

**Об утверждении Правил проведения мониторинга выполнения единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности**

Приказ и.о. Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 февраля 2018 года № 33/НҚ. Зарегистрирован в Министерстве юстиции Республики Казахстан 13 апреля 2018 года № 16756.

      В соответствии с подпунктом 8) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" и подпунктом 2) пункта 3 статьи 16 Закона Республики Казахстан от 19 марта 2010 года "О государственной статистике" ПРИКАЗЫВАЮ:

      1. Утвердить прилагаемые Правила проведения мониторинга выполнения единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности.

      2. 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 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.

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

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

|  |  |
| --- | --- |
| *Исполняющий обязанности Министра*  *оборонной и аэрокосмической*  *промышленности Республики Казахстан* | *М. Нургужин* |

|  |  |
| --- | --- |
| **"СОГЛАСОВАНО"**  **Министр информации и коммуникаций**  **Республики Казахстан**  **\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д. Абаев**  **6 марта 2018 год** | **"СОГЛАСОВАНО"**  **Исполняющий обязанности Председателя**  **Комитета по статистике**  **Министерства национальной экономики**  **Республики Казахстан**  **\_\_\_\_\_\_\_\_\_\_\_ Г. Керимханова**  **30 марта 2018 год** |
| **"СОГЛАСОВАНО"**  **Председатель Комитета**  **национальной безопасности**  **Республики Казахстан**  **\_\_\_\_\_\_\_\_\_\_\_ К. Масимов**  **13 марта 2018 год** |  |

|  |  |
| --- | --- |
|  | Утверждены приказом исполняющего обязанности Министра оборонной и аэрокосмической промышленности Республики Казахстан от 28 февраля 2018 года № 33/НҚ |

**Правила**  
**проведения мониторинга выполнения единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности**

**Глава 1. Общие положения**

      1. Настоящие Правила проведения мониторинга выполнения единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности (далее – Правила) разработаны в соответствии с подпунктом 8) статьи 7-1 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" (далее – Закон) и определяют порядок проведения мониторинга выполнения единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденных постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 (далее – ЕТ), относящихся к сфере обеспечения информационной безопасности.

      2. Мониторинг выполнения ЕТ проводится с целью определения полноты выполнения требований в сфере обеспечения информационной безопасности.

      3. Задачами проведения мониторинга выполнения ЕТ являются сбор, свод и анализ информации о ходе выполнения ЕТ в сфере обеспечения информационной безопасности.

      4. Мониторинг выполнения ЕТ осуществляется уполномоченным органом в сфере обеспечения информационной безопасности (далее – уполномоченный орган).

      5. Мониторинг выполнения ЕТ осуществляется в отношении государственных органов (далее – ГО), местных исполнительных органов (далее – МИО), государственных юридических лиц, субъектов квазигосударственного сектора, собственников и владельцев негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных электронных информационных ресурсов, а также собственников и владельцев критически важных объектов информационно-коммуникационной инфраструктуры, в части выполнения ими ЕТ.

      6. Настоящие Правила не распространяются на:

      1) отношения, возникающие при осуществлении Национальным Банком Республики Казахстан и организациями, входящими в его структуру, работ по созданию или развитию, эксплуатации интернет-ресурсов, информационных систем, не интегрируемых с объектами информационно-коммуникационной инфраструктуры "электронного правительства", локальных сетей и сетей телекоммуникаций, а также при проведении закупок товаров, работ и услуг в сфере информатизации;

      2) информационные системы в защищенном исполнении, отнесенные к государственным секретам в соответствии с законодательством Республики Казахстан о государственных секретах, а также сети телекоммуникаций специального назначения и (или) правительственной, президентской засекреченной, шифрованной и кодированной связи;

      3) информационные системы и интернет ресурсы специальных государственных органов.

