

ПРАВИЛА

осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами министерства образования и молодежной политики Ставропольского края

1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами министерства образования и молодежной политики Ставропольского края (далее – Правила) устанавливают порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в министерстве образования и молодежной политики Ставропольского края (далее – министерство).

2. Осуществление внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в министерстве осуществляется в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), постановлением Правительства РФ от 21 марта 2012 г. № 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», настоящими Правилами и другими нормативными правовыми актами, касающимися обработки персональных данных.

3. Основные понятия и термины, используемые в настоящих Правилах, применяются в том же значении, что и Федеральном законе № 152-ФЗ.

4. Целью осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных (далее – внутренний контроль) является обеспечение защиты персональных данных от несанкционированного доступа, неправомерного их использования или утраты, определение порядка и правил осуществления внутреннего контроля.

5. Внутренний контроль делится на текущий, плановый и внеплановый.

6. Текущий внутренний контроль осуществляется на постоянной основе ответственным за организацию обработки персональных данных в министерстве (далее - ответственный за организацию обработки) в ходе мероприятий по обработке персональных данных.

Ответственный за организацию обработки имеет право:

запрашивать у сотрудников министерства информацию, необходимую для реализации полномочий;

требовать от уполномоченных на обработку персональных данных должностных лиц уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных;

принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации;

вносить министру предложения о совершенствовании правового, технического и организационного регулирования обеспечения безопасности персональных данных при их обработке;

вносить министру предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации о персональных данных.

7. Плановый внутренний контроль осуществляется комиссией, образуемой приказом министра, в состав которой входят работники министерства, допущенные к обработке персональных данных.

Плановый внутренний контроль соответствия обработки персональных данных установленным требованиям в министерстве проводится на основании утвержденного министром плана осуществления внутреннего контроля соответствия обработки персональных данных установленным требованиям, разрабатываемого председателем комиссии. Периодичность плановой проверки – не реже одного раза в год.

8. Внеплановый внутренний контроль может осуществляться на основании поступившего в министерство письменного заявления о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется председателем комиссии в течение 3 рабочих дней с момента поступления соответствующего заявления.

В проведении проверки не может участвовать лицо, прямо или косвенно заинтересованное в её результатах.

9. При проведении внутреннего контроля ответственным за организацию обработки или комиссией должны быть полностью, объективно и всесторонне изучены:

наличие, учет, порядок хранения и обезличивания персональных данных;

порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке;

порядок и условия применения средств защиты информации;

эффективность принимаемых мер по обеспечению безопасности персональных данных;

состояние учёта ПЭВМ и съёмных носителей информации, содержащей персональные данные;

соблюдение правил доступа к персональным данным;

наличие (отсутствие) фактов несанкционированного доступа к персональным данным;

порядок проведения мероприятий и результаты по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

порядок проведения мероприятий по обеспечению целостности персональных данных.

10. В отношении персональных данных, ставших известными членам комиссии или ответственному за организацию обработки в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

11. Срок проведения плановой и внеплановой проверки не может составлять более 30 дней со дня принятия решения о её проведении.

12. Результаты внутреннего контроля оформляются в виде протокола проведения внутренней проверки (далее - протокол).

13. При выявлении в ходе внутреннего контроля нарушений ответственным за организацию обработки либо председателем комиссии в протоколе делается запись о мероприятиях по устранению нарушений и сроках исполнения.

14. Протоколы хранятся у ответственного за организацию обработки в течение текущего года. Уничтожение протоколов проводится ответственным за организацию обработки самостоятельно в январе года, следующего за проверочным годом.

15. О результатах внутреннего контроля и мерах, необходимых для устранения нарушений, министру докладывает ответственный за организацию обработки либо председатель комиссии.

Приложение 5
к приказу министерства
образования и молодежной
политики Ставропольского края
от « 6 » октября 20 16 г. № 1105-нп

ПОРЯДОК ДОСТУПА
служащих министерства образования и молодежной политики
Ставропольского края в помещения, в которых ведется обработка
персональных данных

Настоящий Порядок доступа служащих министерства образования и молодежной политики Ставропольского края в помещения, в которых ведется обработка персональных данных (далее – Порядок), разработан в соответствии с требованиями Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 21 марта 2012 г. № 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» и другими нормативными правовыми актами.

