодействий; 5) протоколы, которые включают механизмы, разрешающие устанавливать последовательность информации
8	Обеспечение непрерывной работы и восстановления	Наличие защитных мер, обеспечивающих продолжение функции бизнеса в случае стихийного бедствия путем обеспечения способности к восстановлению каждой деловой операции в подходящий интервал времени после прерывания
9	Доверенный канал	1) предоставление для связи с удаленным доверенным ИТ-продуктом канала, который логически отличим от других и обеспечивает надежную аутентификацию его сторон, а также защиту данных от модификации и раскрытия; 2) обеспечение у обеих сторон возможности инициировать связь через доверенный канал.
10	Доверенный маршрут	1) предоставление для связи с удаленным пользователем маршрута, который логически отличим от других и обеспечивает надежную аутентификацию его сторон, а также защиту данных от модификации и раскрытия; 2) обеспечение у пользователя возможности инициировать связь через доверенный маршрут; 3) для начальной аутентификации удаленного пользователя и удаленного управления использование доверенного маршрута является обязательным.

Приложение 2
к приказу Министра
оборонной и аэрокосмической
промышленности
Республики Казахстан
от 14 марта 2018 года № 40/НҚ

Правила
проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и

информационной системы на соответствие требованиям информационной безопасности

Глава 1. Общие положения

1. Настоящие Правила проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности (далее - Правила) разработаны в соответствии с подпунктом 5) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" (далее – Закон) и определяют порядок проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы (далее – объекты испытаний) на соответствие требованиям информационной безопасности.

2. Испытания на соответствие требованиям информационной безопасности проводятся в обязательном порядке или по инициативе собственника или владельца.

3. В настоящих Правилах используются следующие основные понятия и сокращения:

1) информационная безопасность в сфере информатизации (далее – ИБ) – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

2) информационная система – организационно упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующих определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач;

3) исходные коды - исходные коды компонентов и модулей объекта испытаний с библиотеками и файлами, необходимыми для успешной компиляции объекта испытаний на компакт-диске.

4) интернет-ресурс – электронный информационный ресурс, отображаемый в текстовом, графическом, аудиовизуальном или ином виде, размещаемый на аппаратно-программном комплексе, имеющий уникальный сетевой адрес и (или) доменное имя и функционирующий в Интернете;

5) государственная техническая служба (далее – ГТС) - республиканское государственное предприятие на праве хозяйственного ведения, созданное по решению Правительства Республики Казахстан;

6) заявитель – собственник (владелец) сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса, информационной системы, а также физическое или юридическое лицо, уполномоченное собственником (владельцем) сервисного программного продукта, информационно-коммуникационной платформы " электронного правительства", интернет-ресурса, информационной системы, подавший(ее) заявку на проведение испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса, информационной системы на соответствие требованиям информационной безопасности;

7) сервисный программный продукт – программный продукт, предназначенный для реализации информационно-коммуникационной услуги;

8) информационно-коммуникационная платформа "электронного правительства" – технологическая платформа, предназначенная для реализации сервисной модели информатизации;

4. К объектам испытаний, подлежащим обязательным испытаниям на соответствие требованиям информационной безопасности, относятся:

1) сервисный программный продукт;

2) информационно-коммуникационная платформа "электронного правительства";

3) интернет-ресурс государственного органа;

4) информационная система государственного органа;

5) информационная система, отнесенная к критически важным объектам информационно-коммуникационной инфраструктуры;

6) негосударственная информационная система, интегрируемая с информационной системой государственного органа или предназначенная для формирования государственных электронных информационных ресурсов.

5. Информационной системе государственного органа и негосударственной информационной системе для использования сервисов Национального удостоверяющего центра Республики Казахстан по проверке подлинности электронной цифровой подписи прохождение испытаний на соответствие требованиям информационной безопасности не требуется.

6. Испытания объектов на соответствие требованиям ИБ (далее – испытания) включают в себя работы по оценке соответствия объектов испытаний

требованиям технической документации, нормативных правовых актов Республики Казахстан и действующих на территории Республики Казахстан стандартов в сфере информатизации.