**Глава 2. Порядок проведения мониторинга выполнения ЕТ в области информационно-коммуникационных технологий и обеспечения информационной безопасности**

      7. Мониторинг выполнения ЕТ осуществляется на основе:

      1) отчета о выполнении ЕТ, представляемой ежегодно субъектами указанными в пункте 5 настоящих Правил по форме согласно приложению к настоящим Правилам, (далее – отчет);

      2) информации, запрашиваемой уполномоченным органом у республиканского государственного предприятия "Государственная техническая служба" Комитета национальной безопасности Республики Казахстан в соответствии с подпунктом 5) статьи 7-1 Закона;

      3) информации, запрашиваемой уполномоченным органом у Оперативного центра информационной безопасности, Национального координационного центра информационной безопасности в соответствии с Законом.

      4) информация, размещенной на архитектурном портале "электронного правительства".

      Сноска. Пункт 7 с изменениями, внесенными приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 19.08.2019 № 200/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

      8. Государственные органы, местные исполнительные органы представляют отчет на казахском и русском языках в срок не позднее 25 числа месяца, следующего за отчетным периодом, в уполномоченный орган в электронном виде посредством единой системы электронного документооборота государственных органов.

      9. Государственные юридические лица, субъекты квазигосударственного сектора, собственники и владельцы негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных электронных информационных ресурсов, а также собственники и владельцы критически важных объектов информационно-коммуникационной инфраструктуры на добровольной основе представляют отчет на казахском и русском языках в срок не позднее 25 числа месяца, следующего за отчетным периодом, в уполномоченный орган на бумажном носителе.

      Отчетным периодом является календарный год.

      10. В случае если последний день срока предоставления отчета приходится на нерабочий день, сроком предоставления является следующий рабочий день.

      11. Уполномоченный орган на основе сводной информации проводит анализ выполнения требований ЕТ в сфере обеспечения информационной безопасности.

|  |  |
| --- | --- |
|  | Приложение  к Правилам проведения мониторинга выполнения единых требований в области информационно- коммуникационных технологий и обеспечения информационной безопасности |
|  | Форма, предназначенная для сбора административных данных |

**Отчет о выполнении ЕТ**

      Сноска. Приложение с изменениями, внесенными приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 19.08.2019 № 200/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования).

      Отчетный период 20\_\_\_ г.

**Индекс:** форма № 1-ФО

**Периодичность:** годовая

**Круг** **лиц** **представляющих:** государственные органы, местные исполнительные органы, государственные юридические лица, субъекты квазигосударственного сектора, собственники и владельцы негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных электронных информационных ресурсов, собственники и владельцы критически важных объектов информационно-коммуникационной инфраструктуры

