МИНИСТЕРСТВО ТРУДА И СОЦИАЛЬНОЙ ЗАЩИТЫ ТУЛЬСКОЙ ОБЛАСТИ

П Р И К А З

«12» мая 2014г. № 141-осн

Об утверждении регламента доступа к информационным ресурсам в автоматизированной системе «Адресная социальная помощь» министерства труда и социальной защиты Тульской области

В целях исполнения требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 23 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» п р и к а з ы в а ю:

1. Утвердить регламент доступа к информационным ресурсам в автоматизированной системе «Адресная социальная помощь» министерства труда и социальной защиты Тульской области (Приложение 1);

2. Контроль за исполнением настоящего приказа возложить на заместителя министра - директора департамента демографической политики, социальной защиты, опеки и попечительства министерства труда и социальной защиты Тульской области Осипова А. А.

Министр труда и социальной защиты Тульской области **Н.В. Николаева**

Приложение № 1

к приказу министерства труда

и социальной защиты Тульской области

от «12» мая 2014 г. № 141-осн

Регламент

доступа к информационным ресурсам в автоматизированной системе «Адресная социальная помощь» министерства труда и социальной защиты Тульской области

1. Общие положения

1.1. Настоящий регламент определяет правила и порядок выполнения процедур по предоставлению и прекращению доступа к информационным ресурсам в автоматизированной системе «Адресная социальная помощь» для сотрудников министерства труда и социальной защиты Тульской области. В регламенте определяется порядок разграничения прав пользователей на выполнение различных операций в автоматизированной системе «Адресная социальная помощь» (создание, просмотр, редактирование и удаление) и ограничения доступа пользователей к информационным ресурсам системы в министерстве труда и социальной защиты Тульской области. Регламент рассматривает и определяет организационно-техническое обеспечение процессов идентификации и аутентификации пользователей, защищаемых информационных ресурсов в автоматизированной системе «Адресная социальная помощь» министерства труда и социальной защиты Тульской области (далее АС «АСП»); определяет перечень защищаемых информационных ресурсов: порядок авторизации пользователей; состав парольной документации и порядок работы с ней, в том числе генерации, смены и прекращения действия паролей (удаления учетных записей пользователей); меры обеспечения безопасности при использовании паролей в АС «АСП» ТО.

1.2. Положение разработано в соответствии с требованиями следующих документов:

- Статьи 19 Главы 4 «Меры по обеспечению безопасности персональных данных при их обработке» Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

- Пункта 5.1.3 «Специальных требований и рекомендаций по технической защите конфиденциальной информации» (СТР-К), утверждённых приказом Гостехкомиссии России от 30.08.2002 г.;
- Подпунктов 8.1, 8.2 «Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденного приказом ФСТЭК России от 18.02.2013 №21;
- Подпунктов 20.1, 20.2 «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утверждённых приказом ФСТЭК России от 11.02.2013 г. №17.

1.3. Исполнение требований настоящего Положения является элементом производственной дисциплины и обязательно для всех должностных лиц в части, их касающейся.

2. Термины и определения

Аутентичность – свойство информации (данных), выражающееся в наличии свидетельства того, что она была создана, размещена законным участником информационного процесса, и что она не подверглась искажению – случайному или преднамеренному.

Авторизация – предоставление пользователю доступа к защищаемому ресурсу в соответствии с уровнем полномочий пользователя.

Аутентификатор – 1) отличительный, никому более не присущий признак субъекта доступа (пользователя); 2) техническое устройство индивидуального использования, служащее для хранения и ввода в ПК отличительного признака субъекта доступа.

Аутентификация – процесс проверки принадлежности субъекту доступа предъявленного им идентификатора; т.е. проверка подлинности пользователя с помощью предъявляемого им аутентификатора.

Администратор приложения – лицо, ответственное за выполнение мероприятий по парольной защите приложения (приложений).

