О внесении изменения в приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ "Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры"

Приказ Министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан от 13 августа 2019 года № 195/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 15 августа 2019 года № 19247

Примечание ИЗПИ!

Настоящий приказ вводится в действие с 20 сентября 2019 года.

ПРИКАЗЫВАЮ:

1. Внести в приказ Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 марта 2018 года № 52/НҚ "Об утверждении Правил проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов за № 17019, опубликован 15 июня 2018 года в Эталонном контрольном банке нормативных правовых актов Республики Казахстан) следующее изменение:

Правила проведения мониторинга обеспечения информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры, утвержденные указанным приказом, изложить в новой редакции согласно приложению к настоящему приказу.

2. Комитету по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан обеспечить:

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

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

3) размещение настоящего приказа на интернет-ресурсе Министерства цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан после его официального опубликования;

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

3. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан.

4. Настоящий приказ вводится в действие с 20 сентября 2019 года.

Министр
цифрового развития, инноваций и
аэрокосмической промышленности
Республики Казахстан *А. Жумагалиев*

"СОГЛАСОВАН"
Комитет национальной безопасности
Республики Казахстан
"___" _____ 2019 года

Приложение
к приказу Министра
цифрового развития, инноваций и
аэрокосмической промышленности
Республики Казахстан
от 13 августа 2019 года
№ 195/НҚ

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, интернет-ресурс 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 или аппаратном обеспечении, обуславливающий возможность нарушения его работоспособности, либо выполнения каких-либо несанкционированных действий в обход разрешений, установленных в программном или аппаратном обеспечении;

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

5) 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;

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

7) 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;

8) уполномоченный орган в сфере обеспечения информационной безопасности (далее – уполномоченный орган) – центральный исполнительный орган, осуществляющий руководство и межотраслевую координацию в сфере обеспечения информационной безопасности;

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

14) 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;

15) объекты информатизации "электронного правительства" (далее – ОИ ЭП) – государственные электронные информационные ресурсы, программное обеспечение государственных органов, интернет-ресурсы государственного органа, объекты информационно-коммуникационной инфраструктуры "электронного правительства", в том числе сервисный программный продукт, программное обеспечение и информационные системы иных лиц, предназначенные для формирования государственных электронных информационных ресурсов в рамках осуществления государственных функций и оказания государственных услуг;

16) мониторинг обеспечения информационной безопасности объектов информатизации "электронного правительства" (далее – МОИБ) – отслеживание полноты и качества реализации собственниками и (или) владельцами объектов

информатизации технических и организационных мероприятий по обеспечению ИБ ОИ ЭП посредством выявления угроз и инцидентов ИБ;

17) 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;

18) 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 НКЦИБ посредством системы мониторинга обеспечения информационной безопасности НКЦИБ и включает в себя следующие виды работ:

мониторинг реагирования на инциденты ИБ;

мониторинг обеспечения защиты;

мониторинг обеспечения безопасного функционирования.

4. Объектами МОИБ являются введенные в промышленную эксплуатацию ОИ ЭП, в том числе отнесенные к КВОИКИ, за исключением:

электронных информационных ресурсов, содержащих сведения, составляющие государственные секреты;

информационных систем в защищенном исполнении, отнесенных к государственным секретам;

объектов информатизации Национального банка Республики Казахстан, не интегрируемых с ОИ ЭП.

5. МОИБ объектов информатизации ЭП проводится по одному из следующих вариантов:

1) по одному виду работ;

2) по нескольким видам работ;

3) в полном составе видов работ.

6. МОИБ ОИ ЭП, отнесенных к КВОИКИ, осуществляется на основании договорных отношений между Комитетом национальной безопасности Республики Казахстан (далее – КНБ РК) и республиканским государственным предприятием на

праве хозяйственного ведения "Государственная техническая служба" Комитета национальной безопасности Республики Казахстан, реализующего задачи и функции НКЦИБ.

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

7. НКЦИБ 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, 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.

8. Собственник или владелец объекта МОИБ уведомляет официальным письмом НКЦИБ о вводе в промышленную эксплуатацию, либо о прекращении эксплуатации объекта МОИБ в течение 10 рабочих дней со дня его ввода в промышленную эксплуатацию, либо прекращения эксплуатации, и предоставляет в бумажном и электронном виде сведения об ОИ ЭП по форме, согласно приложению 1 настоящих Правил (далее – Сведения).