7. В состав испытаний объекта испытаний, за исключением сервисного программного продукта и информационно-коммуникационной платформы " электронного правительства" входят следующие виды работ:

1) анализ исходных кодов;

2) испытание функций информационной безопасности;

3) нагрузочное испытание;

4) обследование сетевой инфраструктуры.

8. В случае отсутствия исходного кода объекта испытания, решение о необязательности проведения анализа исходного кода объекта испытаний устанавливается решением уполномоченного органа в сфере обеспечения информационной безопасности (далее - уполномоченный орган) по запросу заявителя.

9. В испытания сервисного программного продукта входит:

1) анализ исходных кодов;

2) испытание функций информационной безопасности.

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

1) испытание функций информационной безопасности;

2) нагрузочное испытание;

3) обследование сетевой инфраструктуры.

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

12. Испытания проводятся:

1) по одному виду работ;

2) по нескольким видам работ;

3) в полном составе видов работ.

13. Цены на проведение каждого вида работ, входящих в испытания, устанавливаются согласно пункту 2 статьи 14 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации".

14. Расчет стоимости проведения испытаний осуществляется на основании данных анкеты-вопросника о характеристиках объекта испытаний, исходных кодов компонентов и модулей объекта испытаний с библиотеками на компакт-диске и цен, установленных в соответствии с порядком по пункту 12 настоящих Правил.

Глава 2. Порядок проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности

15. Для проведения испытаний заявителем в ГТС в письменном виде подается заявка на проведение испытаний (далее – заявка) согласно Приложению 1 настоящих Правил, с предоставлением следующих документов:

1) копии документа, удостоверяющего личность (для физических лиц);

2) заверенные подписью и печатью (при наличии) заявителя копии учредительных документов (при наличии) и справки или свидетельства о государственной регистрации юридического лица (для юридических лиц);

3) анкета-вопросник о характеристиках объекта испытаний согласно Приложению 2 настоящих Правил;

4) перечень технической документации, необходимой для проведения испытаний, согласно Приложению 3 настоящих Правил;

5) исходные коды компонентов и модулей объекта испытаний с библиотеками и файлами, необходимыми для успешной компиляции, а также схемы баз данных (на языке описания данных) объекта испытаний, на компакт-диске;

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

16. В случае, если заявитель осуществляет закупки посредством веб-портала государственных закупок, заявка на проведение испытаний принимается не позднее 1 ноября текущего года.

17. ГТС в течение пяти рабочих дней со дня получения заявки осуществляет проверку полноты документов указанных в пункте 15 настоящих Правил.

18. В случае несоответствия заявки и приложенных документов в соответствии с требованиями, указанными в пункте 15 настоящих Правил, заявка возвращается заявителю с указанием причин возврата.

19. При наличии полного пакета документов указанных в пункте 15 настоящих Правил, ГТС в течение пяти рабочих дней направляет заявителю:

1) проект технической спецификации к договору на проведение испытаний, если заявитель осуществляет закупки посредством веб-портала государственных закупок. Заявитель в течение 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, если заявитель осуществляет закупки без применения веб-портала государственных закупок. Заявитель в течение пяти рабочих дней со дня получения двух экземпляров вышеуказанного договора подписывает их и возвращает один экземпляр договора в ГТС;

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

В случае невозможности согласования сроков проведения испытания, заявка возвращается заявителю без удовлетворения с указанием возможности обратиться в уполномоченный орган для определения сроков испытаний.

21. Для проведения испытаний заявитель обеспечивает для ГТС:

1) физический доступ к рабочему месту пользователя, серверному и сетевому оборудованию, сети телекоммуникаций объекта испытаний и созданной на время испытаний среде, аналогичной промышленной;

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

22. В случае невозможности обеспечения Заявителем требований пункта 21 настоящих Правил, испытания приостанавливаются на время, необходимое Заявителю для их обеспечения с учетом подписания дополнительного соглашения к договору на продление его срока исполнения.

23. Испытания проводятся согласно Методике проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности.

