ПРАВИТЕЛЬСТВО КУРГАНСКОЙ ОБЛАСТИ

УПРАВЛЕНИЕ ПО ФИЗИЧЕСКОЙ КУЛЬТУРЕ, СПОРТУ И ТУРИЗМУ КУРГАНСКОЙ ОБЛАСТИ

ПРИКАЗ

от 25 февраля 2013г. № 40
г. Курган

Об утверждении Положения об обработке персональных данных в Управлении по физической культуре, спорту и туризму Курганской области

В соответствии с Федеральным законом от 27 июля 2004 года №79-ФЗ «О государственной гражданской службе Российской Федерации», Федеральным законом от 27 июля 2006 года №152-ФЗ «О персональных данных», Трудовым кодексом Российской Федерации, законом Курганской области от 4 марта 2005 года №28 «О государственной гражданской службе Курганской области», Указом Президента Российской Федерации от 30 мая 2005 года № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», Постановлением Правительства Российской Федерации от 17 ноября 2007 года №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

ПРИКАЗЫВАЮ:

1. Утвердить Положение об обработке персональных данных в Управлении по физической культуре, спорту и туризму Курганской области. Приложение 1.
2. Утвердить Список должностей государственных гражданских служащих Управления по физической культуре, спорту и туризму Курганской области, уполномоченных на обработку персональных данных и (или) имеющих доступ к персональным данным. Приложение 2.
3. Утвердить Список информационных систем персональных данных Управления по физической культуре, спорту и туризму Курганской области, включая перечень информации, содержащейся в этих информационных системах. Приложение 3.
4. Утвердить Инструкцию по организации парольной защиты в информационной системе Управления по физической культуре, спорту и туризму Курганской области. Приложение 4.
5. Утвердить Инструкцию по организации антивирусной защиты в информационной системе Управления по физической культуре, спорту и туризму

Курганской области. Приложение 5.

6. Утвердить Инструкцию по организации резервного копирования и восстановления программного обеспечения, баз данных в информационной системе Управления по физической культуре, спорту и туризму Курганской области. Приложение 6.

7. Руководителям структурных подразделений Управления по физической культуре, спорту и туризму Курганской области:

в своей деятельности по обработке персональных данных руководствоваться утвержденным Положением об обработке персональных данных в Управлении по физической культуре, спорту и туризму Курганской области;

доработать должностные регламенты государственных гражданских служащих Управления по физической культуре, спорту и туризму Курганской области, уполномоченных на обработку персональных данных, в части закрепления ответственности, предусмотренной законодательством Российской Федерации за нарушение режима конфиденциальности, а также обеспечения безопасности обрабатываемых ими персональных данных.

8. Пухову А.Ю., начальнику отдела финансово-экономического анализа и отчетности — главному бухгалтеру Управления по физической культуре, спорту и туризму Курганской области обеспечить финансирование затрат, связанных с защитой персональных данных в Управлении по физической культуре, спорту и туризму Курганской области.

9. Контроль за выполнением настоящего приказа возложить на Гаста И.П., заместителя начальника Управления-заведующего сектором организационного обеспечения и кадров.

Начальник Управления
по физической культуре, спорту
и туризму Курганской области А.А. Васильев

С приказом ознакомлены:
Гаста И.П.
Панасенко Н.С.
Суханова Н.А.
Пухов А.Ю.
Шалатов Е.А.
Овчинникова И.В.
Абалина С.А.
Воробьева В.А.
Григорьева Н.И.
Кочурова Ю.И.
Черников П.А.
Досина В.В.
Рязанова Т.А.
Сысолова Ю.В.
Антропова Н.Ю

Н.А.Суханова
(3522) 42-15-59

Приложение 1
к приказу Управления по физической культуре, спорту и туризму Курганской области
от « 25 » февраля 2013 года № 40
«Об утверждении Положения об обработке персональных данных в Управлении по физической культуре, спорту и туризму Курганской области»

Положение об обработке персональных данных в Управлении по физической культуре, спорту и туризму Курганской области

I. Общие положения

1. Положение об обработке персональных данных в Управлении по физической культуре, спорту и туризму Курганской области (далее Положение) разработано в соответствии с Федеральным законом от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», законом Курганской области от 4 марта 2005 года № 28 «О государственной гражданской службе Курганской области», Указом Президента Российской Федерации от 30 мая 2005 года №609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», Постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

2. Положение определяет порядок и условия обработки персональных данных в Управлении по физической культуре, спорту и туризму Курганской области с использованием средств автоматизации и без использования таких средств.

3. Обеспечение безопасности ПДн при их обработке в ИСПДн достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого могут стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия. Для защиты ПДн создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Мероприятия по обеспечению безопасности ПДн формулируются в зависимости от класса ИСПДн, определяемого с учетом возможного возникновения угроз безопасности жизненно важным интересам личности, общества и государства.