9. НКЦИБ разрабатывает график проведения работ по МОИБ и согласовывает его с КНБ РК.

10. НКЦИБ при проведении МОИБ осуществляет:

1) в рамках мониторинга реагирования на инциденты ИБ:

анализ объекта МОИБ на предмет определения перечня журналов регистрации событий, необходимых для передачи в систему управления событиями ИБ НКЦИБ;

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

сбор журналов регистрации событий объекта МОИБ и относящихся к нему средств защиты информации, в системе управления событиями ИБ НКЦИБ, их обработку и анализ с целью выявления событий ИБ и инцидентов ИБ;

первичный анализ событий ИБ или инцидентов ИБ, выявленных на объекте МОИБ;

уведомление ответственных лиц за обеспечение ИБ объекта МОИБ с предоставлением перечня данных об инциденте ИБ, согласно приложению 2 настоящих Правил (далее – Перечень данных), 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 МОИБ;

направление, при необходимости, к месту размещения объекта МОИБ работника НКЦИБ в рамках реагирования на инцидент ИБ (необходимость определяется КНБ РК или НКЦИБ самостоятельно);

уведомление уполномоченного органа и КНБ РК о неустранении собственником или владельцем объекта МОИБ или уполномоченным им лицом причин и последствий инцидента ИБ по истечении 48 часов с момента выявления инцидента ИБ;

2) в рамках мониторинга обеспечения защиты:

обследование объектов МОИБ на предмет наличия уязвимостей (далее – обследование на уязвимости), включая анализ исходного кода программного обеспечения объекта МОИБ, 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) в рамках мониторинга обеспечения безопасного функционирования:

обследование объекта МОИБ на предмет исполнения требований технической документации по информационной безопасности (далее – ТД по ИБ), приведенной в приложении 3 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.

11. Собственник или владелец объекта МОИБ обеспечивает условия для проведения НКЦИБ работ по МОИБ, включая:

физический доступ работникам НКЦИБ к объекту МОИБ, к системе сбора журналов регистрации событий объекта МОИБ в сопровождении работников собственника или владельца объекта МОИБ или уполномоченного им лица;

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

сетевой доступ для НКЦИБ к системе сбора журналов регистрации событий объекта МОИБ с правами на исполнение всех без исключения операций;

доступ к технической документации по информационной безопасности, утвержденной собственником или владельцем объекта МОИБ, заверенной его подписью и печатью (при наличии).

12. При проведении НКЦИБ мониторинга реагирования на инциденты ИБ собственник или владелец объекта МОИБ:

организует журналирование событий объекта МОИБ и относящихся к нему средств защиты информации, в соответствии с форматами и типами записей журналов регистрации событий ОИ ЭП, приведенными в приложении 4 настоящих Правил;

организует систему сбора журналов регистрации событий в контуре телекоммуникационной сети, в котором функционирует объект МОИБ;

организует передачу журналов регистрации событий объекта МОИБ и относящихся к нему средств защиты информации, в систему сбора журналов регистрации событий объекта МОИБ;

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

обеспечивает условия, согласованные с НКЦИБ, для передачи журналов регистрации событий объекта МОИБ из системы сбора журналов регистрации событий объекта МОИБ в систему управления событиями ИБ НКЦИБ;

уведомляет НКЦИБ о самостоятельно выявленном инциденте ИБ на объекте МОИБ в течение 15 минут с момента выявления;

предоставляет в НКЦИБ Перечень данных в течение 24 часов с момента обнаружения инцидента ИБ.

13. При проведении НКЦИБ мониторинга обеспечения защиты собственник или владелец объектов МОИБ:

направляет в НКЦИБ информацию о мерах, принятых для устранения уязвимостей объекта МОИБ, в течение двадцати календарных дней со дня получения результатов обследования на наличие уязвимостей;

в случае самостоятельного обнаружения уязвимости объекта МОИБ, предоставляет в НКЦИБ перечень данных об уязвимости ОИ ЭП по форме согласно приложению 5 настоящих Правил в течение 24 часов с момента выявления уязвимости объекта МОИБ ;

в случае неустранения уязвимости объекта МОИБ может присвоить уязвимости одну из категорий (производственная необходимость, уязвимость нулевого дня, ложное срабатывание) и предоставляет в НКЦИБ категории причин неустранения уязвимости и обоснование причины неустранения согласно приложению 6 настоящих Правил.

