Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры

Приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 7 июня 2018 года № 17019.

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

1. Утвердить прилагаемые Правила проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры.

2. Признать утратившим силу приказ исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 26 января 2016 года № 66 "Об утверждении Правил проведения мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 13178, опубликован 10 марта 2016 года в информационно-правовой системе "Әділет").

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

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

2) в течение десяти календарных дней со дня государственной регистрации в Министерстве юстиции Республики Казахстан 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 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*

"СОГЛАСОВАНО"
Председатель Комитета
национальной безопасности
Республики Казахстан
_____ К. Масимов
"___" _____ 2018 года

	Утверждены приказом Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ

Правила проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры

Глава 1. Общие положения

1. Настоящие Правила проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры (далее – Правила) разработаны в соответствии с подпунктом 7) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" (далее – Закон) и определяют порядок проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры.

2. В настоящих Правилах используются следующие понятия и сокращения:

1) объекты информатизации – электронные информационные ресурсы, программное обеспечение и информационно-коммуникационная инфраструктура;

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

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

4) аттестация информационной системы, информационно-коммуникационной платформы "электронного правительства" и интернет-ресурса государственного органа на соответствие требованиям информационной безопасности (далее – аттестация по ИБ) – организационно-технические мероприятия по определению состояния защищенности объектов аттестации, а также их соответствия требованиям информационной безопасности;

5) техническая документация по информационной безопасности – документация, устанавливающая политику, правила, защитные меры, касающиеся процессов обеспечения ИБ объектов информатизации и (или) организации;

6) агент системы управления событиями информационной безопасности – программное обеспечение, устанавливаемое на серверное и активное сетевое оборудование объекта информатизации для сбора журналов регистрации событий;

7) система управления событиями информационной безопасности – программное обеспечение или аппаратно-программный комплекс, предназначенные для автоматизированного выявления событий информационной безопасности и инцидентов информационной безопасности путем сбора и анализа журналов регистрации событий объекта информатизации;

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

9) оперативный центр информационной безопасности (далее – ОЦИБ) – юридическое лицо или структурное подразделение юридического лица, осуществляющее деятельность по защите электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации;

10) инцидент информационной безопасности – 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;

11) национальный координационный центр информационной безопасности (далее – НКЦИБ) – структурное подразделение республиканского государственного предприятия на праве хозяйственного ведения "Государственная техническая служба" Комитета национальной безопасности Республики Казахстан;

12) критически важные объекты информационно-коммуникационной инфраструктуры (далее – КВОИКИ) – объекты информационно-коммуникационной инфраструктуры, в том числе информационно-коммуникационной инфраструктуры "электронного правительства", нарушение или прекращение функционирования которых приводит к чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства, инфраструктуры Республики Казахстан или для жизнедеятельности населения, проживающего на соответствующей территории;

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

14) журналирование событий – процесс записи информации о происходящих с объектом информатизации программных или аппаратных событиях в журнал регистрации событий;

15) единая система сбора журналов регистрации событий – аппаратно-программный комплекс, обеспечивающий централизованный сбор журналов регистрации событий объектов информатизации, их хранение и дальнейшую передачу в систему управления событиями информационной безопасности;

16) объекты информатизации "электронного правительства" (далее - ОИ ЭП) – 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;

17) мониторинг обеспечения информационной безопасности объектов информатизации "электронного правительства" (далее – МОИБ) – наблюдение за объектами информатизации "электронного правительства" с целью выявления угроз и инцидентов информационной безопасности, а также принятия мер по их устранению и предупреждению;

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

19) архитектурный портал "электронного правительства" – информационная система, предназначенная для осуществления регистрации, учета, хранения и систематизации сведений об объектах информатизации "электронного правительства" в соответствии с классификатором и дальнейшего использования государственными органами для мониторинга, анализа и планирования в сфере информатизации.

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

3. МОИБ проводится РГП "ГТС" посредством системы мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства".

4. Объектами МОИБ являются объекты информатизации "электронного правительства", введенные в промышленную эксплуатацию, за исключением:

электронных информационных ресурсов, содержащих сведения, составляющие государственные секреты;

объектов информатизации "электронного правительства" Национального Банка Республики Казахстан, не интегрируемых с объектами МОИБ.

