

**Об утверждении Правил проведения аудита информационных систем**

Приказ Министра информации и коммуникаций Республики Казахстан от 13 июня 2018 года № 263. Зарегистрирован в Министерстве юстиции Республики Казахстан 29 июня 2018 года № 17141.

      В соответствии с подпунктом 22) статьи 7 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" ПРИКАЗЫВАЮ:

      1. Утвердить прилагаемые Правила проведения аудита информационных систем.

      2. Признать утратившим силу приказ исполняющего обязанности Министра по инвестициям и развитию Республики Казахстан от 28 января 2016 года № 134 "Об утверждении Правил проведения аудита информационных систем" (зарегистрирован в Реестре государственной регистрации нормативных правовых актов под № 13258, опубликован 10 марта 2016 года в информационно-правовой системе "Әділет").

      3. Департаменту информатизации Министерства информации и коммуникаций Республики Казахстан в установленном законодательном 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 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) размещение настоящего приказа на интернет-ресурсе Министерства информации и коммуникаций Республики Казахстан;

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

      4. Контроль за исполнением настоящего приказа возложить на курирующего вице-министра информации и коммуникаций Республики Казахстан.

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

|  |  |
| --- | --- |
|
*Министр информации* *и коммуникаций Республики Казахстан*
 |
*Д. Абаев*
 |

      "СОГЛАСОВАН"
Министр оборонной и аэрокосмической
промышленности Республики Казахстан
Б. Атамкулов
"\_\_" \_\_\_\_\_\_\_\_\_ 2018 год

|  |  |
| --- | --- |
|   | Утвержденыприказом Министраинформации и коммуникацийРеспублики Казахстанот 13 июня 2018 года № 263 |

 **Правила проведения аудита информационных систем**

 **Глава 1. Общие положения**

      1. Настоящие Правила проведения аудита информационных систем (далее – Правила) разработаны в соответствии с подпунктом 22) статьи 7 Закона Республики Казахстан от 24 ноября 2015 года "Об информатизации" (далее – Закон) и определяют порядок проведения аудита информационных систем.

      2. В настоящих правилах используются следующие понятия:

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

      2) аудит информационной системы – независимое обследование информационной системы в целях повышения эффективности ее использования;

      3) информационно-коммуникационная инфраструктура – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

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

      5) нормативно-техническая документация – совокупность документов, определяющих общие задачи, принципы и требования к созданию и использованию (эксплуатации) объектов информатизации, а также контролю их соответствия установленным требованиям в сфере информатизации.

      3. Аудит информационной системы осуществляется с целью:

      1) получения оценки текущего состояния информационной системы, действий и событий, происходящих в них, определяющих уровень их соответствия техническим регламентам, стандартам в сфере информатизации;

      2) установления соответствия нормативно-технической документации требованиям заказчика, а также требованиям информационной безопасности.

      4. Задачами аудита информационных систем являются:

      1) оценка соответствия Единым требованиям в области информационно-коммуникационных технологий и обеспечения информационной безопасности утвержденным постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832 (далее – единые требования).

      2) анализ и оценка разработки политик безопасности и других организационно-распорядительных документов по защите информационных систем;

      3) анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов информационных систем;

      4) оценка постановки задач для персонала, касающихся обеспечения защиты информации;

      5) оценка участия в разборе инцидентов, связанных с нарушением информационной безопасности;

      6) локализация уязвимых мест в системе защиты информационных систем;

      7) определение степени участия в обучении пользователей и обслуживающего персонала информационных систем вопросам обеспечения информационной безопасности;

      8) выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности информационных систем.

      9) оценка соответствия функций информационной системы его целям и задачам;

      10) оценка соответствия создания, внедрения и эксплуатации информационной системы техническим регламентам, стандартам в сфере информатизации;

      11) оценка уровня защищенности информационных систем, включая прикладное программное обеспечение и базы данных;

      12) оценка состояния информационно-коммуникационной инфраструктуры ее технического состояния и топологии;

      13) оценка соответствия нормативно-технической документации требованиям законодательства Республики Казахстан в сфере информатизации.

 **Глава 2. Порядок проведения аудита информационных систем**

      5. Аудит информационных систем проводится на этапе создания, внедрения и эксплуатации информационных систем по инициативе собственника или владельца информационных систем.

