ДЕПАРТАМЕНТ ПО КУЛЬТУРЕ ТОМСКОЙ ОБЛАСТИ

ПРИКАЗ

20.05.2020 № 015/01-09

Об утверждении документов, направленных на выполнение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

В целях исполнения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», предъявляемых к Операторам информационных систем персональных данных

ПРИКАЗЫВАЮ:

1. Утвердить:

1) положение об обработке персональных данных в информационных системах персональных данных Департамента по культуре Томской области, согласно приложению № 1 к настоящему приказу;

2) правила работы с обезличенными персональными данными, согласно приложению № 2 к настоящему приказу;

3) порядок доступа государственных гражданских служащих Департамента по культуре Томской области в помещения, в которых ведется обработка информации ограниченного доступа, и расположены средства криптографической защиты информации, согласно приложению № 3 к настоящему приказу;

4) перечень информационных систем персональных данных Департамента по культуре Томской области, согласно приложению № 4 к настоящему приказу;

5) типовое обязательство государственного гражданского служащего Томской области, занимающего должность государственной гражданской службы Томской области в Департаменте по культуре Томской области, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта прекратить обработку персональных данных, ставших не известными ему в связи с исполнением должностных обязанностей, согласно приложению № 5 к настоящему приказу;

6) положение по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Департамента по культуре Томской области, согласно приложению № 6 к настоящему приказу;

7) перечень должностей государственных гражданских служащих Томской области, состоящих в штате Департамента по культуре Томской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, согласно приложению № 7 к настоящему приказу.

2. Назначить ответственным за организацию обработки персональных данных в Департаменте по культуре Томской области (далее - Департамент), председателя комитета кадровой политики и организационно правовой работы Департамента Шагову Е.М.

3. Китлер О.В. ознакомить под подпись должностных лиц, осуществляющих обработку персональных данных в Департаменте с настоящим приказом.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник Департамента П.Л.Волк

О.В. Китлер

Приложение № 1
к приказу
Департамента по культуре Томской области
от 20.05. 2020 № 015/01-09

Положение
об обработке персональных данных в информационных системах персональных данных Департамента по культуре Томской области

1. Общие положения

1. Настоящим Положение об обработке персональных данных (далее - Положение) определяет порядок получения, хранения, обработки, комбинирования, передачи и любого другого исполнения персональных данных, обрабатываемых в информационных системах (далее - ИС) Департамента по культуре Томской области (далее – Департамент или Оператор).

2. Настоящее Положение разработано в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

3. Для целей настоящего Положения используются понятия, указанные в статье 3 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2. Получение, обработка и защита персональных данных

Порядок получения персональных данных

4. Персональные данные (далее - ПДн) могут быть получены Департаментом только способами, предусмотренными действующим законодательством Российской Федерации. При этом получение письменного согласия, а также разъяснение субъекту ПДн о целях, предполагаемых источниках и способах получения персональных данных, характере подлежащих получению персональных данных и последствиях отказа субъекта ПДн дать письменное согласие на их получение, возлагается на Оператора. Типовая форма согласия на обработку персональных данных приведена в приложении № 1 к настоящему Положению. В случае отказа субъекта ПДн предоставить свои ПДн ему должны быть разъяснены юридические последствия такого отказа. Типовая форма разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональных данных приведена в приложении № 2 к настоящему Положению.

5. Сотрудники Департамента имеют право получать только те ПДн, которые необходимы им для выполнения своих служебных обязанностей.

6. Сотрудники Департамента, получающие персональные данные субъекта ПДн, обязаны соблюдать режим конфиденциальности.

Порядок обработки персональных данных

7. Обработка персональных данных может осуществляться только в заявленных целях.

8. При определении объема и содержания обрабатываемых персональных данных, Оператор должен руководствоваться Конституцией Российской Федерации, Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и иными нормативными правовыми актами в области защиты персональных данных.

9. При принятии решений, затрагивающих интересы субъекта ПДн, Департамент не имеет права основываться на персональных данных субъекта ПДн, полученных исключительно в результате их автоматизированной обработки или электронно.

Порядок защиты персональных данных

10. Защита персональных данных субъекта ПДн от неправомерного их использования или утраты должна быть обеспечена Оператором за счет его средств в порядке, установленном нормативными правовыми актами Российской Федерации в области защиты персональных данных.

11. Оператор обязан при обработке персональных данных субъектов ПДн:

1) принимать необходимые организационные и технические меры для защиты персональных данных от несанкционированного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий;

2) соблюдать порядок получения, учета и хранения персональных данных субъектов ПДн;

3) применять технические средства охраны и сигнализации;

4) взять со всех сотрудников, связанных с получением, обработкой и защитой персональных данных субъектов ПДн, типовое обязательство сотрудника Департамента о неразглашении информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну и о прекращении обработки такой информации в случае расторжения с ним служебного контракта или трудового договора;

5) привлекать к дисциплинарной ответственности сотрудников, виновных в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъектов ПДн;

6) запретить допуск к персональным данным субъектов ПДн сотрудников Департамента, не включенных в «Перечень лиц, имеющих доступ в помещения, в которых расположены технические средства информационных систем, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах Департамента по культуре Томской области».