Глава 2. Порядок проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства"

5. РГП "ГТС" для проведения МОИБ в качестве первичной информации использует сведения об объекте МОИБ из архитектурного портала "электронного правительства", а также сведения, полученные на этапах проведения испытаний сервисного программного продукта, информационно-коммуникационной платформы "электронного правительства", интернет-ресурса государственного органа и информационной системы на соответствие требованиям информационной безопасности и аттестации по ИБ, включая:

1) перечень программных и технических средств;

2) схемы сетей телекоммуникаций;

3) контрольные суммы исходных кодов и/или файлов программных средств;

4) структуры баз данных.

6. Собственник или владелец объекта МОИБ уведомляет РГП "ГТС" о вводе в промышленную эксплуатацию или выводе из нее объекта МОИБ в течение 10 рабочих дней со дня его ввода в промышленную эксплуатацию или вывода из нее и предоставляет сведения о данном объекте информатизации "электронного правительства" по форме, согласно приложению 1 настоящих Правил (далее – Сведения).

7. РГП "ГТС" разрабатывает график проведения работ по МОИБ и согласовывает его с Комитетом национальной безопасности Республики Казахстан (далее – КНБ РК) и собственником или владельцем объекта МОИБ.

8. РГП "ГТС" в рамках проведения МОИБ осуществляет:

1) отслеживание состояния объектов МОИБ государственных органов на предмет возникновения инцидентов ИБ, включающее:

анализ объекта информатизации государственного органа (далее – ГО) на предмет определения перечня журналов регистрации событий, необходимых для передачи в систему управления событиями ИБ РГП "ГТС";

установку агентов системы управления событиями ИБ на единую систему сбора журналов регистрации событий собственника или владельца объекта информатизации ГО и при необходимости на иные объекты информационно-коммуникационной инфраструктуры собственника или владельца объекта информатизации ГО;

сбор журналов регистрации событий объекта информатизации ГО в системе управления событиями ИБ РГП "ГТС", их обработку и анализ с целью выявления событий ИБ и инцидентов ИБ;

первичный анализ событий ИБ или инцидентов ИБ, выявленных на объекте информатизации ГО;

уведомление собственника или владельца объекта информатизации ГО о выявленных событиях ИБ и инцидентах ИБ в течение 30 минут с момента выявления события ИБ или инцидента ИБ, КНБ РК – в течение 24 часов;

выдачу первичных рекомендаций по приостановлению распространения инцидента ИБ собственнику или владельцу объекта информатизации ГО;

направление, при необходимости, к месту размещения объекта информатизации ГО работника РГП "ГТС" в рамках реагирования на инцидент ИБ (необходимость определяется КНБ РК или РГП "ГТС" самостоятельно);

анализ инцидентов ИБ, выявленных на объекте информатизации ГО;

выдачу рекомендаций собственнику или владельцу объекта информатизации ГО по устранению инцидентов ИБ и дальнейшему их предупреждению в течение 48 часов с момента завершения анализа инцидента РГП "ГТС";

уведомление Министерства оборонной и аэрокосмической промышленности Республики Казахстан (далее – МОАП РК) и КНБ РК о неустранении собственником или владельцем объекта информатизации ГО инцидента ИБ в течение 48 часов с момента выдачи рекомендаций по устранению инцидента ИБ и дальнейшему их предупреждению;

2) отслеживание состояния защищенности объекта МОИБ, включающее:

обследование объектов МОИБ на предмет наличия уязвимостей (далее – обследование на уязвимости) согласно графику проведения работ по МОИБ;

предоставление результатов обследования на уязвимости и рекомендаций по устранению уязвимостей объектов МОИБ собственникам или владельцам объектов МОИБ в течение 10 рабочих дней после завершения работ по обследованию на уязвимости;

консультирование собственников или владельцев объектов МОИБ по вопросам устранения уязвимостей объектов МОИБ, выявленных в рамках обследования на уязвимости;

3) отслеживание полноты и качества реализации технических и организационных мероприятий по обеспечению ИБ объектов МОИБ, включающее в себя:

обследование объекта МОИБ на предмет исполнения требований технической документации по информационной безопасности (далее – ТД по ИБ), приведенной в приложении 2 настоящих Правил, согласно графику проведения работ по МОИБ;

предоставление результатов обследования объекта МОИБ на предмет исполнения требований ТД по ИБ и рекомендаций по устранению выявленных нарушений ТД по ИБ собственникам или владельцам объектов МОИБ в течение 10 рабочих дней со дня завершения данного обследования;