Целью настоящего Порядка является исключение несанкционированного доступа к персональным данным, обрабатываемым в министерстве образования и молодежной политики Ставропольского края (далее – министерство), лиц, не допущенных к обработке персональных данных в министерстве.

Персональные данные относятся к конфиденциальной информации. Служащие министерства, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе, установлением правил доступа в помещения, где обрабатываются персональные данные с использованием и без использования средств автоматизации.

Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. При хранении материальных носителей персональных данных, в том числе на бумажном носителе, должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный доступ к ним.

В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только служащие министерства, допущенные к работе с ними.

Нахождение в помещениях, в которых ведется обработка персональных данных, лиц, не являющихся служащими министерства, или служащих министерства, не допущенных к обработке персональных данных, возможно только в присутствии служащих министерства, обрабатывающих в данном помещении персональные данные или допущенных к этим персональным данным. Время нахождения в помещениях ограничивается временем решения служебного вопроса, в рамках которого возникла необходимость пребывания в помещении. Все сотрудники, постоянно работающие в помещении, должны быть допущены к работе с соответствующими видами персональных данных.

Служащие министерства, допущенные к работе с персональными данными, не должны покидать помещение не убедившись, что доступ посторонних лиц к персональным данным невозможен. Запрещается оставлять материальные носители с персональными данными без присмотра в незапертом помещении.

Ответственные за организацию доступа в помещения министерства, в которых ведется обработка персональных данных, назначаются приказом.

Внутренний контроль за соблюдением порядка доступа в помещения, в которых ведется обработка персональных данных, проводится в порядке, определенном Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным Федеральным законом «О персональных данных», принятыми в соответствии с ним нормативными правовыми актами и локальными актами министерства.

После окончания рабочего дня дверь каждого помещения, в котором ведется обработка персональных данных, закрывается на ключ и опечатывается, либо ставится на сигнализацию. Ключи в опечатанных тубусах сдаются дежурному охраннику.

В служебных помещениях, занимаемых министерством, применяются организационные, технические и физические меры, направленные для защиты от нецелевого использования, несанкционированного доступа,

раскрытия, потери, изменения и уничтожения обрабатываемых персональных данных.

К указанным мерам относятся:

физические меры защиты: установка дверей, снабженных замками, сейфов, решеток, штор или жалюзи на окнах, расположение мониторов, уничтожение носителей, содержащих персональные данные, и т.д.;

технические меры защиты: применение антивирусных программ, программ защиты, установление паролей на персональных компьютерах, применение съемных носителей информации и т.д.;

организационные меры защиты: обучение и ознакомление с принципами безопасности и конфиденциальности, доведение до операторов обработки персональных данных важности защиты персональных данных и способов обеспечения защиты, допуск к обработке персональных данных только специально назначенных людей и т.д.

Инструкция
по организации парольной защиты
в министерстве образования и молодежной политики Ставропольского края

1.1. Первичный пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), устанавливаемые системным администратором при создании новой учетной записи.

1.1.1. Установку первичного пароля производит старший инженер-программист сектора программно-информационного обеспечения (далее – системный администратор) при создании новой учетной записи. Ответственность за сохранность первичного пароля лежит на системном администраторе.

1.1.2. Первичный пароль может содержать несложную комбинацию символов, либо повторяющиеся символы.

1.1.3. При создании первичного пароля, системный администратор обязан установить опцию, требующую смену пароля при первом входе в систему, а также уведомить владельца учетной записи о необходимости произвести смену пароля.

1.1.4. Первичный пароль так же используется при сбросе забытого пароля на учетную запись. В любом случае, при использовании первичного пароля все требования настоящего документа сохраняются.

1.2. Основной пароль – комбинация символов (буквы, цифры, знаки препинания, специальные символы), известная только сотруднику организации, используемая для подтверждения подлинности владельца учетной записи.

1.2.1. Установку основного пароля производит пользователь при первом входе в систему с новой учетной записью.

1.2.2. При выборе пароля необходимо руководствоваться «Требованиями к паролям» (Приложение)

1.2.3. Пользователь несет персональную ответственность за сохранение в тайне основного пароля. Запрещается сообщать пароль другим лицам в том числе сотрудникам сектора программно-информационного обеспечения, записывать его, а так же пересылать открытым текстом в электронных сообщениях.