12. Защита доступа к электронной базе данных, содержащей персональные данные субъектов ПДн, должна обеспечиваться путем использования сертифицированных программных и программно-аппаратных средств защиты информации, предотвращающих несанкционированный доступ третьих лиц к персональным данным субъектов ПДн.

13. Копировать и делать выписки персональных данных субъектов ПДн разрешается исключительно в служебных целях с письменного разрешения начальника Департамента.

14. Субъекты ПДн не должны отказываться от прав на сохранение и защиту своих персональных данных.

3. Хранение персональных данных

15. Сведения о субъектах ПДн в Департаменте на материальных носителях должны храниться в специально оборудованных шкафах и сейфах, которые запираются и (или) опечатываются. Ключи от шкафов и сейфов, в которых хранятся сведения о субъектах ПДн, находятся у ответственных сотрудников.

16. Материальные носители ПДн, обработка которых осуществляется в различных целях, должны храниться отдельно. Для обработки различных категорий ПДн, осуществляемой без использования средств автоматизации, для каждой категории ПДн должен использоваться отдельный материальный носитель.

17. Обязанности по организации хранения сведений о субъектах ПДн, заполнения, хранения и выдачи документов, содержащих персональные данные, в ИС Департамента возлагаются на Ответственного за обработку и защиту информации.

18. Съемные электронные носители, на которых хранятся резервные копии персональных данных субъектов ПДн, должны быть промаркированы и учтены в Журнале регистрации, учета и выдачи машинных носителей информации.

19. В процессе хранения персональных данных субъектов ПДн необходимо обеспечивать контроль за достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

4. Передача персональных данных

20. При передаче персональных данных субъекта ПДн Оператор должен соблюдать требования, установленные законами Российской Федерации, нормативными правовыми актами ФСБ России и ФСТЭК России.

5. Уничтожение персональных данных

21. Обрабатываемые ПДн подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законодательством Российской Федерации в сфере обработки ПДн.

22. Уничтожение документов, содержащих ПДн, осуществляется в порядке, предусмотренном архивным законодательством Российской Федерации.

23. При необходимости уничтожения персональных данных Оператор должен руководствоваться следующими требованиями:

1) уничтожение ПДн в ИС Департамента осуществляется комиссией по проведению мероприятий по защите информации;

2) бумажные носители ПДн должны уничтожаться при помощи специального оборудования (измельчителя бумаги);

3) персональные данные, представленные в электронном виде, должны уничтожаться специализированным программным обеспечением, гарантирующим предотвращение восстановления удаленных данных;

4) после окончания процедуры удаления персональных данных комиссией по проведению мероприятий по защите персональных данных должен быть составлен акт уничтожения персональных данных.

6. Реагирование на запросы субъектов ПДн и их законных представителей

24. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (приложение № 3 к настоящему Положению).

25. При рассмотрении запросов, поступающих от субъектов ПДн и их законных представителей, Департамент руководствуется Правилами рассмотрения запросов (приложение № 4 к настоящему Положению).

26. Все обращения, поступающие от субъектов ПДн и их законных представителей, должны регистрироваться ответственным за обработку и защиту Информации в соответствующем журнале (приложение № 5 к настоящему Положению).

27. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных или его представителя, а в случае, если обращение субъекта персональных данных или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган (приложение № 6 и № 7 к настоящему Положению).

7. Ответственность за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъекта ПДн

28. Лица, виновные в нарушении требований федеральных законов, несут предусмотренную законодательством Российской Федерации ответственность.

29. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных федеральными законами, а также нарушения требований к защите персональных данных подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

Приложение № 1
к положению об обработке персональных данных в информационных системах персональных данных Департамента по культуре Томской области

Типовая форма согласия на обработку персональных данных
(в соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»)

Я,_____,
(Фамилия, имя, отчество (последнее - при наличии)
паспорт серия _____ № _____ выдан _____
_____,
(когда и кем)
проживающий(ая) по адресу: _____,
свободно, своей волей и в своем интересе даю согласие оператору, расположенному по адресу:
_____
на обработку моих персональных данных: _____
_____
_____.

Согласен на осуществление с указанными выше персональными данными следующих действий: сбор, систематизация, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в т.ч. передача), обезличивание, блокирование, уничтожение, для реализации полномочий, возложенных на Департамент по культуре Томской области действующим законодательством.

Я ознакомлен, что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока государственной гражданской службы в Департаменте по культуре Томской области;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных, Департамент по культуре Томской области вправе продолжить обработку персональных данных без моего согласия при наличии оснований, указанных в пунктах 2-11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

4) мои персональные данные, предоставляемые третьим лицам, будут обрабатываться только в целях осуществления и выполнения, возложенных законодательством Российской Федерации на Департамент по культуре Томской области функций, полномочий и обязанностей.