Безопасность информации – состояние информации, характеризуемое способностью персонала, используемых технических средств и информационных технологий обеспечить ее доступность, конфиденциальность, целостность и аутентичность при обработке техническими средствами.

Защита информации – деятельность по обеспечению безопасности информации.

Идентификатор – уникальный признак субъекта или объекта доступа.

Имя_Пользователя – идентификатор, представляющий последовательность символов установленного формата.

Конфиденциальность информации – 1) обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя; 2) состояние защищенности информации, характеризуемое способностью сохранения её (информации) в тайне от субъектов доступа, не имеющих полномочий на ознакомление с ней.

Пароль – назначаемый (присваиваемый) аутентификатор пользователя, представляющий собой группу символов определенной длины, являющийся секретом пользователя и служащий для подтверждения принадлежности предъявленного идентификатора (Имени_Пользователя) обращающемуся пользователю.

Парольная документация – документы, предназначенные для обеспечения функционирования системы аутентификации пользователей.

Пользователь (информации) – субъект доступа, обращающийся к информационной системе в целях получения информации или воздействия на нее.

Привилегированная учетная запись – учетная запись, используемая для управления работой АС «АСП» ТО.

Служебная учетная запись – учетная запись, используемая службами либо техническим персоналом АС «АСП» ТО для доступа к ресурсам, необходимым для выполнения их функций. Локальные учетные записи компьютеров Administrator и Guest предназначены для служебного использования при настройке систем и не предназначены для повседневной работы.

Субъект доступа – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Объект доступа – информационный ресурс автоматизированной системы, доступ к которому регламентирован.

Уровень полномочий – совокупность прав доступа субъекта доступа.

3. Порядок организация учета ресурсов в АС «АСП»

3.1 Защищаемые ресурсы АС «АСП», обрабатываемые в министерстве труда и социальной защиты Тульской области (далее Министерство), определяются «Перечнем защищаемых информационных ресурсов в АС «АСП»» (далее Перечень) (Приложение 1).

3.2 Перечень утверждается министром труда и социальной защиты Тульской области.

3.3 Актуализация перечня защищаемых информационных ресурсов осуществляется по мере изменения состава информационных ресурсов АС «АСП».

3.4 Доступ к защищаемому ресурсу АС «АСП» предоставляется минимально необходимому для выполнения производственных задач числу сотрудников, определяемому Таблицей допуска к защищаемому информационному ресурсу (далее Таблица допуска) (Приложение 2). Таблица допуска определяет разрешённые режимы работы пользователей и уровни доступа.

3.5 Ведение Таблицы допуска осуществляется администратором приложения (далее АП), контролируется ответственным за организацию обработки персональных данных, который назначается приказом министра.

3.6 АП назначается приказом руководителя ГАУ ТО «ЦИТ» или руководителя Министерства в зависимости от того, к какой организации (ГАУ ТО «ЦИТ», Министерству) относится АП.

3.7 Приказ о назначении АП издается в ГАУ ТО «ЦИТ» или в Министерстве при назначении нового АП, и переиздается не реже одного раза в год.

3.8 Для АС «АСП», не имеющей возможности обеспечить назначение пароля доступа к ресурсу непосредственно пользователем, АП на основании Таблицы допуска формирует Таблицу доступа пользователей к защищаемым ресурсам (далее Таблица доступа) (Приложение 3). Таблица доступа содержит идентификаторы и аутентификаторы (пароли) пользователей.

3.9 Таблица доступа утверждается руководителем министерства труда и социальной защиты Тульской области. Утвержденная министром таблица доступа хранится у АП в сейфе (запирающемся на замок ящике рабочего стола).

4. Предоставление доступа пользователям

4.1 Заявка на предоставление доступа пользователю к защищаемым ресурсам АС «АСП» (Приложение 4) оформляется за подписью руководителя подразделения пользователя и направляется в отдел технической поддержки ГАУ ТО «ЦИТ»

(руководителю подразделения, в котором состоит АП в случае, когда АП не является сотрудником ГАУ ТО «ЦИТ»).

