МИНИСТЕРСТВО ФИНАНСОВ ПЕНЗЕНСКОЙ ОБЛАСТИ

П Р И К А З

От 28.03.2011 № 21-к

г.Пенза

О назначении ответственных лиц в Министерстве финансов Пензенской области за обработку персональных данных

В целях исполнения в требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (с последующими изменениями), руководствуясь Положением о Министерстве финансов Пензенской области, утвержденным постановлением Правительства Пензенской области от 27.10.2008 № 714-пП (с последующими изменениями), **п р и к а з ы в а ю**:

1. Утвердить:

1.1. Список лиц в Министерстве финансов Пензенской области, ответственных за обработку персональных данных, подлежащих защите (приложение 1).

1.2. Инструкцию пользователя информационной системы персональных данных Министерства финансов Пензенской области (приложение 2).

1.3. Форму журнала учета обращений субъектов персональных данных о выполнении их законных прав, при обработке персональных данных в информационной системе персональных данных подразделения Министерства финансов Пензенской области (далее – журнал учета) (приложение 3).

2. Руководителям структурных подразделений Министерства финансов Пензенской области:

2.1. Регистрировать обращения в журнале учета.

2.2. Ознакомить Инструкцией пользователя информационной системы персональных данных Министерства финансов Пензенской области лиц, ответственных за обработку персональных данных, подлежащих защите.

2.3. Внести дополнения в должностные регламенты государственных гражданских служащих ответственных за обработку персональных данных, подлежащих защите.

3. Контроль за исполнением настоящего приказа возложить на начальника управления исполнения бюджета и обеспечения деятельности Министерства финансов Пензенской области С.Д. Оборина.

Министр Е.И. Крашенинникова

Приложение 1

УТВЕРЖДЕН
приказом Министерства
финансов Пензенской области
от 28.03.2011 № 21-к

СПИСОК
лиц в Министерстве финансов Пензенской области, ответственных за обработку персональных данных, подлежащих защите

№ пп	Должность	Фамилия и инициалы
1	2	3
Отдел кадров		
1	Начальник отдела	Димаев А.М.
2	Заместитель начальника отдела	Немков Р.А.
3	Главный специалист - эксперт	Абрамова С.В.
4	Главный специалист – эксперт по мобилизационной подготовке	Душин Е.Г.
Отдел учета и отчетности		
5	Начальник отдела – главный бухгалтер	Шашанова Л.В.
6	Заместитель начальника отдела – заместитель главного бухгалтера	Шаронова Л.П.
7	Заместитель начальника отдела – заместитель главного бухгалтера	Шатова С.В.
8	Главный специалист-эксперт	Трушкова Л.В.
9	Главный специалист-эксперт	Беликова Н.А.
10	Главный специалист-эксперт	Носырева О.Г.
11	Главный специалист-эксперт	Курышова Н.А.
12	Главный специалист-эксперт	Каменева С.Н.
Отдел информационно-технического обеспечения		
13	Начальник отдела	Карпов А.Н.
14	Заместитель начальника отдела	Майоров В.Н.
15	Заместитель начальника отдела	Анохин Е.А.
16	Главный специалист-эксперт	Шичев В.А.
17	Главный специалист-эксперт	Толкачева М.В.
18	Главный специалист-эксперт	Череп Г.В.
19	Ведущий специалист-эксперт	Балякина К.А.
Отдел делопроизводства и хозяйственного обеспечения		
20	Заместитель начальника отдела	Королева Г.В.
21	Старший специалист 3 разряда	Кузнецова Т.А.
22	Специалист 1 разряда	Леонова Е.Г.

Приложение 2

УТВЕРЖДЕНА
приказом Министерства
финансов Пензенской области
от 28.03.2011 № 21-к

ИНСТРУКЦИЯ
пользователя информационной системы персональных данных Министерства финансов Пензенской области

1. Общие положения

1.1. Настоящая Инструкция разработана для обеспечения защиты персональных данных в Министерстве финансов Пензенской области.

1.2. Персональные данные (далее – ПДн) относятся к категории информации ограниченного распространения.

1.3. Наиболее вероятными каналами утечки информации для информационных систем персональных данных (далее – ИСПДн) являются:

- несанкционированный доступ к информации, обрабатываемой в ИСПДн;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;
- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

1.4 Работа с персональными данными строится на следующих принципах:

- принцип персональной ответственности – в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник, выдача документов осуществляется только под роспись;
- принцип контроля и учета – все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

2. Обязанности работников, имеющих доступ к ПДн.

2.1. Работники, получившие доступ к персональным данным, обязаны хранить в тайне сведения ограниченного распространения, ставшие им известными во время работы или иным путем и пресекать действия других лиц, которые могут привести к разглашению такой информации. О таких фактах, а также о других причинах или условиях возможной утечки персональных

данных немедленно информировать руководителя структурного подразделения, специалиста по защите информации.