Дата начала обработки персональных данных: _____
(число, месяц, год)
_____ / _____
(подпись) (Фамилия и инициалы)

Приложение № 2
к положению об обработке персональных данных в информационных системах персональных данных Департамента по культуре Томской области

Типовая форма
разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Уважаемый (-ая), _____!
(имя, отчество (последнее - при наличии) субъекта персональных данных)

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152- ФЗ «О персональных данных» уведомляем Вас, что обязанность предоставления Вами персональных данных установлена _____
_____
_____.
(реквизиты и наименование нормативных правовых актов)

В случае отказа Вами предоставить свои персональные данные, оператор не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям _____
_____
_____.
(перечисляются юридические последствия для субъекта персональных данных, то есть случаи возникновения, изменения или прекращения личных либо имущественных прав граждан или случаи иным образом затрагивающие его права, свободы и законные интересы)

В соответствии с законодательством в области персональных данных Вы имеете право:

- на получение сведений об операторе, о месте его нахождения, о наличии у оператора своих персональных данных, а также на ознакомление с такими персональными данными;
- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- на получение при обращении или при направлении запроса информации, касающейся обработки своих персональных данных;
- на обжалование действия или бездействия оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

_____	_____	_____
(дата)	(подпись)	(фамилия и инициалы оператора)

Приложение № 3
к положению об обработке персональных данных в информационных системах персональных данных Департамента по культуре Томской области

В Департамент по культуре Томской области

_____
(Фамилия, имя, отчество

_____
(последнее - при наличии) заявителя)

_____

_____

_____
(наименование и реквизиты документа, удостоверяющего личность заявителя)

ЗАЯВЛЕНИЕ

Прошу предоставить мне для ознакомления обрабатываемую Вами информацию, составляющую мои персональные данные, а также:

- указать основания, цели и источник получения такой информации;
- указать способы и сроки ее обработки (в том числе сроки хранения);
- предоставить сведения о лицах, которые имеют к ней доступ (которым может быть предоставлен такой доступ) на основании договора с Департаментом по культуре Томской области или на основании федерального закона;
- предоставить информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- указать наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению Департамента по культуре Томской области, если обработка поручена или будет поручена такому лицу;
- предоставить сведения о том, какие юридические последствия для меня может повлечь её обработка.

В случае отсутствия такой информации прошу Вас уведомить меня об этом.

_____ _____

(дата) (фамилия, имя, отчество (последнее - при наличии))

Приложение № 4
к положению об обработке персональных данных в информационных системах персональных данных Департамента по культуре Томской области

ПРАВИЛА
рассмотрения запросов субъектов персональных данных или их представителей по поводу обработки их персональных данных в информационных системах Департамента по культуре Томской области

1. Общие положения

1. Настоящие Правила рассмотрения запросов субъектов персональных данных или их представителей по поводу обработки их персональных данных в информационных системах Департамента по культуре Томской области (далее - Правила) разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и определяют порядок обработки поступающих в Департамент по культуре Томской области (далее - Департамент) обращений субъектов персональных данных (далее - ПДн) или их законных представителей по поводу обработки их ПДн в информационных системах (далее - ИС) Департамента.

2. Права субъектов персональных данных

2. В соответствии с действующим законодательством субъект ПДн или его законный представитель имеет право на получение при обращении или при получении запроса от субъекта персональных данных или его законного представителя информации, касающейся обработки его персональных данных, в том числе содержащей:

подтверждение факта обработки ПДн оператором;

правовые основания и цели обработки ПДн;

применяемые оператором способы обработки ПДн;

наименование и место нахождения оператора, сведения о лицах (за исключением сотрудников оператора), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с оператором или на основании федерального закона;

обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

сроки обработки ПДн, в том числе сроки их хранения;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;

иные сведения, предусмотренные Федеральным законом от 27 июля 2007 года № 152-ФЗ «О персональных данных» или другими федеральными законами.

3. Право субъекта персональных данных на доступ к своим персональным данным ограничивается в случае, если:

обработка ПДн, включая ПДн, полученные в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, осуществляется в целях обороны страны, безопасности государства и охраны правопорядка;

обработка ПДн осуществляется органами, осуществившими задержание субъекта ПДн по подозрению в совершении преступления, либо предъявившими субъекту ПДн обвинение по уголовному делу, либо применившими к субъекту ПДн меру пресечения до предъявления обвинения, за исключением предусмотренных уголовно-процессуальным законодательством Российской Федерации случаев, если допускается ознакомление подозреваемого или обвиняемого с такими ПДн;

обработка ПДн осуществляется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;

доступ субъекта ПДн к его ПДн нарушает права и законные интересы третьих лиц;

обработка ПДн осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства.

4. Департамент, как оператор ПДн, обязан предоставить безвозмездно субъекту ПДн или его представителю возможность ознакомления с ПДн, относящимися к этому субъекту. В срок, не превышающий семи рабочих дней со дня предоставления субъектом ПДн или его представителем сведений, подтверждающих, что ПДн являются неполными, неточными или неактуальными, Ответственный за обработку и защиту Информации обязан организовать внесение в персональные данные необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом ПДн или его представителем сведений, подтверждающих, что такие ПДн являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Ответственный за обработку и защиту Информации обязан организовать уничтожение таких ПДн (в случае если иное не предусмотрено федеральными законами). Ответственный за обработку и защиту Информации обязан уведомить субъекта ПДн или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым ПДн этого субъекта были переданы. Если субъект персональных данных считает, что Департамент осуществляет обработку его персональных данных с нарушением требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие Департамента в уполномоченном органе по защите прав субъектов персональных данных или в судебном порядке.

