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 и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 63. Зарегистрирован в Министерстве юстиции Республики Казахстан 24 февраля 2016 года № 13207. Утратил силу приказом Министра оборонной и аэрокосмической промышленности Республики Казахстан от 14 марта 2018 года № 40/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования)

Сноска. Утратил силу приказом Министра оборонной и аэрокосмической промышленности РК от 14.03.2018 № 40/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

В соответствии с подпунктом 16) статьи 7 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 Председателя Агентства Республики Казахстан по информатизации и связи от 1 декабря 2009 года № 480 "Об утверждении Правил испытаний, регистрации, передачи, хранения, обеспечения полноты депонирования и представления сведений о регистрации, передаче и хранении программных продуктов, программных кодов и нормативно-технической документации в депозитарий" (зарегистрированный в Реестре государственной регистрации нормативных правовых актов за № 5981,

опубликованный 20 апреля 2010 года в Собрании актов центральных исполнительных и иных центральных государственных органов Республики Казахстан).

3. Комитету связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан (Қазаңғап Т.Б.) обеспечить:

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

2) направление копии настоящего приказа в печатном и электронном виде на официальное опубликование в периодические печатные издания и информационно-правовую систему "Әділет" в течение десяти календарных дней после его государственной регистрации в Министерстве юстиции Республики Казахстан, а также в Республиканский центр правовой информации в течение десяти календарных дней со дня получения зарегистрированного приказа для включения в эталонный контрольный банк нормативных правовых актов Республики Казахстан;

3) размещение настоящего приказа на интернет-ресурсе Министерства по инвестициям и развитию Республики Казахстан и на интранет-портале государственных органов;

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

4. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра по инвестициям и развитию Республики Казахстан.

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

Исполняющий обязанности
Министра по инвестициям и развитию
Республики Казахстан Ж. Касымбек

Приложение 1
к приказу исполняющего обязанности
Министра по инвестициям и развитию
Республики Казахстан
от 26 января 2016 года № 63

Методика
проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного

правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности

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 16) статьи 7 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации.

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

1) испытание функций информационной безопасности – оценка функций сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы (далее – объекты испытаний) на соответствие требованиям информационной безопасности;

2) нагрузочное испытание – оценка соблюдения доступности, целостности и конфиденциальности объектов испытаний при плановых, повышенных и пиковых нагрузках;

3) государственная техническая служба – республиканское государственное предприятие на праве хозяйственного ведения, созданное по решению Правительства Республики Казахстан;

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

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

6) 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;

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

8) испытание сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности (далее – испытание) – технические мероприятия по оценке объектов испытаний требованиям информационной безопасности;

9) объекты испытаний (далее – ОИ) – сервисный программный продукт, информационно-коммуникационная платформа "электронного правительства", интернет-ресурс государственного органа, информационная система.

3. Проведение испытания включает:

1) анализ исходных кодов;

2) испытание функций информационной безопасности;

3) нагрузочное испытание;

4) обследование сети телекоммуникаций и серверного оборудования.

2. Анализ исходных кодов

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

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

6. Анализ исходных кодов включает:

1) выявление недостатков ПО;

2) фиксацию результатов анализа исходного кода.

7. Выявление недостатков ПО осуществляется в следующем порядке:

1) проводится подготовка исходных данных (загрузка исходных кодов 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).

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

9. Результаты анализа исходных кодов фиксируются в Протоколе анализа исходных кодов.

10. По окончанию проведенного анализа исходных кодов ОИ при условии его положительного результата, исходные коды ОИ маркируются и сдаются в опечатанном виде на ответственное хранение в архив государственной технической службы.

3. Испытание функций информационной безопасности

11. Испытание функций информационной безопасности осуществляется с целью оценки их соответствия требованиям стандартов согласованных с заявителем.

12. Испытание функций информационной безопасности включает:

1) оценку соответствия функций безопасности требованиям стандартов согласованных с заявителем;

2) фиксацию результатов оценки.

13. Содержание функций информационной безопасности приведено в перечне функций информационной безопасности, согласно приложению 1 к настоящей Методике.

14. Результаты испытаний функций информационной безопасности фиксируются в Протоколе испытаний функций информационной безопасности.

4. Нагрузочное испытание

15. Нагрузочное испытание проводится с целью оценки соблюдения доступности, целостности и конфиденциальности ОИ под нагрузкой, соответствующей работе реальных пользователей.

