Об утверждении Правил проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства"

Утративший силу

Приказ и.о. Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 66. Зарегистрирован в Министерстве юстиции Республики Казахстан 23 февраля 2016 года № 13178. Утратил силу приказом Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/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 28.03.2018 № 52/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

В соответствии с подпунктом 32) статьи 7 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" **ПРИКАЗЫВАЮ:**

1. Утвердить прилагаемые Правила проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства".

2. Комитету связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан (Казангап 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 течении 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 2 настоящего приказа.

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

4. 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

Утверждены
приказом исполняющего
обязанности Министра по
инвестициям и развитию
Республики Казахстан
от 26 января 2016 года № 66

Правила
проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства"

1. Общие положения

1. Настоящие Правила проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства" (далее – Правила) разработаны в соответствии с подпунктом 32) статьи 7 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" (далее – Закон) и определяют порядок проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства".

2. Мониторинг обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства" (далее – Мониторинг) проводится посредством системы мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" в целях выявления уязвимостей, событий информационной безопасности, угроз и инцидентов информационной безопасности объектов информатизации "электронного правительства" и реагирования на них.

3. В настоящих Правилах используются следующие понятия и сокращения:

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

2) уполномоченный орган в сфере информатизации (далее – уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство и межотраслевую координацию в сфере информатизации и "электронного правительства";

3) событие информационной безопасности – состояние объектов информатизации, свидетельствующее о возможном нарушении существующей политики безопасности либо о прежде неизвестной ситуации, которая может иметь отношение к безопасности объектов информатизации;

4) инцидент информационной безопасности (далее – инцидент) – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов;

5) угроза информационной безопасности (далее – угроза) – действия способные оказать негативное воздействие на конфиденциальность, целостность и доступность объекта информатизации;

6) инструментальное обследование – комплекс мероприятий, направленных на выявление уязвимостей;

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

8) событие — идентифицированное состояние объекта информатизации;

9) агент системы сбора событий (далее – агент) – программное обеспечение, устанавливаемое на активное серверное, сетевое и (или) специализированное оборудование для сбора событий;

10) уязвимость – недостаток в программном обеспечении или средстве защиты информации, использование которого нарушает работоспособность данного программного обеспечения и (или) средства защиты информации либо приводит к несанкционированным действиям в обход установленных разрешений в программном обеспечении и (или) в средстве защиты информации;

11) пользователь – субъект информатизации, использующий объекты информатизации для выполнения конкретной функции и (или) задачи;

12) объекты информатизации "электронного правительства" – государственные электронные информационные ресурсы, программное

обеспечение государственных органов и информационно-коммуникационная инфраструктура "электронного правительства", в том числе негосударственные информационные системы, интегрируемые с информационными системами государственных органов или предназначенные для формирования государственных электронных информационных ресурсов;

13) система мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" (далее – система мониторинга обеспечения информационной безопасности) – организационные и технические мероприятия, направленные на проведение мониторинга безопасного использования информационно-коммуникационных технологий, включая мониторинг событий информационной безопасности и реагирование на инциденты информационной безопасности.

Иные понятия, используемые в настоящих Правилах, применяются в соответствии с Законом.

2. Порядок проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства"

4. Мониторингу подлежат введенные в промышленную эксплуатацию объекты информатизации "электронного правительства", за исключением:

электронных информационных ресурсов, содержащих сведения, составляющие государственные секреты;

содержащие, обрабатывающие и (или) передающие сведения, отнесенные государственным органом к разведывательной, контрразведывательной, оперативно-розыскной деятельности;

интернет-ресурсов и информационных систем Национального Банка Республики Казахстан, не интегрируемых с объектами информационно-коммуникационной инфраструктуры "электронного правительства";

электронных информационных ресурсов, информационно-коммуникационной инфраструктуры Администрации Президента Республики Казахстан, Канцелярии Премьер-Министра Республики Казахстан, Управления Делами Президента Республики Казахстан и его ведомств , Комитета Национальной Безопасности Республики Казахстан.

