МИНИСТЕРСТВО ФИНАНСОВ УДМУРТСКОЙ РЕСПУБЛИКИ

ПРИКАЗ

От 23 августа 2012г № 102

г. Ижевск

О мерах по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Министерства финансов Удмуртской Республики

В целях обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных Министерства финансов Удмуртской Республики и в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»:

1. Утвердить Положение о разграничении прав доступа к обрабатываемым персональным данным в информационных системах персональных данных Министерства финансов Удмуртской Республики (Приложение 1).

2. Утвердить Инструкцию Администратора (Администратора безопасности) информационных систем персональных данных Министерства финансов Удмуртской Республики (Приложение 2).

3. Утвердить Инструкцию Пользователя информационных систем персональных данных Министерства финансов Удмуртской Республики (Приложение 3).

4. Управлению административно-кадровой работы ознакомить с настоящим приказом под роспись гражданских служащих (работников), замещающих должности, указанные в приложениях к настоящему приказу, а также внести соответствующие изменения в их должностные регламенты (должностные инструкции).

5. Контроль за исполнением настоящего Приказа оставляю за собой.

Заместитель Председателя Правительства
Удмуртской Республики –
министр финансов Удмуртской Республики В.В.Богатырев

Приложение 1
к приказу Министерства финансов
Удмуртской Республики
от 23 августа 2012 года № 102

Положение
о разграничении прав доступа
к обрабатываемым персональным данным в информационных системах
персональных данных Министерства финансов Удмуртской Республики

1. Настоящим Положением устанавливается порядок разграничения прав доступа к обрабатываемым персональным данным (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн).

2. Разграничение прав доступа осуществляется на основании результатов проведения внутренней проверки, а также исходя из характера и режима обработки персональных данных в ИСПДн.

3. В настоящем положении утверждаются Перечни групп и лиц, участвующих в обработке персональных данных в ИСПДн, а также уровень прав их доступа для каждой ИСПДн (Приложения 1-3).

4. Настоящее положение утверждается приказом Министерства и является обязательным для исполнения гражданскими служащими (работниками) Министерства, имеющими доступ и участвующими в обработке ПДн.

Приложение 2
к приказу Министерства финансов
Удмуртской Республики
от 23 августа 2012 года № 102

Инструкция Администратора (Администратора безопасности) информационных систем персональных данных Министерства финансов Удмуртской Республики

1. Общие положения

1.1. Администратор (Администратор безопасности) информационных систем персональных данных (далее – Администратор) действует на основании Положения «О разграничении прав доступа к обрабатываемым персональным данным» и осуществляет настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн (систем защиты ПДн). Обладает полномочиями предоставления и разграничения доступа Пользователей ИСПДн к элементам ИСПДн, хранящим ПДн.

1.2. Администратор в своей работе руководствуется настоящей инструкцией, Положением «О работе с персональными данными в Министерстве финансов Удмуртской Республики», документами ФСТЭК России.

2. Должностные обязанности

Администратор обязан:

2.1. Знать и выполнять требования нормативных и руководящих документов, а также инструкций, регламентирующих порядок действий по защите информации.

2.2. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (в том числе операционные системы, прикладное и специальное ПО);
- аппаратных средств;
- аппаратных и программных средств защиты.

2.3. Обеспечивать работоспособность элементов ИСПДн и локальной вычислительной сети.

2.4. Осуществлять контроль учета, создания, хранения и использования резервных и архивных копий массивов данных, машинных (выходных) документов.

2.5. Обеспечивать функционирование и поддерживать работоспособность средств защиты в рамках возложенных на него функций.

2.6. В случае отказа работоспособности технических средств и программного обеспечения элементов ИСПДн, в том числе средств защиты

информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.7. Проводить периодический контроль принятых мер по защите в пределах возложенных на него функций.

2.8. Хранить, осуществлять прием и выдачу персональных паролей пользователей, осуществлять контроль за правильностью использования персонального пароля пользователями ИСПДн.

2.9. Обеспечивать постоянный контроль выполнения пользователями установленного комплекса мероприятий по обеспечению безопасности информации.

2.10. Информировать ответственных руководителей о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к ресурсам ИСПДн.

2.11. Требовать прекращения обработки информации, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты.

2.12. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств и отправке их в ремонт. Техническое обслуживание и ремонт средств вычислительной техники, предназначенных для обработки персональных данных, проводятся организациями, имеющими соответствующие лицензии. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения информации. Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

2.13. Присутствовать при выполнении технического обслуживания элементов ИСПДн третьими лицами (организациями и индивидуальными предпринимателями).

2.14. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий.