4) отслеживание неизменности условий функционирования и функциональности объектов МОИБ, включающее в себя:

проведение организационных и технических мероприятий по выявлению изменений условий функционирования и функциональности объектов МОИБ (далее – изменения объектов МОИБ) согласно графику проведения работ по МОИБ;

учет выявленных изменений объектов МОИБ;

анализ выявленных изменений объектов МОИБ;

предоставление КНБ РК и собственнику или владельцу объекта МОИБ результатов анализа изменений объекта МОИБ в течение 10 рабочих дней с момента выявления изменений объекта МОИБ.

9. Собственник или владелец объекта МОИБ обеспечивает условия для проведения РГП "ГТС" работ по МОИБ, включая:

круглосуточный физический доступ работникам РГП "ГТС" к объекту МОИБ, к единой системе сбора журналов регистрации событий собственника или владельца объекта МОИБ в сопровождении работников собственника или владельца объекта МОИБ;

два рабочих места для работников РГП "ГТС" с предоставлением круглосуточного сетевого доступа к объекту МОИБ на безвозмездной основе;

сетевой доступ для РГП "ГТС" к единой системе сбора журналов регистрации событий собственника или владельца объекта МОИБ с правами на исполнение всех без исключения операций.

10. При проведении РГП "ГТС" отслеживания состояния объектов МОИБ государственных органов на предмет возникновения инцидентов ИБ собственник или владелец объекта информатизации ГО:

организует журналирование событий объекта информатизации ГО в соответствии с форматами и типами записей журналов регистрации событий объектов информатизации "электронного правительства", приведенными в приложении 3 настоящих Правил;

организует передачу журналов регистрации событий объекта информатизации ГО в единую систему сбора журналов регистрации событий собственника или владельца объекта информатизации ГО;

уведомляет РГП "ГТС" о планируемых работах по внесению изменений в журналирование событий объекта информатизации ГО за 5 рабочих дней до внесения изменений. К уведомлению прикладываются образцы изменяемых журналов регистрации событий и их описание;

обеспечивает условия, согласованные с РГП "ГТС", для передачи журналов регистрации событий объекта информатизации ГО из единой системы сбора журналов регистрации событий собственника или владельца объекта информатизации ГО в систему управления событиями ИБ РГП "ГТС";

уведомляет РГП "ГТС" о самостоятельно выявленном инциденте ИБ объекте информатизации ГО в течение 15 минут с момента выявления;

предоставляет в РГП "ГТС" перечень данных об инциденте ИБ, выявленном на объекте информатизации ГО (далее – Перечень данных), по форме, согласно приложению 4 настоящих Правил в течение 24 часов с момента обнаружения инцидента ИБ.

11. При проведении РГП "ГТС" отслеживания состояния защищенности объектов МОИБ собственник или владелец объектов МОИБ:

направляет в РГП "ГТС" информацию о мерах, принятых для устранения уязвимостей объекта МОИБ, в течение 1 месяца со дня получения результатов обследования на наличие уязвимостей;

в случае неустранения уязвимости объекта МОИБ присваивает уязвимости одну из категорий (производственная необходимость, уязвимость нулевого дня, ложное срабатывание) и проводит необходимые действия согласно приложению 5 настоящих Правил;

в случае самостоятельного обнаружения уязвимости объекта МОИБ предоставляет в РГП "ГТС" перечень данных об уязвимости объекта информатизации "электронного правительства" по форме согласно приложению 6 настоящих Правил в течение 24 часов с момента выявления уязвимости объекта МОИБ.

12. При проведении РГП "ГТС" отслеживания полноты и качества реализации технических и организационных мероприятий по обеспечению ИБ объектов МОИБ собственник или владелец объекта МОИБ в течение одного месяца со дня получения результатов обследования объекта МОИБ на предмет исполнения требований ТД по ИБ предоставляет в РГП "ГТС" информацию о мерах, принятых по выявленным нарушениям требований ТД по ИБ.

13. В случае недостаточности данных для анализа изменений объекта МОИБ при проведении отслеживания неизменности условий функционирования и функциональности объекта МОИБ РГП "ГТС" запрашивает дополнительные данные об объекте МОИБ. Собственник или владелец объекта МОИБ предоставляет в РГП "ГТС" дополнительные данные об объекте МОИБ в течение 3 рабочих дней со дня получения запроса от РГП "ГТС".