16. Нагрузочное испытание проводится с использованием специализированного программного средства (далее – ПС) на основании автоматических сценариев, включающих работу пользователей ОИ в одной из следующих сред, предоставленных заказчиком:

тестовой среды, аналогичной среде штатной эксплуатации ОИ;

среды штатной эксплуатации ОИ, в которой отсутствуют персональные данные;

среды штатной эксплуатации ОИ, в которой персональные данные заменены на фиктивные.

17. Параметры нагрузочного испытания предоставляются заявителем в Анкете-вопроснике о характеристиках ОИ и включают:

1) перечень ролей пользователя;

2) перечень типовых действий пользователя;

3) максимальное количество пользователей;

4) максимальное количество, обрабатываемых запросов в секунду и время ожидания между запросами.

18. Нагрузочное испытание осуществляется в следующем порядке:

1) проводится подготовка к испытанию;

2) проводятся испытание;

3) фиксируются результаты испытания.

19. Подготовка к испытанию включает:

1) разработку экспертным методом сценария испытания с описанием операций виртуальных пользователей, а также событий и особенностей их поведения;

2) определение временных характеристик каждой операции и количества виртуальных пользователей, участвующих в испытаниях;

3) формирование скриптов виртуальных пользователей и определение задач, которые будут выполняться:

каждым виртуальным пользователем;

одновременно несколькими виртуальными пользователями;

4) согласование времени проведения испытания с заказчиком.

20. Проведение испытания включает:

1) распределение совокупной нагрузки на ОИ, в процессе которой нескольким виртуальным пользователям выдаются инструкции по одновременному выполнению определенных задач;

2) настройку конфигурации и вписывание сценария испытания в специализированное ПС;

3) запуск специализированного программного средства;

4) формирование и выдачу программного отчета, включающего записи всех транзакций (обработанные запросы к ОИ), определенных в каждом скрипте виртуального пользователя.

21. Работы по проведению нагрузочного тестирования проводятся для одного ОИ по количеству вариантов использования ОИ.

22. Результаты нагрузочного испытания фиксируются в Протоколе нагрузочного испытания.

5. Обследование сети телекоммуникаций и серверного оборудования

23. Обследование сети телекоммуникаций и серверного оборудования проводится с целью оценки безопасности сети телекоммуникаций и серверного оборудования, а также выявления уязвимостей ПО, используемого его компонентами (сервер, рабочие станции, сетевое оборудование).

24. Обследование сети телекоммуникаций и серверного оборудования включает:

1) оценку соответствия функций защиты сети телекоммуникаций и серверного оборудования требованиям стандартов согласованных с заявителем;

2) выявление уязвимостей ПО;

3) фиксацию полученных результатов.

25. Содержание функций защиты сети телекоммуникаций и серверного оборудования приведено в перечне функций защиты сети телекоммуникаций и серверного оборудования, согласно приложению 2 к настоящей Методике.

26. Выявление уязвимостей ПО проводится с использованием программно-аппаратного комплекса (далее – ПАК), на основании учетных записей для доступа к компонентам ОИ, предоставленных заявителем.

27. Выявление уязвимостей ПО включает:

1) настройку ПАК (прописка учетной записи для проведения локальных и удаленных проверок, выбор режима инструментального обследования);

2) запуск ПАК;

3) формирование и выдачу программного отчета, включающего в себя перечень выявленных уязвимостей с указанием их описания, количества и уровня.

28. Работы по обследованию сети телекоммуникаций и серверного оборудования, а также инструментальное обследование компонентов ОИ проводятся для каждой подсети (сегмента сети) в отдельности.

29. Результаты обследования сети телекоммуникаций и серверного оборудования фиксируются в Протоколе обследования сети телекоммуникаций и серверного оборудования.

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 (проверка проводится в разрезе серверов и виртуальных ресурсов)		
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. То есть в каждой регистрационной записи должны присутствовать дата и время события, тип события, идентификатор субъекта и результат (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	Регистрационная информация должна быть надежно защищена от несанкционированной модификации
Организация связи (проверка проводится в разрезе серверов и виртуальных ресурсов)		
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 (проверка проводится в разрезе средств криптографической защиты информации в ОИ)		
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 стандартов
Защита данных пользователя (проверка проводится в разрезе серверов (виртуальных ресурсов))		
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 должно основываться, 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 может быть впоследствии использован 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	Должна обеспечиваться целостность данных пользователя при их передаче между ФБО и другим доверенным продуктом ИТ, а также возможность их восстановления при обнаруживаемых ошибках
Идентификация и аутентификация (проверка проводится в разрезе серверов и виртуальных ресурсов, выполняющих идентификацию и аутентификацию)		