1.2.4. Пользователь обязан не реже одного раза в месяц производить смену основного пароля соблюдая требования настоящего документа.

1.2.5. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом в сектор программно-информационного обеспечения и изменить основной пароль.

1.2.6. Восстановление забытого основного пароля пользователя осуществляется системным администратором путем изменения (сброса) основного пароля пользователя на первичный пароль на основании письменной либо электронной заявки пользователя.

1.2.7. Устная заявка пользователя на изменение пароля не является основанием для проведения таких изменений.

1.2.8. Для предотвращения угадывания паролей системный администратор обязан настроить механизм блокировки учетной записи при трехкратном неправильном вводе пароля.

1.2.9. Разблокирование учетной записи пользователя осуществляется системным администратором на основании заявки владельца учетной записи (возможен вариант автоматического разблокирования через продолжительный промежуток времени).

1.3. Административный пароль – комбинация символом (буквы, цифры, знаки препинания, специальные символы), известная системному администратору (администратору БД, администратору приложения), используемая при настройке служебных учетных записей, учетных записей служб и сервисов, а так же специальных учетных записей.

1.3.1. При выборе административного пароля необходимо руководствоваться «Требованиями к паролям» (Приложение)

1.3.2. Системный администратор несет персональную ответственность за сохранение в тайне административного пароля. Запрещается сообщать пароль другим лицам, в том числе сотрудникам министерства, записывать его, а так же пересылать открытым текстом в электронных сообщениях.

1.3.3. Системный администратор обязан не реже одного раза в месяц производить смену административного пароля, соблюдая требования настоящего документа.

1.3.4. В случае компрометации пароля (либо подозрении на компрометацию) необходимо немедленно сообщить об этом заведующему сектором программно-информационного обеспечения и изменить административный пароль.

Копии административных паролей должны храниться в опечатанном конверте в секторе программно-информационного обеспечения.

Приложение
к Инструкции по организации
парольной защиты в министерстве
образования и молодежной политики
Ставропольского края

Требования к паролям

Пароли НЕ ДОЛЖНЫ состоять из:

- Вашего имени, отчества или фамилии ни в каком виде (т.е. написаны в строчном, в прописном, в смешанном виде, задом наперед, два раза и т.д.)
- Вашего идентификатора входа (login) ни в каком виде.
- Имен Вашей(его) супруги(а) или детей.
- Не используйте какую-либо информацию о себе. Сюда входят: номера телефонов, номера в пропусках и других документах, номер или марка вашего автомобиля, Ваш почтовый адрес и т.д. и т.п.
- Только цифр или одинаковых букв.
- Слов которые можно найти в словаре (любом, включая иностранные) или в каком-либо списке слов.
- Меньше чем шести символов.

Пароли ДОЛЖНЫ:

- Содержать строчные и прописные буквы.
- Содержать небуквенные символы (т.е. цифры, знаки пунктуации, специальные символы).
- Быть легко запоминаемы, чтобы не было необходимости записывать их.
- Быть составлены так, чтобы Вы могли быстро набрать их на клавиатуре. Это осложнит возможность подглядеть пароль.

Несмотря на такие жесткие требования, есть несколько способов выбора паролей, которые все же соответствуют этим правилам:

- * *Выберите предложение из песни или стихотворения, и отберите только первые буквы каждого слова (хотя в примере использовано английское предложение, Вы можете воспользоваться и другими языками)*

Pretty woman walking down the street становится Pwwdts.

- * *Выберите два коротких слова и соедините их с помощью*
 - *пунктуационных знаков и спец символов:*
- Dog+rain, kid<Goat, TOP^rank*

Приложение 7
к приказу министерства
образования и молодежной
политики Ставропольского края
от « 6 » октября 20 16 г. № 1105-нр

ТИПОВАЯ ФОРМА

разъяснения субъекту персональных данных юридических последствий
отказа предоставить свои персональные данные

Мне, _____,
(фамилия, имя, отчество)

разъяснены юридические последствия отказа предоставить свои
персональные данные _____

(министерству образования и молодежной политики Ставропольского края)

В соответствии с Постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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» и «Правилами обработки персональных данных в министерстве образования и молодежной политики Ставропольского края», определён перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с

(решением вопросов в сфере деятельности, оказанием государственной услуги, реализацией права на труд, права на пенсионное обеспечение, права на медицинское страхование работников)

Я предупрежден, что в случае отказа предоставить свои персональные данные, (далее нужное подчеркнуть) министерством образования и молодежной политики Ставропольского края при решении вопросов в сфере деятельности мои права могут быть реализованы не в полном объеме;

мои права на труд, на пенсионное обеспечение и медицинское страхование не могут быть реализованы в полном объёме, а трудовой договор (контракт) подлежит расторжению.