4.2 Пользователям предоставляются минимально необходимые для выполнения производственных задач права доступа к информации. Ответственность за обоснованность предоставляемых пользователям прав возлагается на руководителей отделов департамента демографической политики, социальной защиты, опеки и попечительства Министерства.

4.3 Методическая помощь по уточнению прав разграничения доступа для конкретного пользователя осуществляется отделом технической поддержки ГАУ ТО «ЦИТ» и администратором безопасности Министерства.

5. Порядок разграничения прав пользователей и ограничения доступа пользователей к задачам в АС «АСП».

5.1 Задача «Настройка системы» в АС «АСП» предназначена для разграничения прав пользователей на выполнение различных операций над данными (создание, просмотр, редактирование и удаление) и ограничения доступа пользователей к задачам системы. Для этого в АС «АСП» существуют понятия рабочего места и вида работы, которые настраиваются АП.

5.2 Рабочие места служат для объединения различных задач системы в группы. Для каждого пользователя определяется список доступных рабочих мест и в рамках каждого рабочего места для конкретного пользователя определяются доступные для него виды работ (разрешение на операции создания, просмотра, редактирования и удаления определенных данных). Задача АП в АС «АСП» назначить нужные для работы пользователей права, согласно заявкам на предоставление доступа пользователю к защищаемым ресурсам АС «АСП».

6. Принципы авторизации пользователей

6.1. Авторизация пользователей производится на основании положительных результатов аутентификации. Авторизация не идентифицированных пользователей не допускается.

6.2. Идентификация пользователя в автоматизированной системе «Адресная социальная помощь» защищаемых информационных ресурсов производится присвоением пользователю идентификатора (имя пользователя для входа в систему) – уникальной символьной последовательности, которая состоит из кодификатора отделения и ФИО пользователя. Например, служащему Министерства Иванову Петру Сергеевичу

присваивается логин 210IvanovPS, сотруднику управления социальной защиты населения Дубенского района Боброву Денису Олеговичу присваивается логин 07UBobrovDO. Кодификатор Министерства и подведомственных ему учреждений, а также муниципальных и городских округов Тульской области приведен в (Приложении 5).

6.3. Набор допустимых для идентификации символов – цифры и латинские буквы в верхнем и нижнем регистрах.

6.4. Аутентификация пользователя производится посредством сравнения предъявляемого им аутентификатора с аутентификатором, поставленным в однозначное соответствие предъявленному идентификатору (Имени_Пользователя) из таблицы пользователей в АС «АСП».

6.5. В АС «АСП» используется однофакторная аутентификация пользователей.

6.6. В качестве аутентификатора пользователя в АС «АСП» используется пароль - кодовое слово, которое вводится в ПК с клавиатуры. Аутентификация пользователя в АС «АСП» ТО выполняется при:

- входе в систему;
- обращении к ресурсам.

7. Общие требования к паролям

7.1. Личные пароли пользователей АС «АСП» ТО должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и (или) специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, user, password, 123456 и т.п.);
- при смене пароля новый пароль должен отличаться от старого не менее чем двумя символами;
- при создании паролей личных учетных записей пользователей возможно использование специализированного программного обеспечения для генерации сложных для подбора легко запоминаемых паролей с учетом п. 12 настоящего Положения.

7.2. Пароли служебных и привилегированных учетных записей автоматизированной системы должны выбираться с учетом следующих требований:

- длина пароля должна быть не менее 12 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и (или) специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования рабочих станций и т.д.), а также общепринятые сокращения и термины (qwerty, user, password и т.п.), пароль не должен быть словом русского либо английского языка, в котором заменены некоторые символы (o->0, s->$, a->@ и т.п.);
- при смене пароля новый пароль должен отличаться от старого не менее чем четырьмя символами, расположенными не подряд;
- при создании паролей служебных учетных записей возможно использование специализированного программного обеспечения для генерации сложных для подбора легко запоминаемых паролей с учетом п. 12 настоящего Положения.

