ПРИЛОЖЕНИЕ № 3

к приказу Министерства финансов

Калужской области

от «03» декабря 2014 г. № 197

**Инструкция пользователя**

**информационных систем персональных данных   
Министерства финансов Калужской области**

1. Общие положения
   1. Пользователем информационных систем персональных данных (далее – Пользователь) является уполномоченный сотрудник Министерства финансов Калужской области (далее – Министерство).
   2. Пользователь должен знать законодательные и иные нормативные правовые акты Российской Федерации, Калужской области методические материалы в сфере обработки персональных данных.
   3. В своей деятельности, связанной с обработкой персональных данных, Пользователь руководствуется Политикой в отношении обработки персональных данных в Министерстве финансов Калужской области и настоящей Инструкцией.
   4. Пользователи, участвующие в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющие доступ к аппаратным средствам, программному обеспечению и обрабатываемой информации, несут персональную ответственность за свои действия.
2. Обязанности и права пользователя информационных систем персональных данных
   1. Пользователь обязан:
      * соблюдать требования Политики в отношении обработки персональных данных в Министерстве финансов Калужской области и иных нормативных актов Министерства, устанавливающих порядок работы с персональными данными;
      * выполнять в информационных системах персональных данных (далее – ИСПДн) только те процедуры, которые необходимы для исполнения его должностных обязанностей;
      * использовать для выполнения должностных обязанностей только предоставленное ему автоматизированное рабочее место (далее – АРМ) на базе персонального компьютера (автономной ПЭВМ);
      * пользоваться только зарегистрированными в установленном порядке съемными (отчуждаемыми) машинными носителями информации;
      * обеспечивать безопасное хранение вышеуказанных материальных носителей информации, исключающее несанкционированный доступ к ним;
      * немедленно сообщать руководителю структурного подразделения или ответственному за обеспечение безопасности персональных данных в ИСПДн (далее – Ответственный) о нештатных ситуациях, фактах и попытках несанкционированного доступа к обрабатываемой информации, о блокировании, исчезновении (искажении) защищаемой информации;
      * перед началом обработки в ИСПДн файлов, хранящихся на съемных носителях информации, Пользователь должен осуществлять проверку файлов на наличие компьютерных вирусов. Антивирусный контроль на АРМ должен осуществляться Пользователем не реже одного раза в неделю;
      * располагать экран монитора в помещении во время работы так, чтобы исключалась возможность ознакомления с отображаемой на них информацией посторонними лицами;
      * соблюдать установленный режим разграничения доступа к информационным ресурсам: получать пароль, надежно его запоминать и хранить в тайне.
   2. Пользователям ИСПДн запрещается:
      * записывать и хранить информацию, относящуюся к конфиденциальной информации или персональным данным, на неучтенных материальных носителях информации;
      * оставлять во время работы материальные носители информации без присмотра, несанкционированно передавать материальные носители информации другим лицам и выносить их за пределы помещения, в котором производится обработка информации;
      * отключать средства антивирусной защиты;
      * отключать (блокировать) средства защиты информации;
      * производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств;
      * самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
      * обрабатывать в ИСПДн информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационным ресурсам ИСПДн;
      * сообщать (или передавать) посторонним лицам личные атрибуты доступа к ресурсам в ИСПДн;
      * работать в ИСПДн при обнаружении каких-либо неисправностей;
      * хранить на учтенных носителях информации программы и данные, не относящиеся к рабочей информации;
      * вводить в ИСПДн персональные данные под диктовку или с микрофона;
      * привлекать посторонних лиц для производства ремонта технических средств ИСПДн без согласования с Ответственным.
   3. Пользователь имеет право знакомиться с внутренними документами Министерства, регламентирующими его обязанности по занимаемой должности.
3. Организация парольной защиты при работе на объектах информатизации
   1. Пароли доступа к ИСПДн устанавливаются Ответственным или Пользователем.
   2. При формировании пароля необходимо руководствоваться следующими требованиями:
      * длина пароля должна быть не менее 8-и буквенно-цифровых символов;
      * пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации;
      * запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
      * запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);
      * при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
      * в числе символов пароля, обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;
      * запрещается использовать ранее использованные пароли.
   3. При организации парольной защиты запрещается:
      * записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;
      * хранить пароли в записанном виде на отдельных листах бумаги;
      * сообщать свои пароли посторонним лицам, а также сведения о применяемых средствах защиты от НСД.
4. Порядок применения парольной защиты
   1. Плановую смену паролей на доступ в ИСПДн рекомендуется проводить один раз в месяц.
   2. Пользователь обязан незамедлительно сообщить Ответственному факты утраты, компрометации ключевой, парольной и аутентифицирующей информации.
   3. Внеплановая смена личного пароля должна производиться в обязательном порядке в следующих случаях:
      * компрометации (подозрении на компрометацию) пароля;
      * в случае прекращения полномочий (увольнение, переход на другую работу внутри организации) Пользователя (в течение 24 часов после окончания последнего сеанса работы данного с ИСПДн);
      * по инициативе Ответственного.
5. Технология обработки персональных данных
   1. При первичном допуске к работе с ИСПДн Пользователь:
      * проходит инструктаж по использованию ИСПДн;
      * знакомится с требованиями нормативно-правовых, руководящих и организационно-распорядительных документов, регламентирующих обработку и обеспечение безопасности персональных данных;
      * получает у Ответственного идентификатор и личный пароль для входа в ИСПДн.
   2. Перед началом работы Пользователь визуально проверяет целостность пломб, убеждается в отсутствии посторонних технических средств, включает необходимые средства вычислительной техники.
   3. Авторизацию в ИСПДн (ввод личного идентификатора и пароля) Пользователь осуществляет при отсутствии в помещении посторонних лиц.
   4. В процессе работы на АРМ ИСПДн Пользователь использует технические средства и установленное Ответственным программное обеспечение согласно Техническому паспорту ИСПДн.
   5. Копирование персональных данных на электронные носители информации осуществляется только при наличии производственной необходимости и только на учтенные электронные носители информации.
   6. При необходимости создания на АРМ Пользователя дополнительных электронных документов, содержащих персональные данные, Пользователь создает и хранит такие документы в строго отведенном для этого месте.
   7. Печать документов, содержащих персональные данные, осуществляется только при наличии производственной необходимости на принтер, подключенный Ответственным к АРМ Пользователя. Все бумажные носители, не подлежащие учету по каким-либо техническим или иным причинам (сбой принтера при печати, обнаружение ошибок в документе после распечатки и т.д.) уничтожаются незамедлительно с применением уничтожителей бумаги. Распечатанные черновые бумажные варианты вновь создаваемых документов, содержащих персональные данные, уничтожаются с применением уничтожителей бумаги незамедлительно после подписания (утверждения) окончательного варианта документа.
   8. В случае возникновения необходимости временно покинуть рабочее помещение во время работы в ИСПДн, Пользователь обязан выключить компьютер, либо заблокировать его, для чего нужно нажать комбинацию клавиш <Ctrl-Alt-Del> и выбрать в диалоговом окне кнопку «Блокировать». Разблокирование компьютера производится набором пароля разблокировки, который был создан при настройке системы блокировки АРМ. При отсутствии в покидаемом помещении других служащих Министерства, Пользователь обязан закрыть дверь помещения на ключ или другой используемый ограничитель доступа.
   9. Покидая рабочее помещение в конце рабочего дня, Пользователь обязан выключить все необходимые средства вычислительной техники и закрыть дверь помещения на ключ.