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, должны поддерживаться также открытые и секретные ключи
27	Аутентификация пользователя	Наличие механизмов аутентификации пользователя, предоставляемых ФБО
28	Идентификация пользователя	1) Каждый пользователь должен быть успешно идентифицирован и аутентифицирован до разрешения любого действия, выполняемого сервисом безопасности от имени этого пользователя; 2) Должны иметься возможностей по предотвращению применения аутентификационных данных, которые были подделаны или скопированы у другого пользователя; 3) Следует аутентифицировать любой представленный идентификатор пользователя; 4) Необходимо повторно аутентифицировать пользователя по истечении определенного администратором интервала времени; 5) Функции безопасности должны предоставлять пользователю только скрытую обратную связь во время выполнения аутентификации
29	Связывание пользователь-субъект	Следует ассоциировать соответствующие атрибуты безопасности пользователя с субъектами, действующими от имени этого пользователя
Управление безопасностью (проверка проводится в разрезе серверов и виртуальных ресурсов)		
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 должна быть возможность отмены атрибутов безопасности, ассоциированных с пользователями. Важные для безопасности полномочия должны отменяться 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
Обеспечение приватности (проверка проводится в разрезе серверов и виртуальных ресурсов)		
36	Анонимность	Обеспечение возможности того, чтобы пользователь мог использовать ресурс или услугу ОИ без раскрытия своего идентификатора
37	Псевдонимность	Обеспечение возможности того, чтобы пользователь мог использовать ресурс или услугу без раскрытия своего идентификатора, оставаясь в то же время ответственным за это использование
38	Невозможность ассоциации	Обеспечение возможности того, чтобы пользователь мог неоднократно использовать ресурсы или услуги, не давая никому возможности связать вместе их использование
39	Скрытность	1) Обеспечение возможности того, чтобы пользователь мог использовать ресурс или услугу без предоставления кому-либо, в особенности третьей стороне, информации об использовании ресурса или услуги. 2) Администратор должен иметь возможность наблюдать за использованием ресурсов сервиса безопасности
Защита ФБО (проверка проводится в разрезе серверов и виртуальных ресурсов)		
40	Безопасность при сбое	Сервис должен сохранять безопасное состояние при аппаратных сбоях (вызванных, например, перебоями электропитания)
41	Доступность экспортируемых данных ФБО	Сервис должен предоставлять возможность 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
42	Конфиденциальность экспортируемых данных ФБО	Сервис должен предоставлять возможность 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
43	Целостность экспортируемых данных ФБО	Сервис должен предоставлять возможность 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
44	Передача данных ФБО в пределах ОИ	Сервис должен предоставлять возможность верифицировать доступность, 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
45	Физическая защита ФБО	Должна осуществляться физическая защита ФБО
46	Надежное восстановление	Когда автоматическое восстановление после сбоя или прерывания обслуживания невозможно, сервис должен перейти в режим аварийной поддержки, позволяющей вернуться к безопасному состоянию. После аппаратных сбоев должен обеспечиваться возврат к безопасному состоянию с использованием автоматических процедур