5. В целях проведения ГТС работ по Мониторингу, собственник или владелец организует передачу журналов регистрации событий объектов информатизации " электронного правительства" в электронном виде в единую систему сбора журналов регистрации событий собственника или владельца, в случае если

объект информатизации "электронного правительства" является распределенным также и со всех территориальных подразделений собственника или владельца.

6. Собственник или владелец направляет в ГТС заявку о необходимости проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объекта информатизации "электронного правительства" (далее – заявка) с предоставлением сведений об объекте информатизации "электронного правительства" по форме, согласно приложению 1 к настоящим Правилам с приложением следующих документов:

1) описание по организации системы сбора журналов регистрации событий;

2) информация по организации доступа работникам ГТС от собственника или владельца к объекту информатизации "электронного правительства";

3) перечень технических и программных средств объекта информатизации " электронного правительства" по форме, согласно перечню технических средств объекта информатизации "электронного правительства" и перечню программных средств объекта информатизации "электронного правительства" в соответствии с приложениями 2 и 3 к настоящим Правилам, утвержденный собственником или владельцем и заверенный его подписью и печатью;

4) общая функциональная схема объекта информатизации "электронного правительства" с указанием используемых уникальных сетевых адресов серверов и рабочей станции администратора, утвержденная собственником или владельцем и заверенная его подписью и печатью и пояснительная записка к общей функциональной схеме в произвольной форме;

5) архитектура объекта информатизации "электронного правительства" в произвольной форме;

6) копии технической документации, утвержденной собственником или владельцем, заверенной его подписью и печатью, указанной в перечне технической документации, в соответствии с приложением 4 к настоящим Правилам.

7. После получения заявки ГТС в течение трех рабочих дней осуществляет проверку соответствия заявки и прилагаемых к заявке документов в соответствии с требованиями, установленными пунктом 6 настоящих Правил.

При соответствии заявки и приложенных документов требованиям, указанным в пункте 6 настоящих Правил, ГТС в течение трех рабочих дней после получения заявки уведомляет о проведении Мониторинга собственника или владельца.

8. Для проведения ГТС работ по Мониторингу, собственник или владелец организует:

круглосуточный доступ работникам ГТС в здание серверного центра и в служебные помещения собственника или владельца, в которых размещены

объекты информатизации "электронного правительства", а также доступ работникам ГТС к объекту информатизации "электронного правительства" и системе сбора журналов регистрации событий на основании списка работников, который направляется официальным письмом ГТС ежегодно и при его изменении;

два рабочих места для работников ГТС с предоставлением круглосуточного сетевого доступа к объектам информатизации, в отношении которых ими проводится Мониторинг.

Доступ к системам собственника или владельца работникам ГТС предоставляется в сопровождении представителей собственника или владельца.

9. ГТС при проведении Мониторинга осуществляет:

1) мониторинг обеспечения информационной безопасности объектов информатизации "электронного правительства" посредством системы мониторинга обеспечения информационной безопасности, включающий в себя:

установку агентов с предоставлением собственнику либо владельцу описания общего принципа их работы, запускаемых службах внутри операционных систем , используемых портах, необходимых настройках и дополнительных программных модулях или библиотеках;

по запросу собственника или владельца, ГТС осуществляет установку агентов на тестовом оборудовании, предоставляемом собственником или владельцем, в целях исключения сбоев в работе объекта информатизации;

на постоянной основе сбор событий в системе управления событиями информационной безопасностью, их обработку, анализ и уведомление о них собственника или владельца;

на постоянной основе выявление инцидентов и уведомление о них собственника или владельца в течение 15 минут с момента выявления ГТС инцидента в рабочее время;

анализ инцидентов совместно с собственником или владельцем;

выдачу рекомендаций собственнику или владельцу по устранению инцидентов и дальнейшему их предотвращению в течение одного рабочего дня с момента выявления инцидента ГТС;