5. Субъект персональных данных имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

3. Порядок работы с обращениями субъектов

6. Ответственный за обработку и защиту Информации может принимать запросы в следующем порядке:

сотрудники Департамента, принявшие от субъектов обращение, передают поступившее обращение начальнику своего подразделения в течение 1 (одного) часа после поступления обращения;

в случае отсутствия начальника подразделения на рабочем месте обращение должно быть передано напрямую ответственному за обработку и защиту Информации;

сотрудники Департамента, обращающиеся за разъяснением об обработке их ПДн, передают свое обращение начальнику своего подразделения;

начальники подразделений передают обращение ответственному за обработку и защиту Информации.

7. Запрос или обращение субъекта по вопросу обработки ПДн должен содержать номер основного документа, удостоверяющего личность субъекта ПДн или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта ПДн в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки ПДн оператором, подпись субъекта ПДн или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

8. Ответственный за обработку и защиту Информации регистрирует обращение в журнале учета обращений субъектов ПД по вопросам обработки их ПДн в ИС, после чего:

рассматривает обращение по существу, привлекая в случае необходимости сотрудников любых подразделений Департамента;

запрашивает первичные документы и пояснения (в том числе письменные объяснения) сотрудников по существу обращения (срок предоставления - один рабочий день). Начальники структурных подразделений несут ответственность за своевременность и полноту предоставления сведений ответственному за обработку и защиту Информации;

при необходимости инициирует и контролирует внесение необходимых изменений в ПДн субъекта либо их удаление.

9. Не позднее семи рабочих дней со дня регистрации обращения ответственный за обработку и защиту Информации готовит ответ на обращение.

10. Подготовленный и согласованный ответ вместе со всеми имеющимися материалами ответственный за обработку и защиту Информации передает на подпись начальнику Департамента.

11. Срок предоставления ответа на обращение субъекта ПДн или его законного представителя устанавливается в соответствии с пунктом 1 статьи 20 Федерального закона от 27 июля 2007 года № 152-ФЗ «О персональных данных» не более тридцати дней с момента получения обращения.

12. После подписания начальником Департамента ответ на обращение отправляется субъекту заказным письмом или передается субъекту лично под подпись.

13. В случае отказа в предоставлении информации субъекту ПДн при получении обращения ответственный за обработку и защиту информации готовит в письменной форме мотивированный ответ, содержащий ссылку на положение части 5 статьи 14 Федерального закона от 27 июля 2007 года № 152-ФЗ «О персональных данных» или иного федерального закона, являющегося основанием для такого отказа, в срок не превышающий семи рабочих дней с момента получения обращения субъекта ПДн.

Приложение 5
к положению об обработке персональных данных в информационных системах персональных данных Департамента по культуре Томской области

Форма

ЖУРНАЛ № _____
учета обращений субъектов персональных данных по вопросам обработки их персональных данных в информационных системах Департамента по культуре Томской области

Начат « ___ » _____ 20___ г. На _____ листах
Окончен « ___ »_____ 20___ г.

_____ _____
(Фамилия, имя, отчество (последние – при наличии) ответственного лица за ведение журнала) (подпись)

№ п/п	Дата Обращения	Сведения о запрашивающем лице	Краткое содержание обращения	Отметка о предоставлении или отказе в предоставлении персональных данных (предоставлено/отказано)	Дата передачи/отказа в предоставлении персональных данных	Подпись запрашивающего лица	Подпись ответственного сотрудника
1	2	3	4	5	6	7	8

Приложение № 6
к положению об обработке персональных данных в информационных системах персональных данных Департамента по культуре Томской области

УВЕДОМЛЕНИЕ
об устранении допущенных нарушений

Настоящим уведомлением сообщаем Вам, что допущенные при обработке персональных данных нарушения в информационных системах Департамента по культуре Томской области, а именно: _____
(указать допущенные нарушения)
_____,
устранены.

_____	_____	_____
(должность)	(подпись)	(Фамилия и инициалы)

_____ 20___ г..

Приложение № 7
к положению об обработке персональных данных в информационных системах персональных данных Департамента по культуре Томской области

УВЕДОМЛЕНИЕ
об уничтожении персональных данных

№ _____ « ___ » _____ 20__ г.

На № _____ от _____

_____
(Фамилия, имя, отчество (последнее - при наличии) субъекта персональных данных)

Настоящим уведомлением сообщаем Вам, что в связи с достижением _____ 20___ года цели обработки Ваших персональных данных, а именно: _____
_____
_____
_____
(указать цель обработки персональных данных)

_____ 20___ года, в соответствии с требованиями статьи 21 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Ваши персональные данные в информационной системе Департамента по культуре Томской области уничтожены.

_____	_____	_____
(должность)	(подпись)	(Фамилия и инициалы)

Приложение № 2
к приказу
Департамента по культуре
Томской области
от 20.05. 2020 № 015/01-09

ПРАВИЛА
работы с обезличенными персональными данными

1. Настоящие Правила работы с обезличенными персональными данными (далее - Правила) в Департаменте по культуре Томской области (далее - Департамент) разработаны в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 № 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».