47	Обнаружение повторного использования	Сервис должен обнаруживать повторное использование аутентификационных данных, отказать в доступе, сгенерировать запись регистрационного журнала и сигнализировать администратору о вероятном нарушении безопасности
48	Посредничество при обращениях	Функции, осуществляющие политику безопасности сервиса, должны вызываться и успешно выполняться прежде, чем разрешается выполнение любой другой функции сервиса
49	Разделение домена	Функции безопасности должны поддерживать отдельный домен для собственного выполнения, который защищает их от вмешательства и искажения недоверенными субъектами
50	Протокол синхронизации состояний	Должна обеспечиваться синхронизации состояний
51	Метки времени	Для использования функциями безопасности должны предоставляться надежные метки времени
52	Согласованность данных между ФБО	Должна обеспечиваться согласованная интерпретация регистрационной информации, а также параметров используемых криптографических операций
53	Согласованность данных ФБО при дублировании в пределах ОИ	Должна обеспечиваться согласованность данных функций безопасности при дублировании их в различных частях ОИ. Когда части, содержащие дублируемые данные, разъединены, согласованность должна обеспечиваться после восстановления соединения перед обработкой любых запросов к заданным функциям безопасности
54	Самотестирование ФБО	Для демонстрации правильности работы функций безопасности при запуске, периодически в процессе нормального функционирования и/или по запросу администратора должен выполняться пакет программ самотестирования. У администратора должна быть возможность верифицировать целостность данных и выполняемого кода функций безопасности
Использование ресурсов (проверка проводится в разрезе серверов и виртуальных ресурсов)		
55	Отказоустойчивость	Должна обеспечиваться доступность функциональных возможностей ОИ даже в случае сбоев. Примеры таких сбоев: отключение питания, отказ аппаратуры, сбой программного обеспечения
56	Приоритет обслуживания	Должно обеспечиваться управление использованием ресурсов пользователями и субъектами в пределах своей области действия так, что высокоприоритетные операции в пределах ОИ всегда будут выполняться без препятствий или задержек со стороны операций с более низким приоритетом
57	Распределение ресурсов	Должно обеспечиваться управление использованием ресурсов пользователями и субъектами таким образом, чтобы не допустить несанкционированные отказы в обслуживании из-за монополизации ресурсов другими пользователями или субъектами
58	Доступ к ОИ (проверка проводится для ОИ в целом)	
59	Ограничение области выбираемых атрибутов	Должны ограничиваться как атрибуты безопасности сеанса, которые может выбирать пользователь, так и атрибуты 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)
60	Ограничение на параллельные сеансы	Должно ограничиваться максимальное число параллельных сеансов, предоставляемых одному пользователю. У этой величины должно быть подразумеваемое значение, устанавливаемое администратором
61	Блокирование сеанса	По истечении установленного администратором значения длительности бездействия пользователя сеанс работы должен принудительно завершаться

62	Предупреждения перед предоставлением доступа к ОИ	Должна обеспечиваться возможность еще до идентификации и аутентификации отобразить для потенциальных пользователей предупреждающее сообщение относительно характера использования ОИ
63	История доступа к ОИ	Должна обеспечиваться возможность 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 ОИ, а также число неуспешных попыток доступа к ОИ после последнего успешного доступа идентифицированного пользователя
64	Открытие сеанса с ОИ	Сервис должен быть способен отказать в открытии сеанса, основываясь на идентификаторе субъекта, пароле субъекта, правах доступа субъекта
Обеспечение доверенного маршрута/канала (проверка проводится в разрезе серверов и виртуальных ресурсов)		
65	Доверенный канал	1) для связи с удаленным доверенным ИТ-продуктом функции безопасности должны предоставлять канал, который логически отличим от других и обеспечивает надежную аутентификацию его сторон, а также защиту данных от модификации и раскрытия). 2) у обеих сторон должна быть возможность инициирования связи через доверенный канал
66	Доверенный маршрут	1) для связи с удаленным пользователем функции безопасности должны предоставлять маршрут, который логически отличим от других и обеспечивает надежную аутентификацию его сторон, а также защиту данных от модификации и раскрытия. 2) у пользователя должна быть возможность инициирования связи через доверенный маршрут. 3) для начальной аутентификации удаленного пользователя и удаленного управления использование доверенного маршрута является обязательным

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 сети телекоммуникаций и серверного оборудования

№ п/п	Наименование функций	Содержание функций
1	2	3
1		Обеспечение безопасности сервисов, предоставляемых сетью телекоммуникаций и предохранения соответствующих данных путем

	Идентификация и аутентификация	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 сети телекоммуникаций), выявлять их в реальном масштабе времени и поднимать соответствующую тревогу
4	Предохранение от вредоносного кода	Наличие защитных мер для предохранения от вредоносного кода, включающих в себя: 1) поддержка сканирующего программного обеспечения на современном уровне путем, по меньшей мере, еженедельного обновления версий; 2) наличие руководящих указаний, регламентирующих в общих чертах процедуры и практические действия, направленные на уменьшение возможности поступления вредоносного кода в систему
5	Управление защитой сети	Наличие защитных мер, обеспечивающих предохранение от несанкционированного доступа ко всем портам дистанционной диагностики (виртуальным или физическим)
6	Межсетевые экраны	Для каждого межсетевого экрана необходимо наличие отдельного документа, определяющего политику (безопасность) доступа к сервисам , и реализацию его для каждого соединения, обеспечивающих гарантию прохождения через это соединение только разрешенного трафика
7	Конфиденциальность обмена данными по сетям	В обстоятельствах, когда важно сохранить конфиденциальность, следует предусматривать криптографические меры защиты, чтобы шифровать информацию, проходящую через сетевые соединения
8	Целостность данных, передаваемых по сетям	В обстоятельствах, когда важно сохранить целостность данных, следует предусматривать цифровую подпись и меры защиты целостности сообщения, чтобы предохранять информацию, проходящую через сетевые соединения
9	Неотказуемость от совершенных действий по обмену информацией	В случае, когда требуется представить свидетельство передачи информации по сети, должны использоваться 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
10	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