в случае определения инцидента на объекте информатизации "электронного правительства", направление работника ГТС, находящегося на рабочем месте, обеспеченном собственником или владельцем в соответствии с пунктом 8 настоящих Правил, к месту инцидента при определении необходимости ГТС и собственником или владельцем;

уведомление уполномоченного органа о не устранении собственником или владельцем инцидента в течение пяти рабочих дней с момента выявления данного инцидента;

2) мониторинг обеспечения защиты объектов информатизации "электронного правительства", включающий в себя:

инструментальное обследование объектов информатизации "электронного правительства" из локальной сети серверов, внутренней локальной сети собственника или владельца и Интернета согласно графику проведения работ по Мониторингу, предварительно согласованному с собственником или владельцем (далее – график);

выявление программных и технических уязвимостей согласно графику;

ежегодный анализ конфигурации активного сетевого и серверного оборудования;

тестирование на проникновение с эксплуатацией уязвимостей при определении необходимости уполномоченным органом и по предварительному письменному согласованию с собственником или владельцем;

предоставление в течении пяти рабочих дней после окончания работ по инструментальному обследованию собственника или владельца информации о результатах инструментального обследования, с указанием данных об уникальных уязвимостях и рекомендациями по устранению выявленных уязвимостей, официальным письмом на электронном носителе в форматах PDF и XLS;

в случае необходимости проведение консультаций и разъяснений собственникам или владельцам по вопросам устранения уязвимостей работником ГТС, находящимся на рабочем месте, обеспеченном собственником или владельцем в соответствии с пунктом 8 настоящих Правил;

3) мониторинг обеспечения безопасного функционирования объектов информатизации "электронного правительства", включающий в себя:

направление собственнику или владельцу рекомендаций по устранению угроз при их выявлении;

проверку исполнения технической документации, указанной в приложении 4 к настоящим Правилам;

направление собственнику или владельцу рекомендаций по проведению необходимых мероприятий по результатам проверки исполнения технической документации, указанной в приложении 4 к настоящим Правилам.

10. Собственник или владелец при проведении ГТС мониторинга обеспечения информационной безопасности объектов информатизации " электронного правительства":

организует подключение системы сбора журналов регистрации событий объектов информатизации "электронного правительства" к системе управления событиями информационной безопасностью ГТС;

на постоянной основе сопровождает журнал инцидентов на объектах

информатизации "электронного правительства" и информирует ГТС об их обнаружении в течение пятнадцати минут с момента выявления;

на постоянной основе реализует процедуру уведомления об инцидентах и принимает меры по их устранению в соответствии с технической документацией согласно приложению 4 к настоящим Правилам;

в срок не позднее десяти рабочих дней с момента обнаружения инцидента предоставляет в ГТС информацию о причинах возникновения данных инцидентов, принятых мерах, направленных на предотвращение повторного появления данного инцидента, понесенном ущербе (при наличии).

11. Собственник или владелец при проведении ГТС мониторинга обеспечения защиты объектов информатизации "электронного правительства":

в течение одного месяца после получения результатов инструментального обследования устраняет уязвимости и направляет в ГТС отчет об их устранении;

в случае неустранения уязвимости относит ее к одной из категорий причин неустранения уязвимости и проводит действия в соответствии с перечнем категорий причин неустранения уязвимости и действий собственника или владельца в случае ее неустранения согласно приложению 5 к настоящим Правилам.

12. Собственник или владелец при проведении ГТС мониторинга обеспечения безопасного функционирования объектов информатизации " электронного правительства":

на постоянной основе анализирует выявленные ГТС угрозы и для предотвращения их повторного возникновения в последующем принимает меры по их устранению;

в течение одного месяца после получения информации об угрозах уведомляет ГТС о принятых мерах по устранению угроз;

проводит необходимые мероприятия в соответствии с рекомендациями ГТС;

ежегодно направляет в ГТС информацию по объектам информатизации, введенным в промышленную эксплуатацию.