**Куда** **представляется:** Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан

**Срок** **представления:** до 25 января после отчетного периода

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Перечень требований | Выполнено | Невыполнено | Причина невыполнения |
| 1 | 2 | 3 | 4 | 5 |
| Требования к организации и управлению информатизацией | | | | |
| 1. | Соблюдение требований по оборудованию рабочего пространства и места служащих государственного органа (далее – ГО) и местных исполнительных органов (далее – МИО) |  |  |  |
| 2. | Соблюдение требований по размещению рабочих станций служащих ГО или МИО |  |  |  |
| 3. | Соблюдение требований по защите рабочих станций от отказов в системе электроснабжения и других нарушений, вызываемых сбоями в работе коммунальных служб |  |  |  |
| 4. | Соблюдение требований по процедуре и периодичности технического обслуживания рабочих станций для обеспечения непрерывной доступности и целостности |  |  |  |
| 5. | Соблюдение требований по защите рабочих станций мобильных пользователей, находящихся за пределами ГО или МИО, с учетом различных внешних рисков |  |  |  |
| 6. | Соблюдение требований гарантированного уничтожения информации при повторном использовании рабочих станций или выводе из эксплуатации носителей информации |  |  |  |
| 7. | Соблюдение правил выноса рабочих станций за пределы рабочего места |  |  |  |
| 8. | Соблюдение учета рабочих станций с проверкой конфигураций |  |  |  |
| 9. | Соблюдение требований по отключению или блокированию неиспользуемых портов ввода-вывода рабочих станций и мобильных компьютеров служащих ГО и МИО |  |  |  |
| 10. | Соблюдение требований по обработке и хранению служебной информации ГО и МИО на рабочих станциях, подключенных к локальной сети внутреннего контура ГО или МИО и не имеющих подключения к Интернету |  |  |  |
| Требования к организации информационной безопасности | | | | |
| 11. | Соблюдение требований по наличию обособленного структурного подразделения по информационной безопасности |  |  |  |
| 12. | Наличие нормативно-технической документации по обеспечению информационной безопасности |  |  |  |
| 13. | Наличие методов оценки рисков в сфере информационно-коммуникационных технологий |  |  |  |
| 14. | Наличие каталога угроз (рисков) в сфере информационно-коммуникационных технологий |  |  |  |
| 15. | Осуществление контроля событий нарушений информационной безопасности |  |  |  |
| 16. | Соблюдение требований по хранению журналов регистрации событий в течении трех лет в оперативном доступе не менее трех месяцев |  |  |  |
| 17. | Наличие плана мероприятий по обеспечению непрерывной работы и восстановлению критически важных процессов |  |  |  |
| 18. | Соблюдение обязанностей по обеспечению информационной безопасности внесенных в должностные инструкции и (или) условия трудового договора |  |  |  |
| 19. | Соблюдение требований идентификации |  |  |  |
| 20. | Соблюдение требований по применению средств криптографической защиты информации |  |  |  |
| 21. | Обеспечение доступности и отказоустойчивости методами резервирования серверного оборудования |  |  |  |
| 22. | Обеспечение мониторинга действий пользователей и обеспечение блокировки аномальной деятельности пользователей |  |  |  |
| 23. | Соблюдение требований мониторинга обеспечения информационной безопасности |  |  |  |
| 24. | Наличие средств и систем обеспечения информационной безопасности |  |  |  |
| 25. | Наличие регистрационных свидетельств удостоверяющих центров |  |  |  |
| Требования к электронным информационным ресурсам и интернет-ресурсам | | | | |
| 26. | Соблюдение требований по формированию, размещению и хранению метаданных |  |  |  |
| 27. | Соблюдение требований по созданию или развитию информационных ресурсов |  |  |  |
| 28. | Соблюдение требований по обеспечению информационной безопасности информационных ресурсов |  |  |  |
| Требования к разрабатываемому или приобретаемому прикладному программному обеспечению | | | | |
| 29. | Соблюдение требований к создаваемому или развиваемому прикладному программному обеспечению информационной системы |  |  |  |
| 30. | Соблюдение требований к использованию готового прикладного программного обеспечения |  |  |  |
| 31. | Наличие технической поддержки и сопровождения программного обеспечения |  |  |  |
| 32. | Наличие мероприятия по контролю использования программного обеспечения:  -определение фактически используемого программного обеспечения;  -определение прав на использование программного обеспечения;  -сравнение фактически используемого программного обеспечения и имеющихся лицензий. |  |  |  |
| 33. | Соблюдение требований использования электронной цифровой подписи в прикладном программном обеспечении |  |  |  |
| Требования к информационной системе | | | | |
| 34. | Наличие акта о завершении опытной эксплуатации информационной системы |  |  |  |
| 35. | Строка исключена приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 19.08.2019 № 200/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования). | | | |
| 36. | Строка исключена приказом Министра цифрового развития, инноваций и аэрокосмической промышленности РК от 19.08.2019 № 200/НҚ (вводится в действие по истечении десяти календарных дней после дня его первого официального опубликования). | | | |
| 37. | Соблюдения требования предоставления системному интегратору "электронного правительства" для учета и хранения разработанного программного обеспечения: исходных кодов согласно единым требованиям, комплекса настроек лицензионного прикладного программного обеспечения (при наличии) информационной системы ГО и МИО |  |  |  |
| 38. | Соблюдение требования по обеспечению промышленной эксплуатации информационной системы ГО или МИО |  |  |  |
| 39. | Обеспечение управления информационной системы из внутренней локальной сети |  |  |  |
| Требования к технологической платформе | | | | |
| 40. | Наличие коэффициента бесперебойного и отказоустойчивого функционирования предоставляемых информационно-коммуникационных услуг |  |  |  |
| 41. | Соблюдение требований по управлению идентификацией |  |  |  |
| 42. | Соблюдение требований по управлению доступом |  |  |  |
| 43. | Соблюдение требований по управлению ключами шифрования |  |  |  |
| 44. | Соблюдение требований по проведению аудита событий информационной безопасности |  |  |  |
| 45. | Соблюдение требований регистрации событий информационной безопасности |  |  |  |
| 46. | Соблюдение требований по применению защитных мер аппаратных и программных компонентов инфраструктуры среды виртуализации |  |  |  |
| 47. | Наличие физического разделения сред эксплуатации от сред разработки и тестирования |  |  |  |
| 48. | Исполнение процедур сетевого и системного администрирования |  |  |  |
| Требования к аппаратно-программному комплексу | | | | |
| 49. | Проведение на регулярной основе инвентаризации серверного оборудования с проверкой его конфигурации |  |  |  |
| 50. | Соблюдение требования по размещению серверного оборудования |  |  |  |
| 51. | Наличие системы хранения данных обеспечивающей систему резервного копирования |  |  |  |
| Требования к сетям телекомуникаций | | | | |
| 52. | Соблюдение требований к выделенным каналам связи |  |  |  |
| 53. | Соблюдение требований по использованию служащими только ведомственной электронной почты при исполнении служебных обязанностей |  |  |  |
| 54. | Наличие оборудования кабельной системы |  |  |  |
| 55. | Наличие активного оборудования локальных сетей обеспечивающегося электропитанием от источников бесперебойного питания |  |  |  |
| Требования к системам бесперебойного функционирования технических средств и информационной безопасности | | | | |
| 56. | Соблюдение требований по монтажу оборудования |  |  |  |
| 57. | Наличие документирования при техническом сопровождении оборудования |  |  |  |
| 58. | Наличие системы контроля и управления доступом |  |  |  |
| 59. | Наличие системы обеспечения микроклимата |  |  |  |
| 60. | Наличие системы охранной сигнализации серверного помещения |  |  |  |
| 61. | Наличие системы видеонаблюдения |  |  |  |
| 62. | Наличие системы пожарной сигнализации серверного помещения |  |  |  |
| 63. | Наличие системы пожаротушения серверного помещения |  |  |  |
| 64. | Наличие системы гарантированного электропитания |  |  |  |
| 65. | Наличие системы заземления серверного помещения |  |  |  |