« ____ » _____ 20 ____ г.
(дата)

(подпись)

(расшифровка подписи)

Приложение 8
к приказу министерства
образования и молодежной
политики Ставропольского края
от « 6 » октября 20 16 г. № 1105-н/

ТИПОВАЯ ФОРМА

согласия на обработку персональных данных в министерстве образования и молодежной политики Ставропольского края иных субъектов персональных данных

С целью осуществления возложенных на министерство образования и молодежной политики Ставропольского края (далее - министерство) федеральным законодательством, законодательством Ставропольского края и Положением о министерстве полномочий и обязанностей по обеспечению проведения на территории Ставропольского края государственной политики и осуществлением управления, нормативно-правового регулирования в сфере образования

я, _____,
(фамилия, имя, отчество)

зарегистрированный по адресу: _____

паспорт серия _____ номер _____ выдан « _____ » _____ 20 _____ г.
(дата выдачи)

_____,
(наименование органа, выдавшего документ)

в соответствии со статьей 9 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» своей волей, в своем интересе и с целью решения вопросов сферы деятельности министерства, даю согласие

_____ (министерству образования и молодежной политики Ставропольского края)

(далее – оператору) на автоматизированную, а также без использования средств автоматизации обработку моих персональных данных включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных, а именно:

- 1) фамилия, имя, отчество;
- 2) дата рождения;
- 3) адрес регистрации по месту жительства;
- 4) адрес фактического проживания;
- 5) данные документа, удостоверяющего личность субъекта персональных данных;
- 6) почтовый адрес;
- 7) номер телефона, факса, адрес электронной почты;

- 8) индивидуальный налоговый номер;
- 9) номер страхового свидетельства обязательного пенсионного страхования;
- 10) реквизиты банковского счета;
- 11) данные о семейном положении;
- 12) данные на доверенное лицо;
- 13) сведения о социальных льготах и о социальном статусе.

Если мои персональные данные можно получить только у третьей стороны, то я должен быть уведомлен об этом заранее с указанием целей, предполагаемых источников и способов получения персональных данных. На это должно быть получено мое согласие.

Мне разъяснены мои права и обязанности, связанные с обработкой персональных данных, в том числе моя обязанность проинформировать оператора в случае изменения моих персональных данных и мое право в любое время отозвать свое согласие путем направления соответствующего письменного заявления оператору.

Согласие вступает в силу со дня его подписания и действует в течение неопределенного срока до достижения цели обработки персональных данных или его отзыва мной в письменной форме.

« _____ » _____ 20 ____ г _____ « _____ »
(дата) (подпись) (расшифровка подписи)

Приложение 9
к приказу министерства
образования и молодежной
политики Ставропольского края
от « 6 » октября 20 16 г. № 1105-нп

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО
работника министерства образования и молодежной политики
Ставропольского края, непосредственно осуществляющего обработку
персональных данных, ставших известными ему в связи с исполнением
должностных обязанностей

Я, _____,
(фамилия, имя, отчество)

(должность)

обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей в министерстве образования и молодежной политики Ставропольского края (далее – министерство), в случае расторжения со мной контракта (договора), освобождения меня от замещаемой должности и увольнения.

В соответствии со статьей 7 Федерального закона от 27 июля 2006 года №152-ФЗ «О персональных данных» я уведомлен(а) о том, что персональные данные являются конфиденциальной информацией. Я обязан(а) не раскрывать третьим лицам и не распространять персональные данные, ставшие известными мне в связи с исполнением должностных обязанностей в министерстве, без согласия субъекта персональных данных.

Ответственность, предусмотренная Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и другими федеральными законами, мне разъяснена.