14. С целью формирования перечня объектов МОИБРГП "ГТС" осуществляет запрос Сведений. Собственник или владелец объекта МОИБ предоставляет в РГП "ГТС" Сведения в электронной форме в течение 10 рабочих дней с момента получения запроса от РГП "ГТС".

15. В случае изменения контактных данных лица, ответственного за обеспечение ИБ объекта МОИБ, собственник или владелец объекта МОИБ в течение 48 часов с момента данного изменения направляет в РГП "ГТС" актуальные контактные данные.

16. РГП "ГТС" ежеквартально направляет в МОАП РК и КНБ РК сводную информацию по выявленным событиям ИБ, инцидентам ИБ, уязвимостям ОИ ЭП, изменениям ОИ ЭП и выявленным нарушениям требований ТД по ИБ, а также сведения о принятых собственниками или владельцами объектов МОИБ мерах.

Глава 3. Порядок проведения мониторинга обеспечения информационной безопасности критически важных объектов информационно-коммуникационной инфраструктуры

17. Мониторинг обеспечения информационной безопасности объектов информатизации КВОИКИ осуществляется собственным подразделением по ИБ владельца КВОИКИ или приобретением услуг третьих лиц в соответствии с гражданским законодательством Республики Казахстан.

18. Собственник или владелец КВОИКИ обеспечивает подключение системы мониторинга обеспечения информационной безопасности (далее – СМО ИБ) КВОИКИ к техническим средствам ОЦИБ, а также определяет ответственного по ИБ КВОИКИ в течение тридцати календарных дней со дня включения в перечень КВОИКИ, утверждаемый согласно подпункту 4) статьи 6 Закона.

19. Подключение СМО ИБ КВОИКИ к техническим средствам ОЦИБ осуществляется подразделением по ИБ собственника или владельца КВОИКИ или приобретением услуг третьих лиц в соответствии с гражданским законодательством Республики Казахстан.

20. После подключения СМО ИБ КВОИКИ к техническим средствам ОЦИБ при выявлении системой мониторинга обеспечения ИБ ОЦИБ инцидента ИБ, ОЦИБ уведомляет собственника или владельца КВОИКИ о выявленном инциденте ИБ, путем оповещения ответственного по ИБ КВОИКИ, в срок не позднее 24 часов с момента выявления инцидента ИБ.

21. Собственник или владелец КВОИКИ исправляет выявленные уязвимости в течение тридцати календарных дней после получения уведомления.

22. В случае самостоятельного выявления инцидента ИБ подразделением по ИБ КВОИКИ, ответственный по ИБ КВОИКИ оповещает НКЦИБ и ОЦИБ путем направления Перечня данных в течение 24 часов с момента выявления инцидента ИБ.

	Приложение 1 к Правилам проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры Форма

Сведения об объекте информатизации "электронного правительства"

1. Официальное наименование объекта информатизации "электронного правительства".

2. Собственник объекта информатизации "электронного правительства".

3. Владелец объекта информатизации "электронного правительства" (при наличии).

4. Физическое месторасположение объекта информатизации "электронного правительства" (город, область).

5. Информация о наличии подключения объекта информатизации "электронного правительства" к Единой транспортной среде государственных органов и пропускной способности канала связи.

6. Информация о наличии подключения объекта информатизации "электронного правительства" к Интернету: IP-адрес (или IP-адреса), доменные имена (при наличии).

7. Общая функциональная схема объекта информатизации "электронного правительства" с пояснительной запиской, утвержденная собственником или владельцем объекта информатизации "электронного правительства" и заверенная его подписью и печатью.

8. Логическая и физическая архитектурные схемы объекта информатизации "электронного правительства", утвержденные собственником или владельцем объекта информатизации "электронного правительства" и заверенная его подписью и печатью.

9. Утвержденный собственником или владельцем объекта информатизации "электронного правительства" и заверенный его подписью и печатью перечень технических средств объекта информатизации "электронного правительства" по форме, согласно приложению 1 к настоящей форме.

10. Утвержденный собственником или владельцем объекта информатизации "электронного правительства" и заверенный его подписью и печатью перечень программных средств объекта информатизации "электронного правительства" по форме, согласно приложению 2 к настоящей форме.