II. Порядок обработки персональных данных государственных гражданских служащих Управления по физической культуре, спорту и туризму Курганской области и иных лиц

4. Обработка персональных данных в Управлении по физической культуре, спорту и туризму Курганской области осуществляется в целях осуществления, в пределах

своей компетенции, отраслевого либо межотраслевого регулирования в сфере физической культуры, спорта и туризма Курганской области, а также ведения кадровой работы (ведение и хранение личных дел, учетных карточек и трудовых книжек государственных гражданских служащих, содействия гражданскому служащему в прохождении государственной гражданской службы, в обучении и должностном росте, обеспечения личной безопасности гражданского служащего и членов его семьи, учета результатов исполнения им должностных обязанностей, в целях обеспечения сохранности имущества Управления по физической культуре, спорту и туризму Курганской области, а также документов кандидатов на замещение вакантных должностей государственной гражданской службы (кадровый резерв) Управления по физической культуре, спорту и туризму Курганской области.

5. Обработка персональных данных гражданских служащих осуществляется как с использованием средств автоматизации, так и без использования таких средств.

6. Для обеспечения безопасности ПДн при обработке в ИСПДн осуществляется защита информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, оптической и иной основе, в виде информационных массивов и баз данных в ИСПДн.

7. Для защиты персональных данных необходимо соблюдать ряд мер:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют работы с персональными данными;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест, при котором исключалась бы бесконтрольное использование защищаемой информации;
- знание сотрудниками Управления требований нормативно-методических документов по защите информации;
- наличие необходимых условий в помещениях для работы с конфиденциальными документами и базами данных;
- определение и регламентация состава сотрудников, имеющих право доступа (входа) в помещения, в которых функционируют ИСПДн;
- организация порядка уничтожения информации;
- своевременное выявление нарушений требований разрешительной системы доступа к ПДн,
- обучение сотрудников, воспитательная и разъяснительная работа по вопросам информационной безопасности;
- определение и регламентация состава сотрудников, имеющих право доступа к информационным ресурсам ИСПДн.

III. Основные термины и определения

Персональные данные (ПДн) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уничтожение

(обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Использование персональных данных — действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц.

Блокирование персональных данных — временное прекращение сбора, систематизации, накопления, использования, распространения персональных данных, в том числе их передачи.

Уничтожение персональных данных — действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Обезличивание персональных данных — действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Информационная система персональных данных (ИСПДн) — информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Конфиденциальность персональных данных — обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Угроза или опасность утраты персональных данных — единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

IV. Основные мероприятия по организации обеспечения безопасности персональных данных

8. Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование и реализация совокупности согласованных по цели, задачам, месту и времени организационных и технических мероприятий, направленных на минимизацию ущерба от возможной реализации угроз безопасности ПДн.

9. Обязанности по реализации необходимых организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними, возлагаются на Управление по физической культуре, спорту и туризму Курганской области.

10. Технические и программные средства, используемые для обработки ПДн в ИСПДн, должны удовлетворять установленным в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в ИСПДн, в установленном порядке проходят процедуру оценки соответствия, включая сертификацию на соответствие требованиям по безопасности информации.

11. Обработка персональных данных должна осуществляться на основе принципов:

- законности целей и способов обработки персональных данных и добросовестности;

- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;

- соответствия объема и характера обрабатываемых персональных данных, способов обработки целям обработки персональных данных;

- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных при по отношению к целям, заявленным при сборе персональных данных;

- недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

12. Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой системы (подсистемы) защиты персональных данных (СЗПДн). Структура, состав и основные функции СЗПДн определяются исходя из класса ИСПДн. СЗПДН включает организационные меры и технические средства защиты информации, а также используемые в информационной системе информационные технологии.

13. Сотрудники Управления, ответственные за хранение персональных данных, а также сотрудники Управления, владеющие персональными данными в силу своих должностных обязанностей, подписывают Обязательство о конфиденциальности (Приложение 1).

14. Помещения, в которых хранятся и обрабатываются персональные данные, должны быть оборудованы надежными замками и сигнализацией на вскрытие помещений, в рабочее время данные помещения при отсутствии в них работников должны быть закрыты, проведение уборки помещений должно производится в присутствии работников подразделений, ответственных за данные помещения.