« _____ » _____ 20 ____ г _____ « _____ »
(дата) (подпись) (расшифровка подписи)

Приложение 10
к приказу министерства
образования и молодежной
политики Ставропольского края
от « 6 » октября 20 16 г. № 1105-14

ПЕРЕЧЕНЬ
информационных систем персональных данных
министерства образования и молодежной политики Ставропольского края

№	Наименование	Класс
1.	«Инфин-Бухгалтерия»	К3 специальная
2.	«Аист»	К1 специальная
3.	«Кадры государственных и гражданских служащих Ставропольского края»	К3 специальная
4.	«Дело»	К2 специальная
5.	«Единая информационная система для предоставления государственных и муниципальных услуг в сфере образования»	К3 специальная

Приложение 11
к приказу министерства
образования и молодежной
политики Ставропольского края
от « 6 » октября 20 16 г. № 1105-п/к

ПЕРЕЧЕНЬ

должностей государственных гражданских служащих и работников
министерства образования и молодежной политики Ставропольского края,
ответственных за проведение мероприятий по обезличиванию
обрабатываемых персональных данных

№ п/п	Наименование структурного подразделения	Наименование должности
1.	Руководство	первый заместитель министра
		заместитель министра
2.	Отдел бухгалтерского учета и контроля	начальник отдела (главный бухгалтер)
		консультант отдела
		ведущий специалист
		старший бухгалтер
3.	Отдел организационного и кадрового обеспечения	начальник отдела
		консультант
		ведущий специалист
4.	Отдел развития семейных форм устройства детей, оставшихся без попечения родителей	начальник отдела
		консультант
		ведущий специалист
		старший инженер-программист
5.	Сектор программно-информационного обеспечения	заведующий сектором

Приложение 12
к приказу министерства
образования и молодежной
политики Ставропольского края
от « 6 » октября 2016 г. № 1105-нр

ПЕРЕЧЕНЬ

должностей государственных гражданских служащих и работников министерства образования и молодежной политики Ставропольского края, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

№ п/п	Наименование структурного подразделения	Наименование должности
1.	Руководство	первый заместитель министра
		заместитель министра
2.	Отдел бухгалтерского учета и контроля	начальник отдела (главный бухгалтер)
		консультант отдела
		ведущий специалист
		старший бухгалтер
3.	Отдел организационного и кадрового обеспечения	начальник отдела
		консультант
		ведущий специалист
4.	Отдел развития семейных форм устройства детей, оставшихся без попечения родителей	начальник отдела
		консультант
		ведущий специалист
		старший инженер-программист
5.	Сектор программно-информационного обеспечения	заведующий сектором

ПЕРЕЧЕНЬ

программного обеспечения, разрешенного к использованию в министерстве образования и молодежной политики Ставропольского края

1. Операционные системы: семейства «Microsoft Windows»; семейства «Linux».
2. Средства Microsoft Office; LibreOffice.
3. Программное обеспечение бухгалтерского и кадрового учета:
4. 1С Предприятие 8.2, 1С: Свод отчетов 7.7; 1С 7.7: Бухгалтерский учет; «Инфин-Управление»; «Скиф 3»; «Парус-Сведение отчетности онлайн»; «Удаленное место бюджетополучателя»; «SberSigun»; «Кладр: АРМ «Клиент»»; АС «Клиент- Сбербанк»; «Налогоплательщик ЮЛ»; «НД СПУ» «Криста» «СЭД УФК» «УРМ АС Бюджет» «Кадры государственных гражданских служащих Ставропольского края».
4. Антивирусное программное обеспечение: «Eset nod 32 Antivirus»; «Kaspersky Antivirus».
5. Средства криптографической защиты информации:
6. «Крипто-Про CSP»; «Rutoken Drivers» «Континент-АП» «VipNet Client»
7. Программное обеспечение для просмотра электронной почты:
8. «The Bat!»; «Mozilla Thunderbird».
9. Интернет браузеры: «internet Explorer»; «Mozilla Firefox»; «Opera».
10. Программное обеспечение для архивирования файлов и папок (архиваторы): «HaoZip»; «7Zip».
11. Программное обеспечение ABBYY Fine Reader.
12. Программное обеспечение Adobe Flash Player.
13. Программное обеспечение Adobe Acrobat Reader; Windows Djview.
14. Справочно-правовая система: «Гарант»; «Консультант Плюс».
15. Информационные системы персональных данных.
16. Программный комплекс «10-Strike».
17. Программный комплекс «Nero».
18. Программное обеспечение «Аском-Док»

19. Специализированное программное обеспечение, необходимое для обработки массивов данных, для достижения целей поставленных руководством министерства образования Ставропольского края.