11. Информация о системе сбора журналов регистрации событий с указанием названия системы, разработчика, форматов и приложением образцов журналов регистрации событий.

12. Копия технической документации по информационной безопасности, утвержденной собственником или владельцем, заверенной его подписью и печатью, согласно ТД по ИБ.

13. Контактные данные лица, ответственного за обеспечение информационной безопасности объекта информатизации "электронного правительства".

	Приложение 1 к Сведениям об объекте информатизации "электронного правительства" Форма

Перечень технических средств объекта информатизации "электронного правительства"

№ п/п …	Производитель, модель	Серийный/ инвентарный номер	Сетевой адрес	Физическое месторасположение	Тип (согласно технической документации)	Основное функциональное назначение (согласно программной документации к объекту информатизации "электронного правительства")	Используемые методы защиты информации	Разработчик, название, версия (встроенного программного обеспечения)
1	2	3	4	5	6	7	8	9

	Приложение 2 к Сведениям об объекте 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 2 к Правилам проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно- коммуникационной инфраструктуры Форма

Техническая документации по информационной безопасности

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.
15. Руководство администратора по сопровождению объекта информатизации.

	Приложение 3 к Правилам проведения мониторинга обеспечения информационной безопасности объектов информатизации

	"электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры Форма

Форматы и типы записей журналов регистрации событий объектов информатизации "электронного правительства"

Глава 1. Форматы и типы записей журналов регистрации событий операционной системы

1. Типы событий операционной системы (далее – ОС), подлежащие журналированию:

1) запуск/остановка системы;

2) работа с объектами операционной системы (открытие, сохранение, переименование, удаление, создание, копирование);

3) установка и удаление программного обеспечения (далее – ПО);

4) авторизация (вход и выход) пользователей в операционной системе, успешные и неуспешные попытки авторизации;

5) изменение системной конфигурации;

6) создание, удаление, модификация учетных записей;

7) активация/дезактивация систем защиты, таких как антивирусные системы и системы обнаружения вторжения, и средств ведения журнала регистрации событий;

8) изменение или попытки изменения настроек и средств управления защитой системы;

9) использование привилегированных учетных записей;

10) подключение/отключение устройства ввода/вывода;

11) неудавшиеся или отвергнутые действия пользователя;

12) неудавшиеся или отвергнутые действия, затрагивающие данные и другие ресурсы;

13) запуск, остановка процессов в ОС.

2. Журнал регистрации событий ОС содержит следующие поля:

1) дата и время (формат даты: ДД:ММ:ГГГГ, формат времени: ЧЧ:ММ:СС);

2) наименование хоста;

3) описание события.

3. События, которые следует фиксировать для серверных ОС семейства Linux:

1) фиксация подключений идентичной учетной записи с разных IP-адресов на один и тот же сервер;

2) фиксация запуска новых портов в системе;

3) фиксация ключевых логов: /var/log/secure, /var/log/messages, /var/log/audit.

4. Список событий, включая штатную информацию о них, предоставляемую средствами журналирования ОС семейства Windows:

1) присвоение специальных привилегий новому сеансу (logon) – Windows EID 4672;

2) сетевой вход (Network logon) – Windows EID 4624;

3) доступ к сетевой папке администратора (administrative share access) и доступ к SMB каналам (pipes) – Windows EID 5140/5145;

4) доступ к объекту "Файл" с правами "Запись данных" или "Добавление файла" – Windows EID 4663;

5) запуск потенциально опасных процессов (WmiPrvSE.exe, WinrsHost.exe, wsmprovhost.exe, mmc.exe, psexe*.exe, paexe*.exe) – Sysmon EID 1;

6) установка и запуск службы (сервиса) – Windows EID 7045/7036/4697;

7) создание или изменение параметров заданий в планировщике задач (scheduled tasks) – Windows EID 4698/4702;

8) достигнут таймаут службы– Windows EID 7009;

9) ошибка при запуске службы – Windows EID 7000;

10) изменено значение реестра – Windows EID 4657;

11) запись в пространство имен WMI – Windows EID 4662.

5. Записи в журналах регистрации событий хранятся в текстовом формате.

6. Значения полей журналов регистрации событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует
символ-разделитель, применяются символы-ограничители полей.

7. Для журналов регистрации событий используется кодировка UTF-8.