2. Настоящие Правила определяют порядок работы с обезличенными персональными данными в Департаменте.

3. Термины «персональные данные», «обработка персональных данных», «обезличивание персональных данных» используются в настоящих Правилах в значениях, определенных Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных».

4. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса информационных систем персональных данных Департамента и по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

5. Способы обезличивания при условии дальнейшей обработки персональных данных:

уменьшение перечня обрабатываемых сведений;

замена части сведений идентификаторами;

обобщение - понижение точности некоторых сведений;

понижение точности некоторых сведений (например, "Место жительства" может состоять из страны, индекса, города, улицы, дома и квартиры, а может быть указан только город);

деление сведений на части и обработка в разных информационных системах;

другие способы.

6. Способом обезличивания в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

7. Перечень должностей государственной гражданской службы, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных утверждается приказом Департамента.

8. Начальник Департамента принимает решение о необходимости обезличивания персональных данных.

9. Руководители структурных подразделений, непосредственно осуществляющие обработку персональных данных, готовят предложения по обезличиванию персональных данных, обоснование такой необходимости и способ обезличивания.

10. Сотрудники Департамента, обслуживающие базы данных с персональными данными, совместно с ответственным за организацию обработки персональных данных, осуществляют непосредственное обезличивание выбранным способом.

11 .Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

12. Обезличенные персональные данные могут обрабатываться с использованием и без использования средств автоматизации.

13. При обработке обезличенных персональных данных с использованием средств автоматизации необходимо соблюдение:

парольной политики;

антивирусной политики;

правил работы со съемными носителями (если они используются);

правил резервного копирования;

правил доступа в помещения, где расположены элементы информационных систем.

При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

правил хранения бумажных носителей;

правил доступа к ним и в помещения, где они хранятся.

Приложение № 3
к приказу
Департамента по культуре
Томской области
от 20.05. 2020 № 015/01-09

ПОРЯДОК
доступа государственных гражданских служащих Департамента по культуре Томской области в помещения, в которых ведется обработка информации ограниченного доступа, и расположены средства криптографической защиты информации

1. Настоящий Порядок доступа сотрудников Департамента по культуре Томской области (далее - Департамента) в помещения, в которых ведется обработка информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, и расположены средства криптографической информации (далее - Порядок) разработан в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и другими нормативными правовыми актами.

2. Обеспечение безопасности Информации от уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении Информации достигается, в том числе установлением правил доступа в помещения, где обрабатывается Информация с использованием и/или без использования средств автоматизации.

3. Размещение информационных систем, в которых обрабатывается Информация, должно осуществляться в пределах контролируемой зоны, границы которой зафиксированы распоряжением начальника Департамента. Для помещений, в которых обрабатывается Информация и расположены средства криптографической защиты информации (далее - Помещения), организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей Информации и средств защиты информации, криптосредств и ключевых документов к ним, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц и просмотра ведущихся там работ.

4. В помещения, где размещены технические средства, позволяющие осуществлять обработку Информации, а также хранятся носители Информации, допускаются только сотрудники Департамента, уполномоченные на обработку Информации приказом начальника Департамента в «Перечне лиц, имеющих доступ в помещения, в которых расположены технические средства ИС, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах Департамента по культуре Томской области».

5. При оборудовании Помещений должны выполняться требования к размещению, монтажу криптосредств, а также другого оборудования, функционирующего с криптосредствами.

6. Нахождение в помещениях с информационными системами лиц, не включенных в «Перечень лиц, имеющих доступ в помещения, в которых расположены технические средства ИС, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах Департамента по культуре Томской области», возможно только в присутствии сотрудников Департамента, уполномоченного на обработку Информации. Время нахождения в помещениях ограничивается временем решения вопросов, в рамках которого возникла необходимость пребывания в помещении.

7. Сотрудники Департамента, допущенные к обработке Информации, не должны покидать Помещение, не убедившись, что доступ посторонних лиц к Информации невозможен. Запрещается оставлять материальные носители с Информации без присмотра в незапертом помещении.

8. В нерабочее время дверь каждого помещения, в котором ведется обработка Информации, закрывается на ключ. Ключ ответственный сдает/получает дежурному сотруднику охраны под подпись в журнале.

9. Помещения Департамента, в которых ведется обработка Информации и расположены средства криптографической информации, должны быть оснащены входными дверьми с замками. Кроме того, должно быть обеспечено постоянное закрытие дверей таких помещений на замок и их открытие только для санкционированного прохода, а также опечатывание помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

10. Помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации.

11. Для предотвращения просмотра извне окна Помещений должны быть защищены шторами или жалюзи.

12. Окна Помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в Помещения посторонних лиц, оборудуются металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в Помещения.

13. Внутренний контроль за соблюдением порядка доступа в помещения, проводится в порядке, определенном в плане проведения внутреннего контроля соответствия требованиям по защите, утвержденном в Департаменте. Контроль и управление физическим доступом к информационным системам и средствам криптографической защиты должны предусматривать:

1) определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены - поддерживание в актуальном состоянии «Перечня лиц, имеющих доступ в помещения, в которых расположены технические средства ИС, и доступ к обработке информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, обрабатываемой в информационных системах Департамента по культуре Томской области»;

2) санкционирование физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены - выдача ключей от помещений строго в соответствии с утвержденным перечнем лиц;

3) учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены - выдача ключей от помещений под роспись в соответствующем журнале, проверка раз в месяц данного журнала.