      Примечание:

      Пояснение по заполнению формы отчета о выполнении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности

      1. Настоящее пояснение по заполнению формы отчета, предназначенной для сбора административных данных, детализирует порядок ее заполнения (далее – форма отчет).

      2. Основной задачей формы отчета о выполнении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности (далее – ЕТ) является сбор, свод и анализ информации о ходе выполнения ЕТ в сфере обеспечения информационной безопасности.

      3. Заполненная форма отчета предоставляется в Министерство цифрового развития, инноваций и аэрокосмической промышленности Республики Казахстан:

      1) государственными и местными исполнительными органами отчет на казахском и русском языках в срок не позднее 25 числа месяца, следующего за отчетным периодом, посредством единой системы электронного документооборота государственных органов.

      2) государственными юридическими лицами, субъектами квазигосударственного сектора, собственниками и владельцами негосударственных информационных систем, интегрируемых с информационными системами государственных органов или предназначенных для формирования государственных электронных информационных ресурсов, а также собственниками и владельцами критически важных объектов информационно-коммуникационной инфраструктуры на добровольной основе в срок не позднее 25 числа месяца, следующего за отчетным периодом, на бумажном носителе.

      4. Форма отчета заполняется на казахском и русском языках.

      5. Форму отчета подписывает первый руководитель, а в случае его отсутствия – лицо, исполняющее его обязанности.

      6. Форма отчета заполняется следующим образом:

      в графе 3 "Выполнено" указывается обозначение знаком "+";

      в графе 4 "Не выполнено" указывается обозначение знаком "–";

      в графе 5 "Причина невыполнения" указывается подробная информация о невыполнении требований пунктов ЕТ.

      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(Наименование* *организации,* *БИН)*

      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*(Адрес,* *телефон,* *электронная* *почта)*

|  |  |
| --- | --- |
| Исполнитель  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Фамилия, имя, отчество (при наличии)  дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Руководитель  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Фамилия, имя, отчество (при наличии)  дата \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  подпись\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

© 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан» Министерства юстиции Республики Казахстан