8. В один файл журнала регистрации событий не допускается запись событий, имеющих разные форматы данных.

Глава 2. Форматы и типы записей журналов регистрации событий системы управления базами данных

9. Типы событий системы управления базами данных, подлежащие журналированию:

1) контроль сессий (успешная/неуспешная авторизация, регистрация использования незарегистрированных учетных записей);

2) все действия пользователей базы данных (далее – БД) имеющих административные привилегии (включая команды select, create, alter, drop, truncate, rename, insert, update, delete, call (execute), lock);

3) все действия пользователей имеющих права на присвоение привилегий другим пользователям БД (grant, revoke,deny).

10. Журнал регистрации событий БД содержит следующие поля:

1) дата и время (формат даты: ДД:ММ:ГГГГ, формат времени: ЧЧ:ММ:СС);

2) имя учетной записи/ID пользователя;

3) IP-адрес хоста или наименование хоста;

4) описание события;

5) наименование объекта (таблицы, процедуры, функции, при возможности реализации).

11. Записи в журналах регистрации событий хранятся в текстовом формате.

12. Значения полей журналов регистрации событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует
символ-разделитель, применяются символы-ограничители полей.

13. Для журналов регистрации событий используется кодировка UTF-8.

14. В один файл журнала регистрации событий не допускается запись событий, имеющих разные форматы данных.

Глава 3. Форматы и типы записей журналов регистрации событий телекоммуникационного оборудования

15. Типы событий телекоммуникационного оборудования, подлежащие журналированию:

1) запуск/остановка системы;

2) изменение системной конфигурации;

3) создание, удаление, модификация локальных учетных записей;

4) использование привилегированных учетных записей;

5) подключение/отключение устройства ввода/вывода;

6) неудавшиеся или отвергнутые действия пользователя;

7) запуск, падение, остановка сетевых линков (коннектов).

16. С межсетевых экранов при наличии технической возможности ведется запись логов всего трафика (входящего и исходящего), а также запись всех событий на устройстве.

17. Журнал регистрации событий телекоммуникационного оборудования содержит следующие поля:

1) дата и время (формат даты: ДД:ММ:ГГГГ, формат времени: ЧЧ:ММ:СС);

2) наименование устройства;

3) имя учетной записи/ID пользователя;

4) IP-адрес хоста;

5) IP-адрес источника;

6) IP-адрес назначения;

7) описание события.

18. Записи в журналах регистрации событий хранятся в текстовом формате.

19. Значения полей журналов регистрации событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует символ-разделитель, применяются символы-ограничители полей.

20. Для журналов регистрации событий используется кодировка UTF-8.

21. В один файл журнала регистрации событий не допускается запись событий, имеющих разные форматы данных.

Глава 4. Форматы и типы записей журналов регистрации событий прикладного программного обеспечения

22. Типы событий ПО, подлежащие журналированию:

1) авторизация (вход и выход) пользователей, успешные и неуспешные попытки авторизации;

2) создание, копирование, перемещение, удаление, модификация локальных учетных записей и конфигурационных файлов;

3) неудавшиеся или отвергнутые действия пользователя;

4) получение пользователем доступа к объектам доступа;

5) действия пользователей прикладного ПО (доступ к объекту (данным), изменения объекта (данных), удаления объекта (данных)).

23. Журнал регистрации событий ПО содержит следующие поля:

1) дата и время (формат даты: ДД:ММ:ГГГГ, формат времени: ЧЧ:ММ:СС);

2) наименование источника события (сервис/служба);

3) имя учетной записи/ID пользователя;

4) IP-адрес пользователя;

5) время начала операции;

6) время окончания операции;

7) описание события.

24. Записи в журналах регистрации событий хранятся в текстовом формате.

25. Значения полей журналов регистрации событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует
символ-разделитель, применяются символы-ограничители полей.

26. Для журналов регистрации событий используется кодировка UTF-8.

27. В один файл журнала регистрации событий не допускается запись событий, имеющих разные форматы данных.

Глава 5. Форматы и типы записей журналов регистрации событий средств защиты информации

28. Типы событий средств защиты информации, подлежащие журналированию:

1) создание, копирование, перемещение, удаление, модификация локальных учетных записей и конфигурационных файлов;

2) запуск/остановка службы;

3) изменение системной конфигурации;

4) создание, удаление, модификация локальных учетных записей.