Приложение 2
к приказу исполняющего обязанности
Министра по инвестициям и развитию
Республики Казахстан
от 26 января 2016 года № 63

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

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 16) статьи 7 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. 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) 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;

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

5) 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;

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

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

3. Объектами испытаний являются:

1) сервисный программный продукт;

2) информационно-коммуникационная платформа "электронного правительства";

3) интернет-ресурс государственного органа;

4) информационная система.

4. Испытания объектов на соответствие требованиям ИБ (далее – испытания) включают в себя работы по оценке соответствия объектов испытаний требованиям ИБ, установленных стандартами, принятыми на территории Республики Казахстан.

5. В испытания входит:

1) анализ исходных кодов;

2) испытание функций информационной безопасности;

3) нагрузочное испытание;

4) обследование сети телекоммуникаций и серверного оборудования.

6. В случае интеграции информационной системы государственного органа или предназначенной для формирования государственных электронных информационных ресурсов с негосударственной информационной системой дополнительно к анализу ее исходного кода проводится анализ исходных кодов компонентов интеграции (модуль интеграции, подсистема интеграции, интеграционная шина).

7. Испытания проводятся:

1) по одному виду работ;

2) по нескольким видам работ;

3) в полном составе видов работ.

8. Стоимость проведения каждого вида работ, входящих в испытания, устанавливается уполномоченным органом в сфере информатизации (далее - уполномоченный орган) по согласованию с антимонопольным органом.

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

9. Для проведения испытаний заявителем в ГТС подается заявка на проведение испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности (далее – заявка) по форме, согласно приложению 1 к настоящим Правилам с предоставлением следующих документов:

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

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

3) анкета-вопросник о характеристиках ОИ по форме, согласно приложению 2 к настоящим Правилам;

4) техническая документация в соответствии с Перечнем технической документации, согласно приложению 3 к настоящим Правилам;

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

10. ГТС в течение пяти рабочих дней со дня получения заявки осуществляет проверку заявки в соответствии с требованиями, указанными в пункте 9 настоящих Правил.

11. В случае несоответствия заявки и приложенных документов в соответствии с требованиями, указанными в пункте 9 настоящих Правил, заявка возвращается заявителю с указанием причин возврата.

12. При соответствии заявки и приложенных документов в соответствии с требованиями, указанными в пункте 9 настоящих Правил, ГТС в течение пяти рабочих дней направляет заявителю два экземпляра договора на проведение испытаний. Заявитель в течение пяти рабочих дней со дня получения двух экземпляров вышеуказанного договора подписывает их и возвращает один экземпляр договора в ГТС.

13. Срок испытаний согласовывается с заявителем и зависит от объема работ по испытаниям и классификационных характеристик ОИ.

14. Для проведения испытаний заявитель обеспечивает 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.

15. 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, в соответствии с подпунктом 7) пункта 1 статьи 14 Закона.

16. 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.

17. В случае, если заявитель устранил выявленные при испытаниях несоответствия в течение месяца со дня получения Акта испытаний либо протоколов по проведенным работам, 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.

18. 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.

19. На основании комплекта протоколов ГТС оформляет Акт испытаний по форме, согласно приложению 4 к настоящим Правилам в двух экземплярах (по

одному для ГТС и заявителя), включающий сведения о проведенных работах, их результаты, заключение и рекомендации по устранению выявленных несоответствий (при их наличии).

20. 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.

21. При внесении изменений в ОИ проведение испытаний при условии обеспечения его собственником (владельцем) ГТС проводит повторное испытание в общем порядке, установленном настоящими Правилами.

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

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

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 Методике проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности, утвержденной приказом Министра инвестиций и развития Республики Казахстан от_____ № _____)
2. Сведения о разработчике испытываемого объекта испытаний
_____
___
(информация о разработчике, наименование или Ф.И.О. авторов)
_____
___
(область, город, район, почтовый адрес, телефон)
3. Краткая аннотация на объект испытаний _____
_____
___
(назначение, применение, новизна, аналоги и т.п., используемые средства разработки)
4. Дополнительные сведения:
_____
___
Руководитель организации – заявителя/ Ф.И.О., заявителя _____
(подпись, дата)

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: _____, факс: _____;

4) адрес электронной почты: E-mail: _____@_____.