V. Обязанности должностных лиц, эксплуатирующих ИСПДн, в части обеспечения безопасности персональных данных при их обработке в ИСПДн

15. При обработке персональных данных Управление, выполняя функции оператора Пдн, обязано соблюдать следующие требования:

- обработка персональных данных осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных актов Российской Федерации;

- обработка персональных данных сотрудников Управления осуществляется в целях содействия сотруднику в обучении и должностном росте, обеспечения личной безопасности сотрудников и членов его семьи, а также в целях обеспечения сохранности принадлежащего ему имущества и имущества Управления, учета результатов исполнения им должностных обязанностей;

- персональные данные следует получать лично у субъекта ПДн, в случае возникновения необходимости получения персональных данных субъекта у третьей стороны следует известить об этом объект ПДн заранее, получить его письменное согласие и сообщить ему о целях, предполагаемых источниках и способах получения персональных данных;

- запрещается получать, обрабатывать и вносить в ИСПДн не установленные Федеральными законами "О персональных данных" персональные данные о политических, религиозных и иных убеждениях, частной жизни, членстве в общественных объединениях, в том числе в профессиональных союзах;

- при принятии решений, затрагивающих интересы субъекта ПДн, запрещается основываться на персональных данных, полученных исключительно в результате их автоматизированной обработки или с использованием электронных носителей;

- защита персональных данных от неправомерного их использования или утраты обеспечивается за счет средств оператора в порядке, установленном Федеральным законом "О персональных данных", Трудовым кодексом Российской Федерации и иными нормативными правовыми актами Российской Федерации;

- передача персональных данных субъекта ПДн третьей стороне не допускается без письменного согласия субъекта, за исключение случаев, установленных федеральными законами Российской Федерации;

- обеспечивается конфиденциальность персональных данных, за исключением случаев обезличивания персональных данных и в отношении общедоступных персональных данных;

- хранение персональных данных должно осуществляться в форме, позволяющей определить субъект персональных данных, не дольше, чем этого требуют цели их обработки, и они подлежат уничтожению по достижению целей обработки или в случае утраты необходимости в их достижении.

VI. Порядок предоставления информации, содержащей персональные данные

16. Передача и и предоставление ПДн законным пользователям должна осуществляться способом, не допускающим возможность несанкционированного доступа к ним посторонним лиц.

17. Передача информации, содержащей персональные данные субъекта ПДн, другим учреждениям и организациям, осуществляется только при наличии правомерных письменных запросов в размере, который позволяет не разглашать излишний объем персональных сведений.

18. При передаче персональных данных субъекта ПДн оператор должен соблюдать следующие требования:

- не сообщать персональные данные третьей стороне без письменного согласия субъекта, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровья субъекта ПДн, а также в случаях установленных федеральным законом;

- не сообщать персональные данные в коммерческих целях без его письменного согласия;

- предупредить лиц, получающих персональные данные субъекта, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим конфиденциальности. Данное положение не распространяется на обмен персональными данными субъектов ПДн в порядке, установленном Федеральным законом;

- разрешить доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;

- не запрашивать информацию о состоянии здоровья субъекта ПДн, являющегося сотрудником Управления , за исключением тех сведений, которые относятся к вопросу о возможности выполнения сотрудником трудовой функции;

- передавать персональные данные субъекта ПДн представителю этого субъекта в порядке, установленном Трудовым кодексом, и ограничивать эту информацию только теми персональными данными, которые необходимы для выполнения указанными представителями их функций;

- при обращении с запросом о персональных данных сотрудника Управления лица, не уполномоченного федеральным законом на получение персональных данных, либо при отсутствии письменного согласия сотрудника на предоставление его персональных данных Управление обязан отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

VII. Обеспечение защиты персональных данных, хранящихся в личных делах сотрудников Управления

19. В целях обеспечения защиты персональных данных, хранящихся в личных делах сотрудников Управления, сотрудники имеют право:

- получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

- осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные сотрудника, за исключением случаев, предусмотренных Федеральным законом "О персональных данных";

- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушением Федеральных законов. Сотрудник при отказе оператора исключить или исправить его персональные данные имеет право заявить в письменной форме работодателю о своем несогласии, обосновав соответствующим образом такое несогласие. Персональные данные оценочного характера сотрудник имеет право дополнить заявлением, выражающим его собственную точку зрения;

- требовать от работодателя уведомления всех лиц, которым ранее были сообщены неверные или неполные их персональные данные, обо всех произведенных в них изменениях или исключениях из них;

- обжаловать действия или бездействие работодателя в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке, если

гражданский служащий, являющийся субъектом персональных данных, считает, что оператор осуществляет обработку его персональных данных с нарушением требований Федерального закона "О персональных данных" или иным образом нарушает его права и свободы.

20. В целях достоверности персональных данных, хранящихся в личных делах сотрудников Управления, сотрудники обязаны:

- передавать работодателю или его представителю комплекс достоверных, документированных персональных данных, состав которых установлен действующим законодательством Российской Федерации;

- при изменении сведений, содержащих персональные данные (фамилия, имя, отчество, адрес, паспортные данные, сведения об образовании, семейном положении, состоянии здоровья, при выявлении противопоказаний для выполнения служебных обязанностей), своевременно (как правило, в 3-х дневный срок) сообщать о таких изменениях.