29. Журнал регистрации событий средств защиты информации содержит следующие поля:

1) дата и время (формат даты: ДД:ММ:ГГГГ, формат времени: ЧЧ:ММ:СС);

2) наименование источника события (сервис/служба);

3) имя учетной записи/ID пользователя;

4) IP-адрес клиента;

5) время начала операции;

6) время окончания операции;

7) описание события.

30. Записи в журналах регистрации событий хранятся в текстовом формате.

31. Значения полей журналов регистрации событий разделяются символами-разделителями, в случае если поле имеет длинный формат и в содержании поля присутствует
символ-разделитель, применяются символы-ограничители полей.

32. Для журналов регистрации событий используется кодировка UTF-8.

31. В один файл журнала регистрации событий не допускается запись событий, имеющих разные форматы данных.

	Приложение 4 к Правилам проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры Форма

Перечень данных об инциденте информационной безопасности

Дата регистрации инцидента	
Уровень критичности инцидента информационной безопасности*	Уровень 5 (черный); уровень 4 (красный); уровень 3 (оранжевый); уровень 2 (желтый); уровень 1 (зеленый); уровень 0 (белый).

Тип инцидента	Отказ в облуживании (DoS, DDoS); несанкционированный доступ и модификация содержания; ботнет; вирусная атака; эксплуатация уязвимостей; компрометация средств аутентификации/авторизации; фишинг; другой.
Масштабность	Единичный; массовый.
Детали	Дата и время возникновения; дата и время обнаружения; дата и время сообщения; закончился ли инцидент (если "да", то уточнить, как долго длилось событие в днях/часах/минутах); повторный/новый; индикатор компрометации (IOC).
Признак	Действительный; попытка; подозрение;
Источник	Внутренний контур; внешний контур.
Описание инцидента	
Последствие	Без последствий; нарушение работоспособности; нарушение целостности; нарушение режима; конфиденциальности информации.
Объект, которому нанесен ущерб	
Действия, предпринятые для разрешения инцидента	
Примечание	

Уровни критичности инцидента информационной безопасности

	Уровень критичности	Определение
Критичный	Уровень 5 (черный)	Неизбежные инциденты, которые приведут к невозможности предоставления услуг, значительным негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации.

Серьезный	Уровень 4 (красный)	Возможные инциденты, которые приведут к невозможности предоставления услуг, значительным негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации.
Высокий	Уровень 3 (оранжевый)	Возможные инциденты, которые приведут к существенному ограничению предоставления услуг, существенному ухудшению ситуации или существенным негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации.
Средний	Уровень 2 (желтый)	Вероятные инциденты, которые приведут к ограничению предоставления государственных услуг, ухудшению ситуации или негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации.
Низкий	Уровень 1 (зеленый)	Маловероятные инциденты, которые приведут к ограничению предоставления услуг, ухудшению ситуации или незначительным негативным последствиям для электронных информационных ресурсов, информационных систем, сетей телекоммуникаций и других объектов информатизации.
Не критичный	Уровень 0 (белый)	Несущественные инциденты, не оказывающие влияние на электронные информационные ресурсы, информационные системы, сетей телекоммуникаций и других объектов информатизации.

	Приложение 5 к Правилам проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры Форма

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

Категории причин неустранения уязвимости	Обоснование причины неустранения уязвимости

Производственная необходимость	Описание уязвимости и состояние объекта информатизации "электронного правительства"; предпринятые меры по устранению уязвимости; причины и характер требуемых изменений в объекте информатизации; сроки устранения уязвимости, не превышающие шести месяцев с момента первого обнаружения
Уязвимость нулевого дня	Описание уязвимости и состояние объекта информатизации "электронного правительства", а также проведенные мероприятия по снижению вероятности эксплуатации уязвимости
Ложное срабатывание	Описание характеристики или состояние объекта информатизации "электронного правительства", определенного как уязвимость

	Приложение 6 к Правилам проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры Форма

Перечень данных об уязвимости объекта информатизации "электронного правительства"

Дата и время обнаружения уязвимости	Контур	Название объекта информа-тизации	Компонент объекта информатизации (название, IP, hostname и т.д.)	Порт	Описание уязвимости	Дополни-тельная информация
1	2	3	4	5	6	7
	Внешний/ Внутрен-ний контур					