14. При обнаружении повреждений замков или других признаков, указывающих на возможное проникновение посторонних лиц в помещения, в которых ведется обработка Информации и расположены средства криптографической информации, эти помещения не вскрываются, а составляется акт о случившемся. При этом немедленно ставятся в известность Ответственный за обработку и защиту информации и правоохранительные органы. Одновременно принимаются меры по охране места происшествия и до прибытия работников правоохранительных органов в эти помещения никто не допускается.

15. Ответственность за соблюдение порядка доступа в помещения Департамента, в которых ведется обработка Информации и расположены средства криптографической информации, возлагается на начальника Департамента.

16. В случае нарушения настоящего Порядка сотрудники могут быть привлечены к дисциплинарной и/или иной ответственности в соответствии с законодательством Российской Федерации.

Приложение № 4
к приказу
Департамента по культуре
Томской области
от 20.05. 2020 № 015/01-09

ПЕРЕЧЕНЬ
информационных систем персональных данных Департамента по культуре Томской области

Наименование информационной системы	**Место нахождения ИС**
ВУБ-20	634069, г.Томск, пр-т Ленина, 111, Департамент по культуре Томской области, каб.1
СУФД онлайн	634069, г.Томск, пр-т Ленина, 111, Департамент по культуре Томской области, каб.7
БАРС	634069, г.Томск, пр-т Ленина, 111, Департамент по культуре Томской области, каб.7, 11
Парус бюджет 10	634069, г.Томск, пр-т Ленина, 111, Департамент по культуре Томской области, каб.7
СБИС	634069, г.Томск, пр-т Ленина, 111, Департамент по культуре Томской области, каб.1, 7
ГИС АЦК-Финансы	634069, г.Томск, пр-т Ленина, 111, Департамент по культуре Томской области, каб. 7, 9, 11, 12
Федеральный портал управленческих кадров	634069, г.Томск, пр-т Ленина, 111, Департамент по культуре Томской области, каб.1

Приложение № 5 к приказу
Департамента по культуре
Томской области
от 20.05. 2020 № 015/01-09

ТИПОВОЕ ОБЯЗАТЕЛЬСТВО
государственного гражданского служащего Томской области, замещающего должность государственной гражданской службы Томской области в Департаменте по культуре Томской области, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я,_____,
(Фамилия, имя, отчество (последнее - при наличии))
являясь государственным гражданским служащим Томской области, замещающим должность государственной гражданской службы Томской области в Департаменте по культуре Томской области и непосредственно осуществляя обработку персональных данных, ознакомлен с требованиями по соблюдению конфиденциальности обрабатываемых мною персональных данных субъектов персональных данных и обязуюсь в случае расторжения Департаментом по культуре Томской области со мной служебного контракта прекратить обработку персональных данных, ставших мне известными в связи с исполнением должностных обязанностей.

Я ознакомлен с предусмотренной действующим законодательством Российской Федерации ответственностью за нарушения неприкосновенности частной жизни и установленного Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных).

_____ 20___ г. _____ / _____
(подпись) (Фамилия и инициалы)

Приложение № 6
к приказу
Департамента по культуре
Томской области
от 20.05. 2020 № 015/01-09

ПОЛОЖЕНИЕ
по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Департамента по культуре Томской области

1. Общие положения

1. Настоящее Положение по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - Положение) разработано в соответствии с Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Положение определяет порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке, порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений, порядок приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления, порядок обучения персонала практике работы в ИСПДн, порядок проверки электронного журнала обращений к ИСПДн, порядок контроля соблюдения условий использования средств защиты информации, предусмотренные эксплуатационной и технической документацией, правила организации антивирусной защиты и парольной защиты ИСПДн, порядок охраны и допуска посторонних лиц в защищаемые помещения.

2. Порядок работы персонала ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн

2. Допуск пользователей для работы на компьютере осуществляется на основании разрешения руководителя структурного подразделения Департамента по культуре Томской области (далее - Департамент) в соответствии со списком лиц, допущенных к работе в ИСПДн.

3. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для записи и хранения информации, содержащей ПДн, разрешается использовать только учтенные носители информации.

4. Пользователь несет ответственность за правильность включения и выключения компьютера, входа в систему и все действия при работе в ИСПДн.

5. Вход пользователя в систему может осуществляться по выдаваемому ему электронному идентификатору и по персональному паролю в соответствии с Инструкцией по организации парольной защиты в информационной системе персональных данных.

6. При работе со съемными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ, установленных на компьютере. В случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения и Инструкцией по организации антивирусной защиты в информационной системе персональных данных.

7. Каждый сотрудник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки ПДн и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;

знать и строго выполнять правила работы со средствами защиты информации, установленными на компьютере;

хранить в тайне свой пароль (пароли) и с установленной периодичностью менять свой пароль (пароли);

хранить установленным порядком свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);

выполнять требования антивирусной защиты в полном объеме, размещать средства ИСПДн так, чтобы исключить возможность визуального считывания информации.