13. По результатам Мониторинга ГТС направляет в уполномоченный орган сводную информацию по выявленным уязвимостям, угрозам, событиям информационной безопасности и инцидентам, а также о мерах принятых собственником или владельцем по их устранению ежеквартально, не позднее пятого числа месяца, следующего за отчетным кварталом.

Приложение 1
к Правилам проведения мониторинга
обеспечения информационной
безопасности, защиты и безопасного
функционирования объектов
информатизации "электронного
правительства"

Форма

Заявка

о проведении мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объекта информатизации "электронного правительства"

1) Местонахождение объекта информатизации "электронного правительства".

2) Контактная информация ответственных лиц собственника или владельца.

3) Информация о наличии доступа работникам ГТС к объекту информатизации "электронного правительства".

4) Информация о наличии точки подключения к Единой транспортной среде государственных органов и пропускной способности канала связи.

5) Информация о наличии системы сбора журналов регистрации событий, включая ведение в электронном виде журналов событий всех объектов информатизации "электронного правительства" со всех территориальных подразделений в центральное подразделение собственника или владельца.

6) Информация о внешнем IP-адресе (или IP-адресах), доменном имени (при наличии).

Приложение 2
к Правилам проведения мониторинга
обеспечения информационной
безопасности, защиты и безопасного
функционирования объектов
информатизации "электронного
правительства"

Форма

Перечень технических средств объекта информатизации "электронного правительства"

№ п\п	Производитель, модель	Серийный/ инвентарный номер	Номер сертификата по информационной безопасности (при наличии)	Физическое месторасположение	Тип (согласно технической документации)	Основное функциональное назначение(согласно программной документации к объекту информатизации "электронного правительства")	Используемы методы защиты информации
1	2	3	4	5	6	7	8

Приложение 3

к Правилам проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства"

Форма

Перечень программных средств объекта информатизации "электронного правительства"

№ п\п	Разработчик	Название	Версия	Место установки (из перечня технических средств)	Тип (согласно программной документации)	Основное функциональное назначение (согласно программной документации)	Используемые методы защиты информации
1	2	3	4	5	6	7	8

Приложение 4
к Правилам проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства"

Перечень технической документации

1. Политика информационной безопасности.

2. Методика оценки рисков информационной безопасности. Каталог угроз (рисков) информационной безопасности. План обработки угроз (рисков) информационной безопасности.

3. Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации.

4. Правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации.

5. Правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения.

6. Правила проведения внутреннего аудита информационной безопасности.

7. Правила использования криптографических средств защиты информации.

8. Правила разграничения прав доступа к электронным информационным ресурсам.

9. Правила использования Интернета и электронной почты.

10. Правила организации процедуры аутентификации.

11. Правила организации антивирусного контроля.

12. Правила организации физической защиты средств обработки информации и безопасной среды функционирования электронных информационных ресурсов.

13. Регламент резервного копирования и восстановления информации.

14. Инструкция о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях.

Приложение 5
к Правилам проведения мониторинга
обеспечения информационной
безопасности, защиты и безопасного
функционирования объектов
информатизации "электронного
правительства"

Категории причин неустранения уязвимости и действия собственника или владельца в случае ее неустранения

Категории причин неустранения уязвимости	Действия собственника или владельца в случае неустранения уязвимости и отнесения ее к соответствующей категории
Производственная необходимость	Собственник или владелец отмечает в отчете об устранениях уязвимостей предпринятые меры по устранению уязвимости, причины и характер требуемых изменений, сроки устранения уязвимости, не превышающие шести месяцев с момента первого обнаружения;
Уязвимость нулевого дня	Собственник или владелец отмечает в отчете об устранениях проведенные мероприятия по снижению вероятности эксплуатации уязвимости;
Ложное срабатывание	Собственник или владелец отмечает в отчете об устранениях уязвимостей описание уязвимости и состояния объекта информатизации "электронного правительства", а также предпринятые меры по устранению уязвимости.