24. В случае, если при проведении испытаний выявилось расхождение между данными анкеты-вопросника о характеристиках объекта испытаний, поданной в соответствии с подпунктом 3) пункта 15 настоящих Правил и фактическим состоянием объекта испытаний, заявитель направляет в ГТС обновленную анкету-вопросник о характеристиках объекта испытаний. Обновленная анкета-вопросник о характеристиках объекта испытаний (при необходимости) будет основанием для заключения дополнительного соглашения на продление срока испытаний и изменение стоимости проведения испытаний.

25. При необходимости, если при проведении испытаний выявится необходимость проведения повторного испытания по одному или по нескольким видам испытаний до окончания срока испытания, заявитель обращается с

запросом в ГТС и заключается дополнительное соглашение о проведении повторного испытания по этим видам работ.

26. Результаты каждого вида работ, входящих в испытания, и рекомендации по устранению выявленных несоответствий вносятся в отдельный протокол, оформляемый в двух экземплярах, один из которых выдается заявителю.

27. На основании комплекта протоколов ГТС оформляет Акт испытаний (далее - Акт испытаний) согласно Приложению 4 настоящих Правил в двух экземплярах (по одному для ГТС и заявителя).

28. Испытания признаются положительными при наличии Акта испытаний с положительным заключением, выдаваемого после проведения всех видов работ, входящих в испытания, и наличия по ним протоколов с положительными результатами.

29. В случае, если заявитель устранил выявленные при испытаниях несоответствия в течение месяца со дня получения Акта испытаний либо протоколов по проведенным работам и направил в ГТС запрос на проведение повторных испытаний с приложением сравнительной таблицы с результатами исправления выявленных несоответствий и акта приема-передачи исходных кодов объекта испытаний согласно Приложению 5 настоящих Правил, ГТС на безвозмездной основе в течение десяти рабочих дней со дня получения от заявителя уведомления проводит повторные испытания по данным видам работ с оформлением соответствующих документов.

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

30. При проведении повторных испытаний после исправления несоответствий , связанных с внесением изменений в программное обеспечение объекта испытаний, анализ исходного кода проводится в обязательном порядке, даже если ранее он был выполнен без несоответствий. 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 на компакт-диске.

31. В случае выявления несоответствий при проведении повторных испытаний ГТС оформляет Акт испытаний или протокол с отрицательным заключением, после чего испытания проводятся в порядке, установленном в главе 2 настоящих Правил.

32. В случае изменения условий функционирования и функциональности объекта информатизации, собственник или владелец объекта информатизации после завершения работ, приведших к изменениям, направляет в ГТС заявку о необходимости проведения испытания в порядке, установленном главой 2 настоящих Правил, с приложением описания всех произведенных изменений.

33. При утере, порче или повреждении протоколов и (или) Акта испытаний владелец объекта испытаний направляет в ГТС уведомление с указанием причин.

34. ГТС в течение пяти рабочих дней со дня получения уведомления выдает дубликат протоколов и (или) Акта испытаний.

35. Срок действия Акта испытаний с положительным результатом ограничивается сроком промышленной эксплуатации объекта испытаний или до момента начала модернизации объекта испытаний.

36. Срок действия протокола по отдельному виду испытания, не включенный в Акт испытаний по пункту 27 настоящих Правил не превышает 1 год.

Приложение 1
к Правилам проведения испытаний
сервисного программного продукта,
информационно-коммуникационной
платформы "электронного
правительства", интернет-ресурса
государственного органа и
информационной системы на
соответствие требованиям
информационной безопасности
Форма

Заявка на проведение испытаний

_____
_ _ _ _ _ _
(наименование объекта испытаний)
на соответствие требованиям информационной безопасности (далее – испытания)
1._____
_ _ _ _ _
(наименование организации-заявителя, Ф.И.О. заявителя)
_____
_ _ _ _ _ _
(почтовый адрес, e-mail 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) _____

_ _ _ _

(перечень видов работ согласно пункта 7 / 8 / 9 / 10 настоящих Правил указать нужный пункт))

2. Сведения о владельце (собственнике) испытываемого объекта испытаний

_____

_ _ _ _

(наименование или Ф.И.О.)