8. Немедленно известить администратора информационной безопасности ИСПДн в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при их обнаружении:

несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;

отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию компьютера, выхода из строя или неустойчивого функционирования узлов компьютера или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;

некорректного функционирования установленных на компьютере технических средств защиты;

непредусмотренных отводов кабелей и подключенных устройств.

9. Пользователю компьютера категорически запрещается:

использовать компоненты программного и аппаратного обеспечения компьютера в неслужебных целях;

самовольно вносить какие-либо изменения в конфигурацию аппаратно- программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства;

осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

записывать и хранить персональные данные на неучтенных машинных носителях информации (гибких магнитных дисках и т.п.);

оставлять включенным и/или без присмотра компьютер, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие персональные данные;

умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации.

3. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения баз данных и средств защиты информации

10. Резервирование и восстановление работоспособности технических средств и программного обеспечения баз данных и средств защиты информации в Департаменте определяется «Инструкцией по резервному копированию в информационной системе персональных данных Департамента по культуре Томской области».

4.Порядок контроля ИСПДн, приостановки предоставления ПДн в случае обнаружения нарушений порядка их предоставления. Порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации и принятие мер по предотвращению возможных опасных последствий

11. Контроль защиты информации в ИСПДн - комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения техническими средствами охраняемых сведений, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

Основными задачами контроля являются:

проверка организации выполнения мероприятий по защите информации в подразделениях учреждения/организации, учета требований по защите информации в разрабатываемых плановых и распорядительных документах; выявление демаскирующих признаков объектов ИСПДн;

уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;

проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;

проверка знаний работников по вопросам защиты информации и их соответствия требованиям уровня подготовки для конкретного рабочего места;

оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн Департамента;

разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

12. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей на объектах Департамента и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации.

В ходе контроля проверяются:

соответствие принятых мер по обеспечению безопасности персональных данных (далее - ОБ ПДн);

своевременность и полнота выполнения требований настоящего Положения и других руководящих документов ОБ ПДн;

полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;

эффективность применения организационных и технических мероприятий по защите информации;

устранение ранее выявленных недостатков.

13. Основными видами технического контроля на объектах, являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

14. Полученные в ходе ведения контроля результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации администратор информационной безопасности ИСПДн докладывает начальнику Департамента для принятия решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются в виде записей в соответствующих журналах.

15. Невыполнение предписанных мероприятий по защите ПДн, считается предпосылкой к утечке информации (далее - предпосылка).

По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований по указанию начальника Департамента проводится расследование.

Расследование осуществляется комиссией по проведению мероприятий по защите персональных данных (далее - Комиссия). Комиссия обязана установить, имела ли место утечка сведений и обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, установить причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования начальник Департамента принимает решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

16. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся, силами штатных сотрудников осуществляющих обслуживание баз данных, технических и программных средств с участием администратора информационной безопасности ИСПДн в соответствии с утвержденным Департаментом планом или по предварительному с ним согласованию.

17. Одной из форм контроля защиты информации является обследование объектов ИСПДн. Оно проводится не реже одного раза в год.

18. Обследование объектов информатизации и связи проводится с целью определения соответствия защищаемых помещений, основных и вспомогательных технических средств и систем требованиям по защите информации.

В ходе обследования проверяется:

соответствие категории обследуемого объекта ИСПДн условиям, сложившимся на момент проверки;

соблюдение организационно-режимных требований защищаемых помещений; отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;

выполнение требований предписаний на эксплуатацию на основные технические средства и системы по их размещению относительно вспомогательных технических средств и систем, организации электропитания и заземления;

соответствие выполняемых на объекте ИСПДн мероприятий по защите информации данным, изложенным в техническом паспорте;

выполнение требований по защите автоматизированных систем от несанкционированного доступа;

выполнение требований по антивирусной защите.

19. Периодический контроль состояния защиты информации осуществляется Федеральной службы по техническому и экспортному контролю России в соответствии с действующим законодательством Российской Федерации. Доступ представителя указанного федерального органа исполнительной власти на объекты для проведения проверки, а также к работам и документам в объеме, необходимом для осуществления контроля, обеспечивается в установленном порядке при предъявлении служебного удостоверения сотрудника, справки о допуске, а также предписания установленной формы на право проведения проверки.

5. Порядок обучения персонала практике работы в ИСПДн

20. Обучение практике и методике работы в ИСПДн должно быть непрерывным, систематическим, разделенным по категориям, при этом наибольшее внимание следует уделять практике работы пользователя с ИСПДн.

Обучение по методике делятся на:

совещания;

обучающие занятия, семинары;

инструктажи;

методическая помощь и практические занятия на месте.

21. Совещания, обучающие занятия и семинары проводятся согласно плану мероприятий по защите персональных данных, обрабатываемых в ИСПДн Департамента по культуре Томской области.

22. Инструктажи, методическая помощь и практические занятия по вопросам обеспечения безопасности ИСПДн должны проводиться в ходе плановых, периодических и внезапных проверок состояния обеспечения безопасности ИСПДн на местах.

