

**orgname**

**П Р И К А З**

|  |
| --- |
|  |

*от «\_\_»\_\_\_\_\_\_\_\_\_\_\_ 2015 г . № 01-04 \ \_\_\_\_\_*

**г. Якутск**

**Об ответственном за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах**

**orgname**

В целях выполнения требований Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказа Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»,

ПРИКАЗЫВАЮ:

Для обеспечения безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, назначить ответственным за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах orgname Должность Фамилия Имя Отчество.

1. Утвердить прилагаемую Инструкцию ответственного за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах orgname.

Контроль за исполнением настоящего приказа оставляю за собой.

{{Руководитель}}

Утверждена

приказом orgname

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

**Инструкция ответственного за обеспечение безопасности защищаемой информации, не содержащей сведения, составляющие государственную тайну, в информационных системах orgname**

1. Общие положения
   1. 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.
   2. Ответственный должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки и обеспечения безопасности защищаемой информации.
   3. В своей деятельности Ответственный руководствуется Политикой в отношении обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в Министерстве финансов Республики Саха (Якутия), 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. Соблюдать требования нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности защищаемой информации при ее обработке в ИС.
  2. Знать состав, структуру, назначение и выполняемые задачи ИС, а также состав информационных технологий и технических средств, позволяющих осуществлять обработку защищаемой информации.
  3. 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.
  4. 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.
  5. 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.
  6. Проводить периодическое тестирование функций системы защиты от НСД при изменении программной среды и полномочий Пользователей ИС.
  7. Требовать прекращения обработки защищаемой информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации.
  8. Участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и служебных расследований фактов НСД.
  9. Участвовать при проведении внутреннего контроля соответствия обработки защищаемой информации установленным требованиям.
  10. Контролировать выполнение Пользователями ИС требований Инструкции пользователя информационных систем orgname, а также установленных требований по обеспечению безопасности защищаемой информации.
  11. Контролировать правильность применения Пользователями ИС средств защиты информации.
  12. 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.
  13. Обеспечивать функционирование и поддерживать работоспособность на автоматизированных рабочих местах ИС:
      + антивирусного программного обеспечения;
      + средств защиты от несанкционированного доступа;
      + персональных межсетевых экранов.
  14. Обеспечивать функционирование и поддерживать работоспособность средств обнаружения вторжений, комплексных межсетевых экранов, средств анализа защищенности.
  15. 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.
  16. Своевременно информировать руководителя структурного подразделения о выявленных нарушениях требований по обеспечению безопасности защищаемой информации и попытках несанкционированного доступа к ИС.

1. Права ответственного за обеспечение безопасности защищаемой информации, не составляющей государственной тайны, в информационных системах

Ответственный имеет право:

* 1. Знакомиться с нормативными актами Министерства, регламентирующими процессы обработки защищаемой информации.
  2. Вносить предложения руководителю Министерства по совершенствованию существующей системы защиты информации.
  3. Привлекать по согласованию с руководителем структурного подразделения и руководителем Министерства к работе по созданию и совершенствованию системы защиты информации других сотрудников Министерства.
  4. Требовать от Пользователей ИС соблюдения требований Инструкции пользователя информационных систем orgname и иных нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности защищаемой информации.
  5. Участвовать в работе по совершенствованию мероприятий, обеспечивающих безопасность защищаемой информации, вносить свои предложения по совершенствованию организационных и технических мер обеспечения безопасности защищаемой информации в ИС.
  6. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности защищаемой информации.
  7. Требовать прекращения работы в ИС, как в целом, так и отдельных Пользователей ИС, в случае выявления нарушений требований по обеспечению безопасности защищаемой информации или в связи с нарушением функционирования ИС.