_____

_ _ _ _

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

3. Сведения о разработчике испытываемого объекта испытаний

_____

_ _ _ _

(информация о разработчике, наименование или Ф.И.О. авторов)

_____

_ _ _ _

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

4. Краткая аннотация на объект испытаний или его назначение

_____

_ _ _ _

(назначение, применение, новизна, аналоги и т.п., используемые средства разработки)

4. Дополнительные сведения:

_____

_ _ _ _

Руководитель организации – заявителя/ Ф.И.О., заявителя _____ (подпись, дата) (место печати) при наличии

Приложение 2
к Правилам проведения испытаний
сервисного программного продукта,
информационно-коммуникационной
платформы "электронного
правительства", интернет-ресурса
государственного органа и
информационной системы на
соответствие требованиям
информационной безопасности

Форма

Анкета-вопросник
о характеристиках объекта испытаний

1. Наименование объекта испытаний:

_____

_ _ _
_____
_ _ _
2. Реквизиты разработчика объекта испытаний:
1) наименование разработчика: _____
_____
_ _ ;
2) адрес: г._____, ул. _____;
3) телефон: _____, факс: _____;
4) адрес электронной почты: E-mail: _____@_____.
3. Данные лица, ответственного за заполнение настоящей анкеты и связь с государственной технической службой:
1) фамилия, имя, отчество: _____;
2) должность: _____;
3) телефон рабочий: _____, телефон сотовый: _____;
4) адрес электронной почты: E-mail: _____@_____.
4. Классификация объекта испытаний
1) класс электронных информационных ресурсов _____;
2) класс программного обеспечения _____/_____.
(прикладное / общесистемное)
Примечание. Приложить утвержденную схему классификации по схеме классификации объектов информатизации из Приложения 2 к Правилам классификации объектов информатизации, утвержденный Приказом исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 135 (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 13349, опубликован 17 марта 2016 года в информационно-правовой системе "Әділет").
5. Архитектура объекта испытаний:
1) приложить утвержденную функциональную схему объекта испытаний, с указанием:
расположения компонентов и модулей объекта испытаний;
связей между компонентами или модулями;
интеграционного взаимодействия с другими объектами информатизации;
направления основных информационных потоков;
мест и способов подключения пользователей;
мест и технологий хранения данных;
используемых локальных, ведомственных (корпоративных) и глобальных сетей;
применяемого резервного оборудования;

2) приложить утвержденную схему сети передачи данных/сети телекоммуникаций объекта испытаний с указанием:
архитектуры и характеристик сети;
серверного оборудования;
сетевого и коммуникационного оборудования;
адресации и применяемых сетевых технологий;
решения(й) по обеспечению отказоустойчивости и резервированию.

6. Информация об объекте испытаний:

1) информация о серверном оборудовании (заполнить таблицу):

№ п/п	Наименование сервера или виртуального ресурса (доменное имя, сетевое имя или логическое имя сервера)	Назначение (выполняемые функциональные задачи)	Кол-во	Характеристики сервера или используемых заявленных виртуальных ресурсов	ПО, ОС, приложения и библиотеки установленные на серверах или используемые виртуальные сервисы (состав программной среды)	IP-адрес
1	2	3	4	5	6	7

2) местонахождение серверного оборудования (заполнить таблицу):

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

3) характеристики резервного оборудования (заполнить таблицу):

№ п/п	Наименование сервера или виртуального ресурса (доменное имя, сетевое имя или логическое имя сервера)	Назначение (выполняемые функциональные задачи)	Кол-во	Характеристики сервера или используемых заявленных виртуальных ресурсов	ПО, ОС, приложения и библиотеки установленные на серверах или используемые виртуальные сервисы (состав программной среды)	IP-адрес	Метод резервирования
1	2	3	4	5	6	7	8

4) местонахождение резервного серверного оборудования (заполнить таблицу):

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

5) информация по рабочим станциям администраторов (заполнить таблицу):