23. Первичные инструктажи проводятся администратором информационной безопасности ИСПДн с пользователями ИСПДн при поступлении сотрудника на работу в Департаменте, где происходит обработка персональных данных.

24. Ответственным за организацию обучения и оказание методической помощи Департаменту является администратор информационной безопасности ИСПДн.

25. Для проведения занятий, семинаров и совещаний могут привлекаться специалисты сторонних организаций, а также органов по аттестации объектов ИСПДн.

26. К работе в ИСПДн допускаются только сотрудники, прошедшие инструктаж обеспечения безопасности в ИСПДн.

6. Порядок проверки электронного журнала обращений к ИСПДн

27. Настоящий раздел Положения определяет порядок проверки электронного журнала обращений к ИСПДн.

Проверка электронного журнала обращений проводится с целью выявления несанкционированного доступа к персональным данным. Право проверки электронного журнала обращений имеют:

начальник Департамента;

администратор информационной безопасности ИСПДн.

28. В ИСПДн, где установлены средства защиты информации (далее - СЗИ), проверка электронного журнала производится в соответствии с прилагаемым к указанным СЗИ руководством.

7. Правила антивирусной защиты

29. Правила антивирусной защиты в информационных системах Департамента содержатся в «Инструкции по организации антивирусной защиты в информационных системах персональных данных Департамента по культуре Томской области».

8. Правила парольной защиты

30. Правила, регламентирующие организационно-технические мероприятия по обеспечению процессов генерации, смены и прекращения действия паролей в ИСПДн, а также контроль действий пользователей при работе с паролями, определяются в «Инструкции по организации парольной защиты в информационных системах персональных данных Департамента по культуре Томской области».

9. Порядок контроля соблюдения условий использования средств защиты информации

31. Данный раздел Положения определяет порядок контроля соблюдения условий использования средств защиты информации (далее - СЗИ).

Технические средства защиты информации являются важным компонентом обеспечения безопасности ПДн.

Порядок работы с техническими СЗИ определен в соответствующих Инструкциях к СЗИ, в Руководстве по настройке и использованию СЗИ, обязательных для исполнения, как сотрудниками обрабатывающими персональные данные, так и администратором информационной безопасности ИСПДн Департамента.

Право проверки соблюдения условий использования средств защиты информации имеют:

начальник Департамента;

администратор информационной безопасности ИСПДн Департамента.

Пользователю ИСПДн категорически запрещается:

обработка персональных данных с отключенными СЗИ;

изменение настроек СЗИ.

10. Порядок охраны и допуска посторонних лиц в защищаемые помещения

32. Охрана (сдача под охрану) защищаемых помещений ИСПДн осуществляется в соответствии с порядком доступа государственных гражданских служащих Департамента по культуре Томской области в помещения, в которых ведется обработка персональных данных.

33. Вскрытие и закрытие помещений осуществляется сотрудниками, работающими в данных помещениях. Список сотрудников, имеющих право вскрывать (сдавать под охрану) и опечатывать помещения определяется руководителем структурного подразделения (отдела) по согласованию с администратором информационной безопасности ИСПДн Департамента.

34. При закрытии помещений и сдачей их под охрану сотрудники, ответственные за помещения, проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации на которых содержатся персональные данные, складываются в опечатываемый сейф (металлический шкаф).

35. При обнаружении нарушений целостности оттисков печатей, повреждения запоров или наличия других признаков, указывающих на возможное проникновение в помещение посторонних лиц, помещение не вскрывается, а составляется акт. О происшествии немедленно сообщается начальнику Департамента и администратору информационной безопасности ИСПДн.

Одновременно принимаются меры по охране места происшествия и до прибытия руководителя структурного подразделения и администратора информационной безопасности ИСПДн в помещение никто не допускается.

36. Руководитель структурного подразделения и администратор информационной безопасности ИСПДн организуют проверку АРМ, ИСПДн на предмет несанкционированного доступа к персональных данных и наличие документов и машинных носителей информации, о чём докладывается непосредственно начальнику Департамента.

37. В соответствии с требованиями данного Положения при обработке персональных данных в ИСПДн необходимо исключить возможность неконтролируемого пребывания посторонних лиц в пределах границ контролируемой зоны ИСПДн.

11. Заключительные положения

38. Требования настоящего Положения обязательны для всех сотрудников обрабатывающих персональные данные в ИСПДн Департамента.

39. Нарушение требований настоящего Положения влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 7
к приказу
Департамента по культуре
Томской области
от 20.05. 2020 № 015/01-09

ПЕРЕЧЕНЬ
должностей государственных гражданских служащих Томской области, состоящих в штате Департамента по культуре Томской области, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

Структурное подразделение	Должность
Администрация	начальник Департамента
	заместитель начальника Департамента
Комитет кадровой политики и организационно-правовой работы	председатель комитета
	консультант
	главный специалист
	ведущий специалист
	специалист 1 категории
Комитет финансирования, бухгалтерского учета и отчетности	председатель комитета
	главный специалист
	специалист 1 категории
Комитет экономики	председатель комитета
	консультант
	главный специалист
Комитет по делам архивов	председатель комитета