VIII. Порядок приостановки предоставления ПДн в случае обнаружения нарушения порядка их предоставления

21. В случае обнаружения нарушений порядка предоставления ПДн ответственным за обеспечение безопасности ПДн выносится предписание, по которому приостанавливается обработка ПДн до выяснения и устранения причин нарушений.

22. Регистрация и расследование фактов нарушения порядка предоставления ПДн проводится в соответствии с разделом XIV данного Положения.

IX. Правила парольной защиты

23. Правила парольной защиты содержатся в Инструкции по организации парольной защиты в информационной системе Управления по физической культуре, спорту и туризму Курганской области (Приложение 4).

X. Правила антивирусной защиты

24. Правила антивирусной защиты содержатся в Инструкции по организации антивирусной защиты в информационной системе Управления по физической культуре, спорту и туризму Курганской области (Приложение 5).

XI. Правила резервного копирования и восстановления программного обеспечения, баз данных в информационной системе

25. Правила резервного копирования и восстановления программного обеспечения, баз данных в информационной системе содержатся в Инструкции по организации резервного копирования и восстановления программного обеспечения, баз данных в информационной системе Управления физической культуры, спорту итуризму Курганской области (Приложение № 6).

XII. Требования к помещениям, в которых располагаются ИСПДн

26. ПДн, обрабатываемые в ИСПДн, являются информационными данными, защищаемыми в соответствии с требованиями, установленными законодательством Российской Федерации.

27. В соответствии с требованиями ИБ, архивы ПДн и ИСПДн (как на электронных, бумажных, так и на иных носителях), оборудование, доступ к которому должен быть ограничен в силу его важности для технологического цикла предприятия (помещения серверных, АТС, АРМов и т.п.), а также обработка ПДн в ИСПДн должны производиться в помещениях, относящихся к категории "помещения ограниченного доступа".

28. Помещения ограниченного доступа должны располагаться в контролируемой зоне.

29. Пребывание посторонних лиц в помещениях разрешено только в сопровождении сотрудников, работающих в указанных помещениях, и только с разрешения руководства вышеупомянутых сотрудников.

30. Помещения ограниченного доступа должны отвечать следующим требованиям:

- помещение должно располагаться в контролируемой зоне;

- двери помещения должны иметь надежные запоры, приспособления для опечатывания, должны быть обеспечены пожарной и охранной сигнализацией;

- должны быть задействованы все меры, исключающие неконтролируемое пребывание в помещении любых лиц, включая сотрудников Управления, не допущенных к работе с ПДн;

- от дверей помещения должны быть резервные ключи;

- размещение в помещении оборудования и вспомогательных технических средств должно отвечать санитарно-гигиеническим нормам, а также требованиям техники безопасности и пожарной безопасности.

31. Работник, осуществляющий хранение архивов и /или резервных копий ИСПДн, должен иметь печать для опечатывания дверей и сейфа или металлического хранилища.

32. Выполнение требований по обеспечению ИБ на рабочих местах осуществляется работниками, работающими в помещениях ограниченного доступа.

33. Ответственность за невыполнение требований по Иб для помещений ограниченного доступа несут руководители структурных подразделений, работники которых работают в этих помещениях.

XIII. Порядок проведения служебной проверки при нарушениях режима безопасности при обработке ПДн в ИСПДн

34. Служебная проверка при нарушениях режима безопасности при обработке ПДн в ИСПДн (далее — служебная проверка) проводится для определения уровня защищенности ИСПДн и мер по возможному предотвращению инцидентов ИБ.

35. Служебная проверка назначается по нарушениям 1 и 2 категории по каждому отдельному факту нарушения.

36. Основаниями для назначения служебной проверки являются устное заявление, докладная или служебная записка сотрудника Управления, а также выявление факта одного или нескольких нарушений.

37. Состав комиссии, а также сроки проведения служебной проверки назначаются приказом Управления, по каждому отдельному факту нарушения или по факту группы нарушений.

38. Члены комиссии имеют право:

- требовать документального подтверждения факта нарушений информационной безопасности ИСПДн;

- устанавливать причины допущенных нарушений любым из способов, не противоречащих законодательству Российской Федерации;

- брать письменное объяснение по поводу выявленных нарушений у любого сотрудника Управления.

39. По результатам работы комиссии оформляется акт о результатах служебной проверки, который подписывается членами комиссии и направляется руководителю, назначившему служебную проверку.

XIV. Перечень нарушений ИБ ИСПДн

40. К нарушениям 1 категории относятся события, повлекшие за собой разглашение (утечку) защищаемых ПДн и/или утрату содержащих их отчуждаемых носителей, уничтожение (искажение) баз данных ИСПДн, выведение из строя технических и программных средств, а именно:

- несанкционированная переконфигурация параметров ИСПДн;

- утрата или кража резервной копии базы данных ИСПДн;

- необоснованная передача базы данных ИСПДн;

- организация утечки ПДн ИСПДн по техническим каналам;

- умышленное нарушение работоспособности ИСПДн;

- НСД к ПДн ИСПДн;

- несанкционированное внесение изменений в базу данных ИСПДн;

- умышленное заражение компьютеров и серверов ИСПДн вирусами;

- проведение работ с ИСПДн, повлекшее за собой необратимую потерю данных;

- другие действия, подпадающие под действия статей 272, 273, 274 УК РФ.