2.2. Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает работника от взятых им обязательств по неразглашению сведений ограниченного распространения.

2.3. В случае освобождения от занимаемой должности работник обязан вернуть все документы и материалы, относящиеся к деятельности подразделения, организации. В том числе: отчеты, инструкции, переписку, списки работников, компьютерные программы, а также все прочие материалы и копии названных материалов, имеющих какое-либо отношение к деятельности Правительства области, полученные в течение срока работы.

2.4. Работники при работе с персональными данными обязаны:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- выполнять требования специалиста по защите информации;
- знать и строго выполнять правила работы со средствами защиты информации (средствами разграничения доступа), используемыми на персональных компьютерах;
- хранить в тайне свой аудентификатор (пароль доступа в автоматизированную систему, либо ключевой носитель), а также информацию о системе защиты, установленной в ИСПДн;
- использовать для работы только учтенные съемные накопители информации (гибкие магнитные диски, компакт диски и т.д.);
- контролировать обновление антивирусных баз и в случае необходимости сообщать о необходимости обновления администратору безопасности, ответственному за антивирусную защиту автоматизированной системы;

2.5. Немедленно ставить в известность руководителя подразделения, администратора безопасности ИСПДн:

- в случае утери носителя с персональными данными или при подозрении компрометации личных ключей и паролей;
- нарушений целостности пломб (наклеек с защитной и идентификационной информацией, нарушении или несоответствии номеров печатей) на аппаратных средствах ПЭВМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее - НСД) к защищенной ИСПДн;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн.
- в случае отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию рабочей станции, выхода из строя или неустойчивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения, некорректного функционирования установленных в автоматизированной системе технических средств защиты ставить в известность ответственного за техническое обслуживание и (или) ответственного за обслуживание программного обеспечения.

2.6. Ставить в известность администратора безопасности ИСПДн при:

- необходимости обновления антивирусных баз;
- обновлении программного обеспечения;
- проведении регламентных работ, модернизации аппаратных средств или изменении конфигурации ИСПДн;
- необходимости вскрытия системных блоков персональных компьютеров входящих в состав ИСПДн;
- резервном копировании информации;
- и в других случаях, связанных с обработкой и защитой персональных данных.

2.7. Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

2.8. Вынос ПЭВМ, на которых проводилась обработка персональных данных, за пределы территории здания с целью их ремонта, замены и т. п. без согласования с руководителем подразделения запрещен. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному лицу за учет служебных документов ограниченного распространения структурного подразделения.

2.9. ПЭВМ, используемые для работы с персональными данными, должны быть размещены таким образом, чтобы исключалась возможность визуального просмотра экрана видеомонитора работниками, не имеющими отношения к конкретно обрабатываемой информации.

Запрещается:

- передавать, кому бы то ни было (в том числе родственникам) устно или письменно сведения о персональных данных субъектов;
- использовать персональные данные, не являющиеся общедоступными, при подготовке открытых публикаций, докладов, научных работ и т.д.;
- обрабатывать персональные данные, не являющиеся общедоступными, на дому, выносить их из служебных помещений, снимать копии или производить выписки из таких документов без разрешения руководителя;
- накапливать ненужные для работы персональные данные;
- передавать или принимать без расписки материальные носители с персональными данными, не являющимися общедоступными;
- оставлять на рабочих столах, в столах и незакрытых сейфах материальные носители с персональными данными, не являющимися общедоступными, а также оставлять после окончания работы незапертыми и неопечатанными сейфы, помещения и хранилища с документами конфиденциального характера.
- использовать компоненты программного и аппаратного обеспечения ИСПДн подразделения в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить персональные данные на неучтенных носителях информации (гибких магнитных дисках и т.п.);

- оставлять включенной без присмотра свою рабочую станцию (ПЭВМ), не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок – ставить в известность руководителя своего подразделения, ответственного за техническое и (или) программное обеспечение, администратора безопасности.

3. Ответственность

3.1. Пользователь несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации.

3.2. За разглашение информации ограниченного распространения, нарушение порядка работы с документами или машинными носителями, содержащими такую информацию, работники привлекаются к дисциплинарной или иной, предусмотренной законодательством, ответственности.

_____

Приложение № 3

УТВЕРЖДЕН
приказом Министерства
финансов Пензенской области
от 28.03.2011 № 21-к

ЖУРНАЛ
учета обращений субъектов персональных данных о выполнении их законных прав при обработке персональных данных в информационной системе персональных данных подразделения Министерства финансов Пензенской области

Начат «____» _____2011г.
Окончен «____» _____20__г.

№ п/п	ФИО субъекта	Дата обращения	Цель	Отметка об исполнении	ФИО исполнителя	Роспись