      6. Проведение аудита информационных систем осуществляется физическими (или) юридическими лицами, обладающими специальными знаниями и опытом работы в области информационно-коммуникационных технологий (далее – аудитор).

      7. Аудит информационных систем в защищенном исполнении, отнесенных к государственным секретам, не проводится.

      8. Заказчиком аудита информационных систем является собственник и (или) владелец информационной системы.

      9. Аудит информационных систем проводится в соответствии с договором между заказчиком и аудитором.

      10. Срок проведения аудита информационной системы зависит от функциональной сложности информационной системы, количества структурных компонентов (подпрограмм), условий ее эксплуатации (организация рабочих мест, доступ к серверам, наличия региональных (территориальных) центров сопровождения информационной системы), а также конкретных целей аудита информационной системы со стороны заказчика и указывается в договоре.

      11. При проведении аудита информационных систем государственных юридических лиц выбор аудитора осуществляется в соответствии с Законом Республики Казахстан от 4 декабря 2015 года "О государственных закупках".

      12. Работы по аудиту информационных систем включают в себя ряд последовательных этапов:

      инициирование процедуры аудита информационных систем;

      сбор информации аудита информационных систем;

      анализ данных аудита информационных систем;

      выработка рекомендаций;

      подготовка и подписание заключения.

      13. К видам работ по аудиту информационных систем относятся:

      проведение анализа экспертным методом;

      оценка соответствия рекомендациям стандартов по информационной безопасности и единым требованиям;

      инструментальное обследование компонентов информационных систем.

      14. В ходе проведения анализа экспертным методом выявляются недостатки в системе мер защиты информации на основе опыта экспертов, участвующих в процедуре обследования.

      15. В качестве критериев для оценки механизмов безопасности организационного уровня, включая административные, процедурные и физические меры защиты, используются стандарты СТ РК ИСО/МЭК 27002-2015 "Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления информационной безопасностью" и СТ РК ГОСТ Р 50739-2006 "Средства вычислительной техники Защита от несанкционированного доступа к информации. Общие технические требования".

      16. При инструментальном обследовании компонентов информационных систем компоненты направляются на выявление и устранение уязвимостей программно-аппаратного обеспечения системы.

      17. Оформление результатов аудита информационных систем включает:

      1) оценку соответствия стандартам СТ РК ИСО/МЭК 27002-2015 "Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления информационной безопасностью" и СТ РК ГОСТ Р 50739-2006 "Средства вычислительной техники

      Защита от несанкционированного доступа к информации

      Общие технические требования";

      2) подведение результатов инструментального обследования;

      3) выработку рекомендаций;

      4) подготовку заключения.

      18. Со дня окончания аудита информационной системы готовится аудиторское заключение (далее – заключение) в срок не более 30 календарных дней по форме согласно приложению к настоящим Правилам.

      19. Заключение составляется на казахском и русском языках в двух экземплярах, один из которых передается заказчику, второй остается у аудитора.

      20. Заключение носит рекомендательный характер.

|  |  |
| --- | --- |
|   | Приложениек Правилам проведения аудитаинформационных систем |
|   | Форма |

 **Аудиторское заключение по результатам проведения аудита**
 **информационной системы**

      \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
                         (наименование информационной системы)
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
                   (наименование организации заказчика)
в области \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
                         (область проведения аудита)
от "\_\_\_" \_\_\_\_\_\_\_\_ 20\_\_ года
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
             (фамилия, имя, отчество (при его наличии) физического лица и (или)
       наименование юридического лица, осуществляющего аудит информационных систем)
согласно договору от "\_\_\_" \_\_\_\_\_\_\_ 20\_\_ года
проведен аудит в соответствии с Правилами проведения аудита информационных систем, в ходе аудиторской проверки
было установлено, что данная информационная система имеет следующие оценочные показатели:
1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
что соответствует/не соответствует установленным требованиям и стандартам в области
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
                         (область проведения аудита)
Рекомендации по сопровождению и развитию информационной системы
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
                   (фамилия, имя, отчество (при его наличии), подпись)
"\_\_\_" \_\_\_\_\_\_\_\_\_ 20\_\_ года
Место для печати
(при ее наличии)

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