41. К нарушениям 2 категории относятся события, в результате которых возникают предпосылки к разглашению (утечке) защищаемых ПДн, утрате содержащих их отчуждаемых носителей, уничтожению (искажению) баз данных ИСПДн, выведению из строя технических и программных средств, а именно:

- подбор административного пароля (успешный);

- ошибка при входе в ИСПДн (набор не назначенного пароля, более трех раз подряд, периодически);

- несанкционированное (неоднократное) оставление включенного ПК;

- утрата учтенного отчуждаемого съемного носителя;

- попытка входа по чужим именем, паролем, многократная неудача;

- попытка входа по чужим именем, паролем, удачная;

- несанкционированная очистка журналов аудита;

- несанкционированное копирование ПДн на внешние носители;

- несанкционированная установка (удаление) ПО на ПК ИСПДн;

- попытка получения прав администратора на локальном ПК (увеличения собственных прав, получение прав на отладку программ), удачная и неудачная;

- попытка получения прав администратора в домене или на удаленной машине, удачная и неудачная;

- неумышленное заражение компьютеров и серверов ИСПДн вирусами;

- несанкционированное использование сканируемого ПО;

- несанкционированный просмотр, вывод на печать ПДн.

42. К нарушениям 3 категории относятся события, не несущие признаков нарушений 1 и 2 категории, а именно:

- ошибка при входе в ИСПДн (набор неправильного пароля, сетевого имени более 3-х раз подряд);

- попытка неудачного доступа к ПДн ИСПДн (периодическая);

- перевод времени на ПК;

- работа на ПК в неразрешенное время;

- перезагрузка компьютера при сбоях в работе ПК (однократная), в т.ч. аварийная перезагрузка, путем нажатия кнопки RESET;

- нецелевое использование корпоративных ресурсов (печать, Internet, mail, и др).

XV. Порядок взаимодействия с вышестоящими службами и федеральными органами

43. Уведомление об обработке персональных данных направляется в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор).

44. Получение Выписки регламентируется приказом Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 28.03.2008 г. № 154 "Об утверждении положения о ведении реестра операторов, осуществляющих обработку персональных данных".

45. Операторы, включенные в Реестр, вправе получить выписку из Реестра по письменному обращению в Службу в срок не позднее 30-ти дней.

XVI. Общедоступные источники персональных данных сотрудников Управления

46. В целях информационного обеспечения в Управлении могут создаваться общедоступные источники персональных данных сотрудников (далее -справочники), в которых с письменного согласия субъекта персональных данных включается его фамилия, имя, отчество, сведения о занимаемой им должности, номер служебного телефона, иные персональные данные, предоставленные субъектом персональных данных.

47. Форматирование, ведение и иные действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных, содержащихся в справочниках, а также получение письменного согласия субъекта персональных данных осуществляются подразделениями предприятия, ответственными за ведение каждого справочника.

XVII. Ответственность за нарушение требований, регулирующих получение, обработку и хранение персональных данных сотрудника

48. Лица, виновные в нарушении требований, регулирующих получение, обработку и хранение персональных данных сотрудника несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

49. Персональная ответственность — одно из главных требований к организации функционирования системы защиты персональной информации и обязательное условие обеспечения эффективности этой системы:

- руководитель, разрешающий доступ сотрудника к персональным данным несет персональную ответственность за данное разрешение;

- каждый сотрудник несет единоличную ответственность за сохранность носителей персональных данных и соблюдение конфиденциальности информации;

- сотрудник Управления, предоставивший работодателю подложные документы или заведомо ложные сведения о себе, либо своевременно не сообщивший об изменениях персональных данных, несет дисциплинарную ответственность, вплоть до увольнения;

- лица, виновные, в нарушении условий использования средств защиты информации или нарушении режима защиты персональных данных, несут ответственность в соответствии с законодательством Российской Федерации.

ОБЯЗАТЕЛЬСТВО

о неразглашении конфиденциальной информации (персональных данных), не содержащих сведений, составляющих государственную тайну

(ФИО государственного гражданского служащего Курганской области)

исполняющий (ая) должностные обязанности по занимаемой должности

предупрежден(а), что на период исполнения должностных обязанностей в соответствии с должностным регламентом, мне будет предоставлен допуск к конфиденциальной информации (персональным данным), не содержащих сведений, составляющих государственную тайну. Настоящим добровольно принимаю на себя обязательства:

1. Не разглашать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
2. Не передавать и не раскрывать третьим лицам конфиденциальные сведения, которые мне доверены (будут доверены) или станут известными в связи с выполнением должностных обязанностей.
3. В случае попытки третьих лиц получить от меня конфиденциальные сведения, сообщать непосредственному руководителю.
4. Не использовать конфиденциальные сведения с целью получения выгоды.
5. Выполнять требования нормативных правовых актов, регламентирующих вопросы защиты конфиденциальных сведений.
6. В течение года после прекращения права на доступ к конфиденциальным сведениям не разглашать и не передавать третьим лицам известные мне конфиденциальные сведения.