*Внесение изменений в список разрешенного программного обеспечения или установка и использование неуказанных в списке программных продуктов возможно только при письменном согласовании с заведующим сектором программно-информационного обеспечения.

ПЕРЕЧНИ

персональных данных, обрабатываемых в министерстве образования и молодежной политики Ставропольского края в связи с реализацией служебных или трудовых отношений, а также в связи оказанием государственных услуг и осуществлением государственных функций

I. Перечень персональных данных, обрабатываемых в министерстве образования и молодежной политики Ставропольского края в связи с реализацией служебных и трудовых отношений:

- 1) фамилия, имя, отчество;
- 2) дата рождения;
- 3) пол;
- 4) месторождения;
- 5) информация о смене фамилии;
- 6) гражданство;
- 7) адрес регистрации по месту жительства;
- 8) адрес фактического проживания;
- 9) данные документ, удостоверяющего личность субъекта персональных данных;
- 10) номер телефона, факса, адрес электронной почты;
- 11) индивидуальный налоговый номер;
- 12) номер страхового свидетельства обязательного пенсионного страхования;
- 13) данные на доверенное лицо;
сведения о социальных льготах и о социальном статусе;
- 14) номер страхового медицинского полиса обязательного медицинского страхования граждан;
- 15) информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающих образование (наименование, номер, дата выдачи, специальность, квалификация);
- 16) информация о трудовой деятельности до приема на работу;
- 17) информация о трудовом стаже (место работы, должность, период работы, причины увольнения);
- 18) информация о знании иностранных языков;
- 19) форма допуска к государственной тайне;

- 20) ученая степень, ученое звание;
- 21) денежное содержание, оклад;
- 22) справка с Главного управления министерства внутренних дел Российской Федерации по Ставропольскому краю об отсутствии судимости;
- 23) данные о служебном контракте (номер, дата заключения, вид работы, наличие испытания, режим труда, длительность основного и дополнительных отпусков, дополнительные социальные льготы и гарантии, характер работы, форма оплаты, условия труда, продолжительность рабочей недели, система оплаты);
- 24) сведения о воинском учете (категория запаса, воинское звание, категория годности к военной службе, информация о снятии с воинского учета);
- 25) данные об аттестации;
- 26) данные о повышении квалификации;
- 27) информация о профессиональной переподготовке, стажировке;
- 28) данные о наградах, поощрениях, почетных званиях;
- 29) информация о дисциплинарных взысканиях, судимостях, исполнительных листах;
- 30) информация о приеме на работу, перемещении по должности, увольнении;
- 31) информация об отпусках;
- 32) информация о командировках;
- 33) сведения и заключения о состоянии здоровья установленной формы об отсутствии у гражданина заболеваний, препятствующих поступлению на государственную гражданскую службу или ее прохождению;
- 34) сведения и заключения установленной формы об отсутствии медицинских противопоказаний для работы со сведениями составляющими государственную тайну;
- 35) информация о государственном/негосударственном пенсионном обеспечении;
- 36) реквизиты банковского счета;
- 37) данные о семейном положении, составе семьи, сведения о близких родственниках;
- 38) сведения о доходах, об имуществе и обязательствах имущественного характера, о доходах, об имуществе и обязательствах имущественного характера супруги (супруга) и несовершеннолетних детей;
- 39) фотография.

II. Перечень персональных данных, обрабатываемых в министерстве образования и молодежной политики Ставропольского края в связи с оказанием государственных услуг и осуществлением государственных функций:

- 1) фамилия, имя, отчество;