Приложение 3
к приказу Министерства финансов
Удмуртской Республики
от 23 августа 2012 года № 102

Инструкция Пользователя информационных систем персональных данных Министерства финансов Удмуртской Республики

1. Общие положения

1.1. Пользователь информационных системы персональных данных (далее – Пользователь) осуществляет обработку персональных данных (далее – ПДн) в информационных системах персональных данных, утвержденных приказом Министерства финансов Удмуртской Республики (далее – ИСПДн).

1.2. Пользователем является гражданский служащий (работник), имеющий доступ к аппаратным средствам, программному обеспечению и средствам защиты и участвующий в рамках своих должностных обязанностей в процессах автоматизированной обработки информации, включая:

- возможность просмотра ПДн;
- ручной ввод ПДн в ИСПДн;
- формирование справок, отчетов и иных документов по информации, полученной из ИСПДн.

Пользователь не имеет полномочий для управления подсистемами обработки ПДн и системами защиты ПДн.

1.3. Пользователь несет персональную ответственность за свои действия.

1.4. Пользователь в своей работе руководствуется настоящей инструкцией, Положением «О работе с персональными данными в Министерстве финансов Удмуртской Республики», документами ФСТЭК России.

2. Должностные обязанности

Пользователь обязан:

2.1. Знать и выполнять требования нормативных и руководящих документов, а также инструкций, регламентирующих порядок действий по защите информации.

2.2. Выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него должностными обязанностями.

2.3. Знать и соблюдать установленные требования по режиму обработки персональных данных, учету, хранению и пересылке носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

2.4. Соблюдать требования парольной политики (раздел 3 настоящей инструкции).

2.5. Соблюдать правила при работе в сетях общего доступа и (или) информационно - телекоммуникационной сети Интернет и других (раздел 4 настоящей инструкции).

2.6. Экран монитора в помещении располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

2.7. Обо всех выявленных нарушениях, связанных с информационной безопасностью Министерства финансов Удмуртской Республики, а так же для получений консультаций по вопросам информационной безопасности, необходимо обратиться к ответственному за техническое обеспечение безопасности информации в ИСПДн.

2.8. Для получения консультаций по вопросам работы и настройке элементов ИСПДн необходимо обращаться к Администратору ИСПДн.

2.9. Пользователям запрещается:

- разглашать защищаемую информацию третьим лицам;
- копировать защищаемую информацию на внешние носители без разрешения непосредственного руководителя;
- самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;
- несанкционированно открывать общий доступ к папкам на своей рабочей станции;
- запрещено подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;
- отключать (блокировать) средства защиты информации;
- обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к ИСПДн;
- сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам ИСПДн;
- произносить вслух обрабатываемые персональные данные;
- привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за техническое обеспечение безопасности информации в ИСПДн.

2.10. При отсутствии визуального контроля за рабочей станцией: доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировать компьютер>.

2.11. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него обязанностей.

3. Организация парольной защиты

3.1 Личные пароли доступа к элементам ИСПДн выдаются пользователям Администратором ИСПДн или создаются самостоятельно.

3.2. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в 3 месяца.

3.3. Правила формирования пароля:

- пароль не может содержать имя учетной записи пользователя или какую-либо его часть;
- пароль должен состоять не менее чем из 8 символов;
- в пароле должны присутствовать символы трех категорий из числа следующих четырех:
  - прописные буквы английского алфавита от A до Z;
  - строчные буквы английского алфавита от a до z;
  - десятичные цифры (от 0 до 9);
  - символы, не принадлежащие алфавитно-цифровому набору (например, !, $, #, %).
- запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;
- 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.);
- запрещается выбирать пароли, которые уже использовались ранее.

3.4. Правила ввода пароля:

- ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;
- во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

3.5. Правила хранения пароля:

- запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и других носителях информации, в том числе на предметах;

- запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

3.6. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию.
- своевременно сообщать Администратору ИСПДн об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

4. Правила работы в сетях общего доступа и (или) международного обмена

4.1. Работа в сетях общего доступа и (или) международного обмена (информационно – телекоммуникационной сети Интернет и других) (далее – Сеть) на элементах ИСПДн, должна проводиться при служебной необходимости.

4.2. При работе в Сети запрещается:

- осуществлять работу при отключенных средствах защиты (антивирус и других);
- передавать по Сети защищаемую информацию без использования средств шифрования;
- запрещается скачивать из Сети программное обеспечение и другие файлы;
- запрещается посещение сайтов сомнительной репутации (порно-сайты, сайты, содержащие нелегально распространяемое ПО и другие);
- запрещается нецелевое использование подключения к Сети.