14. При проведении НКЦИБ мониторинга обеспечения безопасного функционирования 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 НКЦИБ информацию о мерах, принятых по выявленным нарушениям требований ТД по ИБ.

15. С целью формирования перечня объектов МОИБ, НКЦИБ направляет запрос собственникам или владельцам объектов МОИБ о предоставлении Сведений. Собственник или владелец объекта МОИБ предоставляет в НКЦИБ Сведения в электронной форме в течение 10 рабочих дней с момента получения запроса от НКЦИБ
.

16. 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 НКЦИБ актуальные контактные данные.

17. НКЦИБ ежеквартально направляет в 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.

18. КНБ РК ежеквартально направляет в уполномоченный орган сводную информацию по выявленным 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, не относящихся к объектам информатизации "электронного правительства"

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

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

21. 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.

22. После подключения СМО ИБ КВОИКИ к техническим средствам ОЦИБ при выявлении СМО 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.

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

24. 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 (при наличии).

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

информатизации "электронного правительства" и заверенная его подписью и печатью (при наличии).

9. Утвержденный собственником или владельцем объекта информатизации " электронного правительства" и заверенный его подписью и печатью (при наличии) 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 (при наличии) 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 объекта МОИБ, заверенной его подписью и печатью (при наличии).

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

14. Перечень сетевых IP-адресов объекта информатизации "электронного правительства" и относящихся к нему средств защиты информации.

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 программно 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

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 3
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. Документы первого уровня:

1) политика информационной безопасности.

2. Документы второго уровня:

1) методика оценки рисков информационной безопасности;

2) правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации;

3) правила по обеспечению непрерывной работы активов, связанных со средствами обработки информации;

4) правила инвентаризации и паспортизации средств вычислительной техники, телекоммуникационного оборудования и программного обеспечения;

5) правила проведения внутреннего аудита ИБ;

6) правила использования средств криптографической защиты информации;

7) правила разграничения прав доступа к электронным информационным ресурсам;

8) правила использования Интернет и электронной почты;

9) правила организации процедуры аутентификации;

10) правила организации антивирусного контроля;

11) правила использования мобильных устройств и носителей информации;

12) правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов.

3. Документы третьего уровня:

1) каталог угроз (рисков) ИБ;

2) план обработки угроз (рисков) ИБ;

3) регламент резервного копирования и восстановления информации;

4) план мероприятий по обеспечению непрерывной работы и восстановлению работоспособности активов, связанных со средствами обработки информации;

5) руководство администратора по сопровождению объекта информатизации;

6) инструкцию о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях.

4. Документы четвертого уровня:

1) журнал регистрации инцидентов ИБ и учета внештатных ситуаций;

2) журнал посещения серверных помещений;

3) отчет о проведении оценки уязвимости сетевых ресурсов;

4) журнал учета кабельных соединений;

5) журнал учета резервных копий (резервного копирования, восстановления), тестирования резервных копий;

6) журнал учета изменений конфигурации оборудования, тестирования и учета изменений свободного программного обеспечения и прикладного программного обеспечения информационной системы, регистрации и устранения уязвимостей программного обеспечения;

7) журнал тестирования дизель-генераторных установок и источников бесперебойного питания для серверного помещения;

8) журнал тестирования систем обеспечения микроклимата, видеонаблюдения, пожаротушения серверных помещений.

Приложение 4
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 ОС (открытие, сохранение, переименование, удаление, создание, копирование);

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

4) авторизация (вход и выход) пользователей в ОС, 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. Для серверных ОС семейства Unix-подобных систем (Unix, Linux, AIX, HPUX и др.) дополнительно к событиям из пункта 1, необходима фиксация следующих событий :

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

2) открытие новых портов в системе;

3) всех событий в ключевых логах: /var/log/secure, /var/log/messages, /var/log/audit.

4. Для серверных ОС семейства Windows, дополнительно к событиям из пункта 1, необходима фиксация следующих событий:

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, выявляемые средствами защиты информации

28. Типы событий, выявляемые средствами 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.

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

Приложение 5
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 информатизации	Компонент объекта информатизации (название, IP, hostname и т.д.)	Порт	Описание уязвимости	Дополнительная информация
1	2	3	4	5	6	7
	Внешний/ Внутренний контур					

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

Категории причин неустранения уязвимости и обоснование причины 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.