7.3. Срок действия паролей, вводимых с клавиатуры, составляет 180 суток, по истечении которых пароль должен быть сменен.

8. Назначение паролей

8.1. Назначение паролей для доступа к защищаемым информационным ресурсам производится АП, в соответствии с правилами и сроками, установленными п.7 данного Положения.

8.2 Порядок действий пользователей при смене паролей доступа к ресурсу, определяется АП и администратор безопасности (далее АБ).

8.3 Выработка паролей для АС «АСП» ТО, не имеющей возможности обеспечить назначение пароля доступа к данному ресурсу непосредственно пользователем, осуществляется с использованием средств вычислительной техники и специального программного обеспечения.

8.4 Доведение до пользователей паролей, выработанных АП и предназначенных для ввода с клавиатуры, осуществляется:

- посредством выдачи пользователю Карточки паролей (приложение 6)
- под роспись с отметкой в Журнале выдачи парольной документации (приложение 7).

9. Парольная документация

9.1. АП АС «АСП» на основании Таблиц допуска формирует пакет парольной документации, в который входят следующие документы:

- комплект Таблиц доступа с указанием срока их действия;
- комплект Карточек паролей;

9.2. Таблица доступа формируется отдельно для каждого ресурса. Допускается сведение таблиц доступа к нескольким ресурсам в одну при условии установки указанных в них паролей одним АП.

9.3. В Таблице доступа указываются только пароли, предназначенные для замены паролей с истекающим сроком действия.

9.4. На основании Таблицы допуска в соответствии с предоставленными полномочиями АП АС «АСП» осуществляет настройку соответствующей системы разграничения доступа к ресурсу (с использованием специализированных или встроенных средств защиты).

9.5. Для обеспечения возможности оперативной смены пароля в случае его компрометации, а также в случае кадровых перестановок пользователей, в Таблице доступа для каждого из защищаемых ресурсов АС «АСП» указывается несколько резервных паролей без привязки их к конкретному пользователю. Количество резервных паролей определяется исходя из реальных потребностей.

10. Смена аутентификаторов при кадровых изменениях

10.1. В случае прекращения действия служебного контракта (трудового договора) с государственным гражданским служащим (работником), а при необходимости и при кадровых перестановках, руководители отделов департамента демографической политики, социальной защиты, опеки и попечительства Министерства обязаны предоставить АП письменную заявку на внесение изменения в таблицу допуска пользователей к защищаемым ресурсам не позднее, чем за 3 календарных дня до предполагаемой даты увольнения (кадровой перестановки).

10.2. Карточки паролей увольняемых, а также перемещаемых в связи с изменением должностных обязанностей пользователей, подлежат возвращению АП.

10.3. Аутентификатор учетной записи уволенных пользователей меняется не позднее, чем в день увольнения, с изменением в парольной карточке уволенного пользователя. АП несет персональную ответственность за своевременную смену

идентификатора учетной записи уволенного сотрудника, а также за хранение парольных карточек уволенных сотрудников.

10.4. Факт внесения изменений в настройку системы аутентификации фиксируется АП на заявке с указанием даты и времени внесения изменений и заверяется его подписью.

10.5. Заявка на внесение изменений в Таблицу допуска хранится у АП и подлежит уничтожению не ранее уничтожения соответствующей таблицы.

10.6. После окончания срока действия паролей комплект парольной документации подлежит уничтожению. Уничтожение парольной документации производится комиссией в составе 3-х человек, назначаемой руководителем соответствующего учреждения, и оформляется актом.