№ п/п	Роль администратора	Количество учетных записей администраторов	Наличие доступа к Интернет	Наличие удаленного доступа к серверу	IP-адрес рабочей станции администратора	Характеристики рабочей станции администратора
1	2	3	4	5	6	7

6) информация о пользователях (заполнить таблицу):

№ п/п	Роль пользователя	Перечень типовых действий пользователя	Способ и адрес подключения пользователей	Максимальное количество пользователей	Максимальное количество, обрабатываемых запросов (пакетов) в секунду	Максимальное время ожидания между запросами
1	2	3	4	5	6	7

7) Информация об интеграционном взаимодействии объекта испытаний, в том числе, планируемые (заполнить таблицу):

№ п/п	Наименование интеграционной связи (объекта информатизации)	Владелец (собственник) интегрируемого объекта	Действующая / планируемая	Наличие модуля интеграции	Используемые протоколы интеграции	Максимальное количество запросов (пакетов) в секунду	Максимальное время ожидания между запросами
1	2	3	4	5	6	7	8

8) информация о средствах, используемых для мониторинга работоспособности серверного, сетевого оборудования, системных служб и процессов, свободного дискового пространства (заполнить таблицу):

№ п/п	Наименование средств мониторинга	Назначение мониторинга	Ответственный сотрудник за мониторинг	Периодичность проведении анализа
1	2	3	4	5

9) информация об анализе журналов событий (заполнить таблицу):

№ п/п	Наименование сервисов, журнала событий	Средства для анализа	Периодичность проведения анализа	Срок хранения журналов событий	Места хранения журналов событий
1	2	3	4	5	6

10) языковая среда разработки испытываемого образца (заполнить таблицу):

№ п/п	Наименование модуля	Применяемый язык программирования	Используемые библиотеки, компоненты и файлы	Объем исходного кода, Мбайт
1	2	3	4	5

11) структура корпоративной сети (заполнить таблицу):

№ п/п	Наименование сегмента сети	Количество межсетевых соединений	Аппаратно-программные средства защиты сети	Другие средства защиты сетей
1	2	3	4	5

7. Документирование испытываемого объекта (заполнить таблицу):

№ п/п	Наименование документа	Наличие	Количество страниц	Дата утверждения	Стандарт, в соответствии с которым был разработан документ
1	2	3	4	5	6
1.	Техническое задание или задание на проектирование сервисного программного продукта				
2.	Руководство пользователя				
3.	Текст программы				
4.	Описание программы				

8. Наличие другой документации, предусмотренной стандартами (заполнить таблицу):

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

9. Сведения о ранее пройденных видах работ или испытаниях (номер протокола, дата):

_____
_ _ _ _ _ _

10. Наличие лицензии на испытываемый объект (наличие авторских прав, наличие соглашения с организацией-разработчиком на предоставление исходного кода) _____
_ _ _ _ _ _
_____
_ _ _ _ _ _

11. Дополнительная информация: _____
_ _ _
_____
_ _ _ _ _ _
_____
_ _ _ _ _ _

Примечание: расшифровка аббревиатур:
ПО – программное обеспечение
ОС – операционное обеспечение

Приложение 3
к Правилам проведения испытаний
сервисного программного продукта,
информационно-коммуникационной
платформы "электронного
правительства", интернет-ресурса
государственного органа и
информационной системы
на соответствие требованиям
информационной безопасности

П е р е ч е н ь

технической документации, необходимой для проведения испытаний

1. Техническое задание или задание на проектирование сервисного программного продукта (для сервисного программного продукта).

2. Руководство пользователя.

3. Текст программы (за исключением ИКП ЭП и объектов испытаний, в которых отсутствует исходный код).

4. Описание программы (за исключением ИКП ЭП и объектов испытаний, в которых отсутствует исходный код).

Приложение 4
к Правилам проведения испытаний
сервисного программного продукта,
информационно-коммуникационной
платформы "электронного
правительства", интернет-ресурса
государственного органа и
информационной системы

на соответствие требованиям
информационной безопасности
"Утверждаю"
Директор Государственной
технической службы

_____ _____
(Ф.И.О.) (подпись)
"_____" _____ 20__ г.

Форма

Акт испытаний №___

"_____" _____ 20__ г.

