Утверждена

приказом orgname

от «\_\_\_» \_\_\_\_\_\_\_\_\_\_20\_\_г. № \_\_\_

**Инструкция по эксплуатации систем обеспечения информационной безопасности информационных системах orgname**

1. Общие положения
   1. Для автоматизации информационных процессов Оператором используется следующие информационные системы в orgname:
      * Информационная система «Бухгалтерия» с признаками информационной системы персональных данных (далее ‑ ИСПДн) и государственной информационной системы (далее - ГИС);
      * Информационная система «Отдел кадров» с признаками ИСПДн;
      * Информационная система «Автоматизированная система по организации исполнения государственного бюджета «Бюджет КС» и ее подсистемы» с признаками ГИС.
   2. В ИС «Бухгалтерия» осуществляется обработка сведений, необходимых для выполнения требований трудового законодательства Российской Федерации и законодательства о государственной гражданской службе Российской Федерации в части ведения бухгалтерского учета, исполнения условий договоров гражданско-правового характера.
   3. В ИС «Отдел кадров» осуществляется обработка сведений, необходимых для выполнения требований трудового законодательства Российской Федерации и законодательства о государственной гражданской службе Российской Федерации в части ведения кадрового учета.
   4. ИС «Автоматизированная система по организации исполнения государственного бюджета «Бюджет КС» и ее подсистемы» предназначена для планирования бюджета и ведения реестра расходных обязательств, исполнения бюджета, администрирования неналоговых доходов, ведения делопроизводства, формирования произвольной отчетности, проведения финансового контроля.
   5. Поддержку корректной и правильной эксплуатации систем обеспечения информационной безопасности гарантирует Ответственный за обеспечение безопасности защищаемой информации;
   6. Ответственный за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах orgname (далее – Ответственный) назначается приказом orgname (далее – Министерство) и отвечает за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну (далее – защищаемая информация), в процессе ее обработки в информационных системах (далее – ИС) Министерства.
   7. Ответственный должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки и обеспечения безопасности защищаемой информации.
   8. В своей деятельности Ответственный руководствуется настоящей Инструкцией.
2. Основные функции и обязанности ответственного за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственной тайну, в информационных системах

Функции Ответственного:

* 1. Ответственный изучает все стороны деятельности Министерства и вырабатывает рекомендации по обеспечению безопасности защищаемой информации при решении следующих основных вопросов:
     + проведение аналитической работы по комплексной защите и предупреждению утечки защищаемой информации;
     + подготовка решений в отношении сведений о работах, выполняемых Министерством, подлежащих защите;
     + рассмотрение проектов технических заданий, нормативных актов и указаний, договоров на выполнение работ, отчетной документации, с целью определения достаточности предусмотренных в них требований и мероприятий по комплексной защите информации, при научных исследованиях, при проведении других работ;
     + координация внедрения и эксплуатации систем защиты и безопасности информации, обрабатываемой техническими средствами;
     + проведение работ по контролю эффективности принимаемых мер по выявлению и закрытию возможных каналов утечки защищаемой информации;
     + подготовка предложений по совершенствованию действующей системы защиты информации с последующим предоставлением руководителю структурного подразделения и/или руководителю Министерства;
     + учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей защищаемой информации;
     + обеспечение соответствия проводимых работ в части обработки защищаемой информации технике безопасности, правилам и нормам охраны труда;
     + осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Министерства.

Ответственный обязан:

* 1. Регулярно осуществлять выявление (поиск), анализ и устранение уязвимостей в информационной системе. Поиск должен проводиться с помощью средства анализа защищенности XSpider.
  2. Регулярно осуществлять обновления программного обеспечения, включая программное обеспечение средств защиты информации.
  3. Проводить контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ.
  4. Проводить контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в информационных системах.
  5. Проводить контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе
  6. Осуществлять общее техническое сопровождение ИС:
     + контролировать соблюдение требований по размещению и использованию технических средств, указанных в инструкциях по эксплуатации этих средств;
     + контролировать сохранность пломб на оборудовании автоматизированных рабочих мест;
     + вести журнал учета и выдачи используемых материальных носителей информации;
     + контролировать использование съемных материальных носителей информации, в том числе запрещать использование неучтенных носителей информации;
     + проводить инструктаж сотрудников, осуществляющих обработку защищаемой информации и имеющих доступ к защищаемой информации, обрабатываемой в ИС Министерства (далее – Пользователи ИС) по правилам работы в ИС.
  7. Осуществлять настройку и сопровождение подсистемы регистрации и учета ИС:
     + реализовывать полномочия доступа (чтение, запись) для каждого Пользователя ИС к элементам защищаемых информационных ресурсов (том, каталог, файл, запись, поле записи) на основе утвержденного руководителем списка сотрудников, допущенных к работе в ИС;
     + назначать пароли Пользователей ИС;
     + контролировать плановую смену паролей Пользователями ИС для доступа в ИС;
     + своевременно удалять профиль Пользователя ИС при увольнении или переводе сотрудника;
     + вводить в базу данных системы защиты от несанкционированного доступа (далее – НСД) описания событий, подлежащих регистрации в системном журнале;
     + регулярно проводить анализ системного журнала для выявления попыток несанкционированного доступа к ИС;
     + своевременно информировать руководителя структурного подразделения о несанкционированных действиях персонала для организации расследования попыток НСД.
  8. Сопровождать подсистему обеспечения целостности рабочего программного обеспечения (ПО) ИС:
     + обеспечивать регулярное и своевременное обновление антивирусного программного обеспечения Министерства;
     + обеспечивать поддержание установленного порядка эксплуатации антивирусного программного обеспечения;
     + обеспечивать регулярное и своевременное создание резервных копий ИС Министерства;
     + осуществлять настройку и сопровождение системы защиты от НСД в ИС.
  9. Проводить периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий Пользователей ИС.
  10. Требовать прекращения обработки защищаемой информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.
  11. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и служебных расследований фактов НСД.
  12. Участвовать при проведении внутреннего контроля соответствия обработки защищаемой информации установленным требованиям.
  13. Контролировать выполнение Пользователями ИС требований Инструкции пользователя информационных систем orgname, а также установленных требований по обеспечению безопасности защищаемой информации.
  14. Контролировать правильность применения Пользователями ИС средств защиты информации.
  15. В случае получения от Пользователей ИС информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, незамедлительно принять все необходимые меры для обеспечения безопасности защищаемой информации в пределах своих полномочий.
  16. Обеспечивать функционирование и поддерживать работоспособность на автоматизированных рабочих местах ИС:
      + антивирусного программного обеспечения;
      + средств защиты от несанкционированного доступа;
      + персональных межсетевых экранов.
      + средства защиты от НСД;
      + комплексные межсетевые экраны.
  17. Обеспечивать функционирование и поддерживать работоспособность средств обнаружения вторжений, комплексных межсетевых экранов, средств анализа защищенности.
  18. В случае нарушения работоспособности технических средств и программного обеспечения ИС, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.
  19. Своевременно информировать руководителя структурного подразделения о выявленных нарушениях требований по обеспечению безопасности защищаемой информации и попытках несанкционированного доступа к ИС.