10.7. Уничтожение карточек паролей пользователей производится в 10-дневный срок с момента вывода паролей из действия. Отметка об уничтожении карточек паролей пользователей производится на обратной стороне Таблицы доступа. Уничтожение Таблиц доступа пользователей с паролями, выведенными из действия, производится в конце календарного года.

10.8. При увольнении или кадровом перемещении АП, ответственного за выработку и установку паролей или хранение парольной документации, замене подлежат все установленные им пароли и доступная ему парольная документация.

11. Действия при компрометации аутентификатора или парольной документации

11.1. Под компрометацией аутентификатора понимается: утрата Карточки паролей, разглашение пароля, утрата Таблиц доступа пользователей (явная компрометация) или иная ситуация, которая дает основание для предположения о нарушении секретности пароля (неявная компрометация).

11.2. При выявлении факта компрометации аутентификатора пользователь незамедлительно обязан сообщить о факте выявления непосредственному руководителю. Руководитель сообщает о факте компрометации АП.

11.3. В случае выявления факта компрометации аутентификатора пользователя АП обязан немедленно заблокировать учетную запись пользователя, аутентификатор которого скомпрометирован.

11.4. Расследование факта компрометации проводится комиссией, назначаемой приказом руководителя Министерства.

11.5. Результаты работы комиссии оформляются актом. Акт подлежит утверждению руководителем Министерства.

11.6. Акты на уничтожение выведенных из действия парольных документов, материалы расследования фактов компрометации хранятся не менее 2-х лет.

11.7. Выдача пользователю нового аутентификатора производится по решению руководителя Министерства.

11.8. При компрометации парольной документации (всей или части) АП обязан немедленно принять меры по замене всех паролей системы на резервные, доложить о факте компрометации паролей в отдел информационной безопасности комитета Тульской области по информатизации и связи.

Приложение 1

ФОРМА

УТВЕРЖДАЮ
Министр труда и социальной защиты
Тульской области
_____ Николаева Н.В.
(подпись) (Ф.И.О.)

«__» _____201_ г.

Перечень защищаемых ресурсов в автоматизированной системе "Адресная социальная помощь" министерства труда и социальной защиты Тульской области.

№ п/п	Полное наименование защищаемого ресурса	Орган исполнительной власти – владелец защищаемого ресурса	Идентификатор ресурса (краткое наименование ресурса)	Название основной операционной системы	IP адрес ЭВМ, на которой размещен ресурс	СУБД с указанием версии (при наличии)	Путь к ресурсу (при наличии)	Адрес размещения ресурса, № помещения
1	2	3	4	5	6	7	8	9
1								
2								
3								

Директор ГАУ ТО «ЦИТ» _____ _____
(должность) (подпись) (фамилия, инициалы)

Приложение 2

ФОРМА

УТВЕРЖДАЮ

_____
(наименование должности руководителя)

_____ _____
(подпись) (Ф.И.О.)

«__» _____201__ г.

Таблица допуска пользователей _____
(наименование ОИВ, подведомственного учреждения)

к защищаемым ресурсам правительства Тульской области

_____
(наименование ресурса (базы данных, сервиса, др.))

№ п/п	Должность	Фамилия и инициалы	Идентификатор пользователя	Уровень доступа к данным	Режим функционирования АРМ и уровень доступа к нему			
					Наименование режима	Наименование режима	Наименование режима	Наименование режима
1	2	3	4	4	5.1	5.2	5....	5.N
1	*Главный специалист отдела ...*	Иванов И.И.	Идентификатор1	Все данные	Просмотр	Просмотр		Просмотр
2	*Ведущий специалист отдела....*	Петрова П.П.	Идентификатор2	Данные пользователя	*Запрещен*	*Просмотр*		*Запрещен*

Примечание: 1. В графе 4 указываются уровни, обеспечиваемые системой разграничения доступа к конкретному ресурсу.

2. В заголовке графы 5 указываются все возможные режимы АРМ.

3. В подграфах графы 5 указываются разрешенные уровни доступа к режимам АРМ работы с базой.