- 2) дата рождения;
- 3) пол;
- 4) место рождения;
- 5) информация о смене фамилии;
- 6) гражданство;
- 7) адрес регистрации по месту жительства;
- 8) адрес фактического проживания;
- 9) данные документа, удостоверяющего личность субъекта персональных данных;
- 10) номер телефона, факса, адрес электронной почты;
- 11) индивидуальный налоговый номер;
- 12) номер страхового свидетельства обязательного пенсионного страхования;
- 13) медицинское заключение о состоянии здоровья;
- 14) данные на доверенное лицо;
- 15) информация об образовании (наименование образовательного учреждения, сведения о документах, подтверждающих образование (наименование, номер, дата выдачи, специальность, квалификация));
- 16) информация о трудовой деятельности;
- 17) информация о трудовом стаже (место работы, должность, период работы, причины увольнения);
- 18) денежное содержание, оклад;
- 19) реквизиты банковского счета;
- 20) данные о семейном положении, составе семьи, сведения о близких родственниках;
- 21) сведения об имуществе и обязательствах имущественного характера;
- 22) национальность;
- 23) сведения: внешность (цвет глаз, цвет волос); физическое развитие (рост, вес и др.); особенности характера; этническое происхождение; принадлежность к определенной религии и культуре;
- 24) документы, подтверждающие правовой статус ребенка-сироты (свидетельства о смерти родителей, решение суда о лишении их родительских прав, признании недееспособными и иные, установленные действующим законодательством);
- 25) свидетельство о рождении.

Приложение 15
к приказу министерства
образования и молодежной
политики Ставропольского края
от « 6 » октября 20 16 г. № 1105-п/к

ДОЛЖНОСТНОЙ РЕГЛАМЕНТ
ответственного за организацию обработки персональных данных в
министерстве образования и молодежной политики
Ставропольского края

1. Общие положения

1.1. Ответственный за организацию обработки персональных данных в министерстве образования и молодежной политики Ставропольского края (далее - ответственный за организацию обработки персональных данных) назначается приказом министра образования и молодежной политики Ставропольского края.

1.2. Ответственный за организацию обработки персональных данных в своей деятельности руководствуется Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 15 сентября 2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», от 21 марта 2012 г. №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». Постановлением Правительства Ставропольского края от 20 ноября 2013 г. № 421-п «Об утверждении Положения о министерстве образования и молодежной политики Ставропольского края», настоящей должностной инструкцией.

1.3. Ответственный за организацию обработки персональных данных является уполномоченным на поддержание достигнутого уровня защиты информационных систем персональных данных и ее ресурсов на этапах эксплуатации.

1.4. Ответственный за организацию обработки персональных данных осуществляет методическое руководство работников министерства образования и молодежной политики Ставропольского края (далее - министерство), имеющих доступ к персональным данным, в вопросах обеспечения безопасности персональных данных. Требования ответственного за организацию обработки персональных данных, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми

работниками министерства, имеющими доступ к персональным данным.

1.5. Ответственный за организацию обработки персональных данных несет персональную ответственность за качество проводимых им работ по контролю за соблюдением министерством и его работниками, имеющими доступ к персональным данным, законодательства Российской Федерации, в том числе требований к защите персональных данных, нормативных правовых актов министерства по вопросам обработки персональных данных, состояние и поддержание установленного уровня защиты информационных систем персональных данных.

2. Функции ответственного за организацию обработки персональных данных

2.1. Ответственный за организацию обработки персональных данных обязан:

предоставлять субъекту персональных данных либо его представителю по запросу информацию об обработке его персональных данных;

осуществлять внутренний текущий контроль за соблюдением требований законодательства Российской Федерации и Правил обработки персональных данных в министерстве при обработке персональных данных, в том числе требований к защите персональных данных;

доводить до сведения работников министерства, имеющих доступ к персональным данным, положения законодательства Российской Федерации о персональных данных, нормативных правовых актов министерства по вопросам обработки персональных данных, требований к защите персональных данных;

организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой их обращений и запросов;

получать обязательство от работников министерства, имеющих доступ к персональным данным, в случае расторжения с ними государственного контракта, о прекращении обработки персональных данных, ставших известными им в связи с исполнением должностных обязанностей;

получать согласие на обработку персональных данных у субъекта персональных данных;

разъяснять субъекту персональных данных юридические последствия отказа предоставления его персональных данных.

2.2. Ответственный за организацию обработки персональных данных имеет право:

подать ходатайство руководству о прохождении обучения по защите персональных данных в учебных центрах и курсах повышения квалификации;

вносить руководству предложения о привлечении к ответственности отдельных работников министерства, имеющих доступ к персональным данным, допустивших серьезные нарушения в обеспечении безопасности персональных данных.