_____
_ _ _ _
(наименование объекта испытаний (далее – ОИ))

_____
_ _ _ _
(наименование организации-заявителя / Ф.И.О. заявителя)

1. В соответствии с Заявкой на проведение испытаний на соответствие требованиям информационной безопасности (далее – испытания) от "___" _____20__г. и Договором №___ от "___" _____20__г. Государственная техническая служба провела испытание

_____
_ _ _
(наименование ОИ)

в составе следующих работ:

1) анализ исходных кодов;

2) испытание функций информационной безопасности;

3) нагрузочное испытание;

4) обследование сетевой инфраструктуры.

2. В ходе испытаний установлено:

1) по анализу исходного кода:

анализ исходных кодов ОИ завершен без ошибок (при отсутствии недостатков ПО);

анализ исходных кодов ОИ завершен с ошибками (при наличии недостатков ПО);

анализ исходных кодов ОИ не проводился на основании (указать основание по пункту 8, 9 или 10 настоящих Правил);

Протокол (номер и дата протокола анализ исходных кодов ОИ);

2) по испытаниям функций информационной безопасности:

реализация функций информационной безопасности ОИ соответствуют требованиям ИБ (при отсутствии несоответствий);

реализация функций информационной безопасности ОИ не соответствуют требованиям ИБ (при наличии несоответствий);

Протокол (номер и дата протокола испытания функций информационной безопасности ОИ);

3) по нагрузочному испытанию:

нагрузочное испытание прошло успешно (при стабильном и устойчивом функционировании (без сбоев) ОИ при заданных параметрах);

нагрузочное испытание прошло не успешно (при нарушениях стабильности и устойчивости (наличие сбоев) функционирования ОИ при заданных параметрах);

Протокол (номер и дата протокола нагрузочного испытания);

4) по обследованию сетевой инфраструктуры:

безопасность сетевой инфраструктуры соответствует требованиям ИБ (при отсутствии несоответствий и уязвимостей, влияющих на безопасное функционирование ОИ);

безопасность сетевой инфраструктуры не соответствует требованиям ИБ (при наличии несоответствий, влияющих на безопасное функционирование ОИ);

Протокол (номер и дата протокола обследования сетевой инфраструктуры ОИ).

Заключение

На основании проведенных испытаний _____

(наименование объекта испытаний)

соответствует / не соответствует требованиям информационной безопасности.

СОГЛАСОВАНО:	ПОДГОТОВЛЕНО:
_____	_____
(должность)	(должность)
_____	_____
(подпись) (Ф.И.О.) при наличии	(подпись) (Ф.И.О.) при наличии
"____" _____20____ г.	"____" _____20____ г.

Приложение 5
к Правилам проведения испытаний
сервисного программного продукта,
информационно-коммуникационной
платформы "электронного
правительства", интернет-ресурса
государственного органа и
информационной системы на
соответствие требованиям
информационной безопасности
Форма

Акт приема-передачи
исходных кодов объекта испытаний

_____

_ _ _ _

(наименование объекта испытаний (далее – ОИ))

_____

_ _ _ _

(наименование организации-заявителя / Ф.И.О. заявителя)

"_____" _____ 20__ г.

Версия передаваемого ПО _____.

Количество дисков _____.

№ п/п	Маркировка диска	Наименование каталога на диске	Наименование файла	Размер файла, Мбайт	Применяемый язык программирования (при необходимости)	Дата модификации файла
1	2	3	4	5	6	7

Передал:

_____

(должность)

_____

(подпись) (Ф.И.О.) при наличии

"____" _____20____ г.

Принял:

_____

(должность)

_____

(подпись) (Ф.И.О.) при наличии

"____" _____20____ г.

Зарегистрирован в Журнале регистрации образцов №_ "___" _____ 20__ г.

Зарегистрировал _____

(подпись) (Ф.И.О.) при наличии