4. Количество подграф графы 5 определяется числом реализуемых в системе режимов.

Приложение 3

ФОРМА

УТВЕРЖДАЮ

_____
(наименование должности руководителя)

_____ _____
(подпись) (Ф.И.О.)

«__» _____201__ г.

Таблица доступа пользователей к _____
(наименование информационного ресурса)

на период с ___.___.20____ г. По ___.___.20___г.

Наименование защищаемого ресурса № п/п	Должность	Фамилия и инициалы	Имя_Пользователя (идентификатор)	Пароль (аутентификатор)
1	2	3	6	7
1	Главный специалист отдела …Управления…	Иванов И.И.	1111	GN7U
2	Ведущий специалист отдела	Петрова П.П.	1112	F6R0
3				

Приложение 4

ФОРМА

Изменение прав доступа в локальную вычислительную сеть,
к информационным, техническим ресурсам

Директору ГАУ ТО «ЦИТ»
_____
(Ф.И.О.)

ЗАЯВКА

В связи с _____
(приемом на работу, переводом, изменением должностных обязанностей, увольнением, пр.)

_____
(полное наименование должности сотрудника)

_____
(Ф.И.О. сотрудника полностью)

прошу _____ доступ указанному сотруднику в домен
(установить, изменить, отменить)

локальной вычислительной сети и к следующим информационным (техническим) ресурсам:

1. _____
(указать наименование ресурса и тип прав доступа – пользователь, локальный администратор и пр.)

2. _____
(указать наименование ресурса и тип прав доступа – пользователь, локальный администратор и пр.)

_____ _____/_____/
(должность руководителя подразделения) (подпись) (Ф.И.О.)

"___"_____201_ г.

Приложение 5

Кодификатор Министерства.

Код	ОИВ
210	Министерство труда и социальной защиты Тульской области
U	Управление социальной защиты населения
C	Центр социального обслуживания

Кодификатор муниципальных районов и городских округов Тульской области

Код	Муниципальные районы и городские округа
01	МО Алексинский район
02	МО Арсеньевский район
03	МО Белевский район
04	МО Богородицкий район
05	МО Веневский район
06	МО Воловский район
08	МО Дубенский район
07	МО город Донской
09	МО Ефремовский район
10	МО Заокский район
11	МО Каменский район
13	МО Кимовский район
12	МО Киреевский район
14	МО Куркинский район
15	МО Ленинский район
16	МО город Новомосковск
17	МО Одоевский район
18	МО Плавский район
19	МО Суворовский район
20	МО Тепло-Огаревский район
21	МО Узловский район
22	МО Чернский район
23	МО Щекинский район
24	МО Ясногорский район
30	МО город Тула
25	Зареченский район города Тулы
26	Привокзальный район города Тулы
27	Пролетарский район города Тулы
29	Советский район города Тулы
28	Центральный район города Тулы

Приложение 6

ФОРМА

Карточка № 0000
на период с 00.00.00 по 00.00.00

_____

(Ф.И.О.)

_____

(наименование подразделения)

_____

(наименование должности.)

Краткое наименование ресурса	Идентификатор пользователя (Имя_Пользователя)	Аутентификатор пользователя (пароль)

Выдал

_____ _____/_____/

(должность сотрудника) (подпись) (Ф.И.О.)

«__» _____201__ г.

Приложение 7

ФОРМА

Журнала выдачи парольной документации

№ п/п	Фамилия И.О.	Номер карточки или наименование документа	Выдача			Обратный прием			
			Дата	Время*	Подпись	Дата	Время*	Фамилия И.О.	Подпись
1	Иванов И.И.	1	15.06.2013						
2	Петров П.П.	2	16.06.2013						
3	Кузнецов К.К.	Таблица допуска к базе …	17.06. 2013						
4									

* графа подлежит обязательному заполнению при выдаче паролей администраторам серверов