4. Архитектура объекта испытаний (приложить схему архитектуры испытываемого ОИ, с указанием всех связей и настройками резервирования, схему корпоративной сети):

1) информация о серверах (заполнить таблицу):

Наименование сервера или виртуального ресурса	Назначение	Кол-во	Характеристики сервера или используемых заявленных виртуальных ресурсов	ПО, ОС, приложения и библиотеки установленные на серверах или используемые виртуальные сервисы	IP-адрес
1	2	3	4	5	6

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

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

3) информация о пользователях (заполнить таблицу):

Роль пользователя	Перечень типовых действий пользователя	Минимальные требования к техническим характеристикам рабочей станции Пользователя	Максимальное количество пользователей	Максимальное количество, обрабатываемых запросов в секунду/ время ожидания между запросами	ПО, ОС, приложения и библиотеки установленные на рабочей станции
1	2	3	4	5	6

4) характеристики резервного оборудования (заполнить таблицу):

Наименование сервера или виртуального ресурса	Назначение	Кол-во	Характеристики резервного оборудования или используемых заявленных виртуальных ресурсов	ПО, ОС, приложения и библиотеки, установленные на серверах, или используемые виртуальные сервисы	IP-адрес	Метод резервирования
1	2	3	4	5	6	7

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

Наименование средств мониторинга	Назначение мониторинга	Ответственный сотрудник за мониторинг	Информация о проведении анализа по результатам мониторинга
1	2	3	4

6) информация об анализе журнальных событий (заполнить таблицу):

Наименование сервисов	Средства для анализа	Частота анализа
1	2	3

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

Наименование модулей системы	Языки программирования	Используемые библиотеки	Объем исходного кода и используемых библиотек, файлов, Мбайт
1	2	3	

8) структура корпоративной сети (заполнить таблицу):

Наименование подсети (сегмента сети)	Количество межсетевых соединений	Количество аппаратно-программных средств защиты сети	Другие средства защиты сетей	Средства мониторинга

5. Дополнительные сведения:

1) конфигурация и характеристика используемой сети передачи данных/сети телекоммуникаций (приложить схему):

_____;

2) конфигурация и характеристика резервной сети передачи данных/сети телекоммуникаций (приложить схему):

_____.

6. 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				

5.	Функциональная схема или описание ресурсов информационно-коммуникационной платформы " электронного правительства"				

7. Готовность исходных кодов испытываемого объекта (версия, наименование, предоставить на диске) для компиляции с расширением среды разработки:

_____

___

8. Наличие другой документации, предусмотренной стандартами:

№ 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

Перечень
технической документации

1. Техническое задание или задание на проектирование сервисного программного продукта.

2. Руководство пользователя.

3. Текст программы.

4. Описание программы.

5. Функциональная схема или описание ресурсов информационно-коммуникационной платформы "электронного правительства".

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

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

1. В соответствии с Заявкой на проведение испытаний на соответствие требованиям информационной безопасности (далее – испытания) 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 сети телекоммуникаций и серверного оборудования.
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 и необходим повторный анализ исходных кодов ОИ после их устранения (при наличии недостатков ПО);
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);
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);
4) по обследованию сети телекоммуникаций и серверного оборудования:
безопасность сети телекоммуникаций и серверного оборудования соответствует требованиям ИБ (при отсутствии несоответствий и уязвимостей, влияющих на безопасное функционирование ОИ);
безопасность сети телекоммуникаций и серверного оборудования не соответствует требованиям ИБ (при наличии несоответствий и уязвимостей, влияющих на безопасное функционирование ОИ).
Заключение
На основании проведенных испытаний _____
(наименование объекта испытаний)
соответствует / не соответствует требованиям информационной безопасности.
Рекомендуется устранить выявленные несоответствия и провести повторные испытания (в случае, если выдается акт испытаний с

отрицательным заключением).
СОГЛАСОВАНО: ПОДГОТОВЛЕНО:

_____ _____
(должность) (должность)

_____ _____
(подпись) (Ф.И.О.) при наличии (подпись) (Ф.И.О.) при наличии
"_____" _____20____ г. "_____" _____20____ г.