Я предупрежден(а), что в случае нарушения данного обязательства буду привлечен(а) к дисциплинарной и/или иной ответственности в соответствии с законодательством Российской Федерации.

_____

"_____"_____20___г.

Приложение 2
к приказу Управления по физической культуре, спорту и туризму Курганской области
от « 25 » февраля 2013 года № 40
«Об утверждении Положения об обработке персональных данных в Управлении по физической культуре, спорту и туризму Курганской области»

Список должностей государственных гражданских служащих Управления по физической культуре, спорту и туризму Курганской области, уполномоченных на обработку персональных данных и (или) имеющих доступ к персональным данным

1. Начальник Управления по физической культуре, спорту и туризму Курганской области
2. Заместитель начальника Управления - заведующий сектором организационного обеспечения и кадров
3. Заместитель начальника Управления- заведующий сектором туризма и аналитической работы
4. Начальник отдела финансово-экономического анализа и отчетности — главный бухгалтер
5. Заведующий сектором физической культуры и спорта
6. Главный специалист сектора организационного обеспечения и кадров
7. Ведущий специалист сектора организационного обеспечения и кадров
8. Ведущий специалист отдела финансово-экономического анализа и отчетности
9. Ведущий специалист отдела финансово-экономического анализа и отчетности
10. Ведущий специалист отдела финансово-экономического анализа и отчетности
11. Бухгалтер отдела финансово-экономического анализа и отчетности
12. Оператор ЭВМ сектора организационного обеспечения и кадров

Приложение 3
к приказу Управления по физической культуре,
спорту и туризму Курганской области
от « 25 » февраля 2013 года № 40
«Об утверждении Положения об обработке
персональных данных в Управлении по
физической культуре, спорту и туризму
Курганской области»

Список информационных систем персональных данных Управления по физической культуре, спорту и туризму Курганской области, включая перечень информации содержащейся в этих информационных системах

1. Информационная система «Учет труда и заработной платы АМБа», включающая:

фамилию, имя, отчество субъекта персональных данных;

дату рождения субъекта персональных данных;

место рождения субъекта персональных данных;

серию и номер основного документа, удостоверяющего личность субъекта персональных данных;

сведения о дате выдачи указанного документа и выдавшем его органе;

адрес места жительства субъекта персональных данных;

почтовый адрес субъекта персональных данных;

телефон субъекта персональных данных;

ИНН субъекта персональных данных;

табельный номер субъекта персональных данных;

должность субъекта персональных данных;

номер приказа и дату приема на работу (увольнения) субъекта персональных данных;

номер страхового свидетельства государственного пенсионного страхования субъекта персональных данных.

2. Информационная система «1С: Предприятие 8.0», включающая:

фамилию, имя, отчество субъекта персональных данных;

дату рождения субъекта персональных данных;

место рождения субъекта персональных данных;

серию и номер основного документа, удостоверяющего личность субъекта персональных данных;

сведения о дате выдачи указанного документа и выдавшем его органе;

адрес места жительства субъекта персональных данных;

почтовый адрес субъекта персональных данных;

телефон субъекта персональных данных;

ИНН субъекта персональных данных;

табельный номер субъекта персональных данных;

должность субъекта персональных данных.

Приложение 4
к приказу Управления по физической культуре,
спорту и туризму Курганской области
от « 25 » февраля 2013 года № 40
«Об утверждении Положения об обработке
персональных данных в Управлении по
физической культуре, спорту и туризму
Курганской области»

ИНСТРУКЦИЯ
по организации парольной защиты в информационной системе
Управления по физической культуре, спорту и туризму Курганской области

1. Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия пароля пользователя информационной системы Управления по физической культуре, спорту и туризму Курганской области (далее — Управление), а также контроль за действиями пользователя информационной системы Управления при работе с паролем.

2. Пароль пользователя информационной системы генерирует и выдает оператор ЭВМ сектора организационного обеспечения и кадров с учетом следующих требований:

1) длина пароля должна быть не менее 8 символов;

2) в наборе символов пароля должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры или специальные символы (@, #, $, %, & и т. п.);

3) пароль не должен включать в себя легко вычисляемые сочетания символов (имя, фамилию, наименование рабочей станции в локальной вычислительной сети Управления и т. д.), а также общепринятые сокращения (user, password и т. п.);

4) при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях

5) пользователь информационной системы Управления не имеет права сообщать пароль другим лицам, кроме ситуаций, указанных в пунктах 5 и 6.

3. Владелец пароля должен быть ознакомлен под роспись с настоящей Инструкцией и предупрежден об ответственности за использование пароля, не соответствующего указанным выше требованиям, а также за разглашение информации о пароле.

4. Ответственность за централизованное формирование и распределение паролей, соответствие их перечисленным выше требованиям несет оператор ЭВМ сектора организационного обеспечения и кадров.

5. В случае отсутствия пользователя информационной системы Управления на рабочем месте, право использования его пароля в служебных целях для входа в информационную систему Управления имеют руководитель структурного подразделения Управления, в котором работает владелец пароля и оператор ЭВМ сектора организационного обеспечения и кадров.

6. Оператор ЭВМ сектора организационного обеспечения и кадров имеет право использовать пароль пользователя информационной системы Управления для настройки и отладки программного обеспечения.

7. Плановая смена пароля пользователя информационной системы

Управления проводится не реже раза в год.

8. Внеплановая смена пароля пользователя информационной системы Управления (в случае увольнения, перехода в другое подразделение Управления и т. п.) производится оператором ЭВМ сектора организационного обеспечения и кадров после окончания последнего сеанса работы данного пользователя в информационной системе Управления.

9. Внеплановая смена паролей всех пользователей информационных систем Управления производится в случае увольнения, перехода в другое подразделение Управления и т. п. оператора ЭВМ сектора организационного обеспечения и кадров.

10. В случае компрометации пароля пользователя информационной системы Управления должны быть немедленно предприняты меры, указанные в пунктах 8 и 9 настоящей Инструкции в зависимости от должности владельца скомпрометированного пароля.

11. Хранение пользователем информационной системы Управления набора символов своего пароля на бумажном носителе допускается в личном сейфе, в сейфе главного специалиста сектора организационного обеспечения и кадров или руководителя подразделения Управления, в котором работает владелец пароля.

12. Повседневный контроль за действиями пользователя информационной системы Управления при работе с паролем, соблюдением порядка его смены, хранения и использования возлагается на оператора ЭВМ сектора организационного обеспечения и кадров.

Приложение 5
к приказу Управления по физической культуре,
спорту и туризму Курганской области
от « 25 » февраля 2013 года № 40
«Об утверждении Положения об обработке
персональных данных в Управлении по
физической культуре, спорту и туризму
Курганской области»

»

ИНСТРУКЦИЯ
по организации антивирусной защиты в информационной системе Управления по физической культуре, спорту и туризму Курганской области

1. Настоящая инструкция определяет требования к организации защиты информационной системы Управления по физической культуре, спорту и туризму Курганской области (далее – Управление) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность работников Управления, эксплуатирующих и сопровождающих информационную систему Управления, за их выполнение.

2. В информационной системе Управления допускается использование только лицензионного антивирусного программного обеспечения, успешно прошедшего процедуру оценки соответствия требованиям ФСТЭК и ФСБ.

3. Антивирусная защита информационной системы Управления состоит в установке, настройке, обновлении антивирусного программного обеспечения на рабочей станции (сервере) и проведении мероприятий антивирусного контроля.

4. Обновление антивирусных баз осуществляется не реже одного раза в день.

5. При выполнении антивирусного контроля носителей информации информационной системы Управления (как стационарных, так и съемных) антивирусному контролю подлежит любая информация (загрузочные записи (сектора), исполняемые файлы, текстовые файлы любых форматов, файлы данных, прочие файлы).

6. Антивирусный контроль рабочей станции (сервера) производится ежедневно в автоматическом режиме.

7. Установка и настройка антивирусного программного обеспечения на рабочей станции (сервере) информационной системе Управления осуществляется оператором ЭВМ сектора организационного обеспечения и кадров в соответствии с руководствами по применению используемых антивирусных средств.

8. Устанавливаемое (изменяемое, обновляемое) на рабочей станции (сервере) программное обеспечение должно быть предварительно проверено оператором ЭВМ сектора организационного обеспечения и кадров.

9. Антивирусный контроль входящей информации проводится в момент непосредственного обращения к ней перед началом работы (после установки съемного носителя информации: гибкого магнитного диска, CD-, DVD-диска, флеш-накопителя и т. п.).

10. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.) пользователь информационной системы Управления обязан поставить

об этом в известность оператора ЭВМ сектора организационного обеспечения и кадров Оператор ЭВМ сектора организационного обеспечения и кадров обязан провести внеочередной антивирусный контроль рабочей станции.

11. В случае обнаружения при проведении антивирусного контроля заражения компьютерным вирусом пользователь информационной системы Управления обязан:

1) приостановить работу в информационной системе Управления;

2) немедленно поставить в известность о факте обнаружения заражения компьютерным вирусом оператора ЭВМ сектора организационного обеспечения и кадров Управления.

12. В случае обнаружения при проведении антивирусного контроля заражения компьютерным вирусом или получения соответствующего сообщения от пользователя оператор ЭВМ сектора организационного обеспечения и кадров обязан:

1) поставить в известность о факте обнаружения заражения компьютерным вирусом пользователя информационной системы Управления, а также других пользователей, использующих зараженные файлы в работе;

2) совместно с пользователем информационной системы Управления провести анализ необходимости дальнейшего использования зараженных файлов;

3) провести «лечение» или уничтожение зараженных файлов.

13. Ответственность за соблюдение требований настоящей Инструкции возлагается на пользователя информационной системы Управления.

14. Контроль за состоянием антивирусной защиты в информационной системе Управления, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции осуществляется оператором ЭВМ сектора организационного обеспечения и кадров.

Приложение 6
к приказу Управления по физической культуре,
спорту и туризму Курганской области
от « 25 » февраля 2013 года № 40
«Об утверждении Положения об обработке
персональных данных в Управлении по
физической культуре, спорту и туризму
Курганской области»

ИНСТРУКЦИЯ
по организации резервного копирования и восстановления программного обеспечения, баз данных в информационной системе Управления по физической культуре, спорту и туризму Курганской области

1. Настоящая Инструкция по организации резервного копирования и восстановления программного обеспечения, баз данных в информационной системе Управления по физической культуре, спорту и туризму Курганской области (далее – Управление) разработана с целью определения порядка:

- резервного копирования информационной системы Управления для последующего восстановления работоспособности при полной или частичной потере данных, вызванной сбоями или отказами аппаратного или программного обеспечения, ошибками пользователей, чрезвычайными обстоятельствами (пожаром, стихийными бедствиями и т. д.);
- восстановления данных информационной системы Управления в случае возникновения такой необходимости;
- работы должностных лиц Управления, связанной с резервным копированием и восстановлением данных.

2. Резервному копированию подлежит информация следующих основных категорий:

- персональная информация пользователя информационной системы Управления (каталог с документами на рабочей станции);
- групповая информация пользователей информационной системы Управления (общие каталоги с документами на файловом сервере);
- данные информационных систем персональных данных Управления.

3. Создание резервных копий производится в автоматическом режиме с использованием специализированного программного обеспечения, исходя из перечня резервируемых данных информационной системы Управления.

4. Резервные копии хранятся в виде архивных файлов (архивов):

- ежедневный архив (архив, сделанный в конце рабочего дня);
- еженедельный архив (архив, сделанный в последний день недели);
- ежемесячный архив (архив, сделанный в последний день месяца).

5. О выявленных попытках несанкционированного доступа к архивам, а также иных нарушениях информационной безопасности произошедших в процессе резервного копирования, специалист сектора организационного обеспечения и кадров с

сообщает председателю постоянно действующей технической комиссии по защите информации (далее — ПДТК) служебной запиской в течение рабочего дня после обнаружения указанного события.

6. Создание резервных копий происходит путем копирования и архивирования файлов и папок данных информационной системы Управления.

7. Контроль результатов всех процедур резервного копирования осуществляется специалистом сектора организационного обеспечения и кадров.

8. На протяжении периода времени, когда резервное копирование находится в аварийном состоянии, процессе настройки, осуществляется ежедневное копирование данных информационной системы Управления, подлежащих резервному копированию, с использованием средств операционной системы сервера, располагающего необходимым объемом дискового пространства для их хранения.

9. Любое восстановление данных информационной системы Управления из резервных копий, не вызванное необходимостью экстренного восстановления, связанной с потерей работоспособности информационной системы Управления или ее компонентов, выполняется на основании заявки руководителя структурного подразделения Управления, работнику которого требуется восстановление утраченных данных. (Приложение 1. Форма заявки).

10. Заявка руководителя структурного подразделения Управления, работнику которого требуется восстановление данных информационной системы Управления, оформляется на имя специалиста сектора организационного обеспечения и кадров. Заявка хранится у специалиста сектора организационного обеспечения и кадров.

11. Действия по восстановлению данных информационной системы Управления из резервных копий фиксируются специалистом сектора организационного обеспечения и кадров в «Журнале учета нештатных ситуаций».

Приложение к пункту 9 Инструкции
по организации резервного
копирования и восстановления
программного обеспечения, баз
данных в информационной
системе
Управления по физической
культуре, спорту и туризму
Курганской области

ЗАЯВКА
на восстановление информации из резервных копий

_____

(наименование отдела, сектора)

В связи с _____

_____

_____

(описание причины восстановления)

Прошу произвести восстановление следующей информации

_____

(наименование файла с полным указанием места нахождения)

Руководитель структурного
подразделения Управления

«____»_____ 20___ г. _____/_____
(подпись) (расшифровка)