АГЕНТСТВО ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ

ПРИКАЗ

«28» августа 2015 г. Красноярск №33-211

Об обработке и защите персональных данных в агентстве труда и занятости населения Красноярского края

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 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», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Положением об агентстве труда и занятости населения Красноярского края, утвержденным постановлением Правительства Красноярского края от 15.07.2010 № 387-п ПРИКАЗЫВАЮ:

1. Назначить Крылову Т.М., заместителя руководителя, ответственным за организацию обработки и защиты персональных данных.

2. Утвердить Правила обработки персональных данных в агентстве труда и занятости населения Красноярского края согласно приложению № 1.

3. Утвердить Правила рассмотрения запросов субъектов персональных данных или их представителей, поступающих в агентство труда и занятости населения Красноярского края, согласно приложению № 2.

4. Утвердить Правила работы с обезличенными персональными данными в агентстве труда и занятости населения Красноярского края согласно приложению № 3.

5. Утвердить Правила осуществления в агентстве труда и занятости населения Красноярского края внутреннего контроля соответствия обработки персональных данных требованиям законодательства в сфере защиты персональных данных согласно приложению № 4.

6. Утвердить Перечень информационных систем персональных данных агентства труда и занятости населения Красноярского края согласно приложению № 5.

7. Утвердить Перечень персональных данных, обрабатываемых в агентстве труда и занятости населения Красноярского края в связи с реализацией служебных или трудовых отношений, согласно приложению № 6.

8. Утвердить Перечень должностей государственных гражданских служащих агентства труда и занятости населения Красноярского края, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, согласно приложению № 7.

9. Утвердить Положение об администраторе информационной безопасности в агентстве труда и занятости населения Красноярского края согласно приложению № 8.

10. Утвердить Перечень должностей государственных гражданских служащих агентства труда и занятости населения Красноярского края, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, согласно приложению № 9.

11. Утвердить типовое обязательство государственного гражданского служащего агентства труда и занятости населения Красноярского края, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей, согласно приложению № 10.

12. Утвердить типовую форму согласия на обработку персональных данных государственного гражданского служащего агентства труда и занятости населения Красноярского края, иных субъектов персональных данных согласно приложению № 11.

13. Утвердить типовую форму согласия на обработку персональных данных директора краевого государственного учреждения службы занятости населения, иных субъектов персональных данных согласно приложению № 12.

14. Утвердить типовую форму разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные согласно приложению № 13.

15. Утвердить Порядок доступа государственных гражданских служащих агентства труда и занятости населения Красноярского края в помещения, в которых ведется обработка персональных данных, согласно приложению № 14.

16. Утвердить Положение об экспертной комиссии в агентстве труда и занятости населения Красноярского края согласно приложению № 15.

17. Утвердить Инструкцию по обеспечению информационной безопасности при подключении и использовании информационно-вычислительной сети общего пользования в агентстве труда и занятости населения Красноярского края согласно приложению № 16.

18. Утвердить Инструкцию по учету, маркировке, очистке и утилизации отчуждаемых носителей информации и жестких магнитных дисков в агентстве труда и занятости населения Красноярского края согласно приложению № 17.

19. Утвердить Инструкцию по организации антивирусной защиты информационных систем в агентстве труда и занятости населения Красноярского края согласно приложению № 18.

20. Утвердить Инструкцию по организации парольной защиты информационных систем в агентстве труда и занятости населения Красноярского края согласно приложению № 19.

21. Отделу персонала и документационного обеспечения управления агентства труда и занятости населения Красноярского края довести настоящий приказ до сведения всех государственных гражданских служащих агентства труда и занятости населения Красноярского края.

22. Признать утратившим силу приказ агентства труда и занятости населения Красноярского края от 19.07.2012 № 159.

23. Опубликовать приказ на «Официальном интернет-портале правовой информации Красноярского края» (www.zakon.krskstate.ru).

24. Приказ вступает в силу в день, следующий за днем его официального опубликования.

25. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель агентства В.В. Новиков

Приложение № 1
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08 2015 г. №83-211

ПРАВИЛА
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АГЕНТСТВЕ ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Правила обработки персональных данных в агентстве труда и занятости населения Красноярского края (далее - Правила) устанавливают процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяют для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются, сроки их обработки и хранения, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований в агентстве труда и занятости населения Красноярского края (далее - Агентство).

1.2. Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 21.03.2012 № 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», иными нормативными правовыми актами.

1.3. Понятия и термины, используемые в Правилах, применяются в том же значении, что и в Федеральном законе № 152-ФЗ.

2. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка персональных данных должна осуществляться на основе принципов.

Обработка персональных данных должна осуществляться на законной и справедливой основе.

Обработка персональных данных должна ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, несовместимая с целями сбора персональных данных.

Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

Обработке подлежат только персональные данные, которые отвечают целям их обработки.

Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

При обработке персональных данных должны быть обеспечены точность персональных данных, их достаточность, а в необходимых случаях и актуальность по отношению к целям обработки персональных данных. Агентство должно принимать необходимые меры либо обеспечивать их принятие по удалению или уточнению неполных или неточных данных.

Хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

2.2. Агентство может осуществлять обработку персональных данных с использованием средств автоматизации, а также без использования таких средств.

2.3. При обработке персональных данных Агентством может осуществляться любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление,

уничтожение персональных данных.

2.4. До начала обработки персональных данных Агентство обязано уведомить уполномоченный орган по защите прав субъектов персональных данных об обработке персональных данных согласно статье 22 Федерального закона № 152-ФЗ.

3. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Обработка в Агентство персональных данных осуществляется в следующих информационных системах персональных данных (далее – ИСПД):

«Зарплата и кадры»;

«Бухгалтерия для бюджетных организаций».

Агентство является оператором.

3.2. Целями обработки персональных данных в ИСПД являются учет операций по ведению организационной структуры, штатного расписания, кадрового учета, табельного учета, ведение реестра гражданских служащих, решение задач управленческого и финансового учета, учет операций по ведению пенсионных начислений, выполнение операций по налогообложению.

3.3. Порядок обработки персональных данных:

3.3.1. Получение персональных данных может осуществляться как путем их представления Агентству самим субъектом персональных данных, так и путем получения персональных данных Агентство из иных источников, в том случае, если персональные данные представляется возможным получить только у третьей стороны. Если персональные данные получены не от субъекта персональных данных и такое получение не предусмотрено частью 4 статьи 18 Федерального закона № 152-ФЗ, то до начала обработки таких персональных данных Агентство обязано предоставить субъекту персональных данных информацию, предусмотренную частью 3 статьи 18 Федерального закона № 152-ФЗ.

3.3.2. Агентство не имеет права получать и обрабатывать персональные данные субъекта, не связанные с целями обработки персональных данных. В случаях, непосредственно связанных с вопросами трудовых отношений, данные о частной жизни субъекта персональных данных (информация о жизнедеятельности в сфере семейных, бытовых, личных отношений) могут быть получены и обработаны Агентством только с письменного согласия субъекта персональных данных.

3.3.3. Для осуществления процесса обработки персональных данных на автоматизированных рабочих местах (далее – АРМ) используется сертифицированное программное обеспечение.

3.3.4. Пользователи ИСПД осуществляют обработку в многопользовательском режиме. Доступ в ИСПД осуществляется пользователями с использованием персональных идентификаторов и паролей. Права доступа пользователей к программам, каталогам и файлам

на АРМ регламентированы настройками локальных политик безопасности Windows.

3.3.5. Передача информации, содержащей персональные данные, за пределы контролируемой зоны по сети Интернет не осуществляется.

3.3.6. Срок обработки персональных данных исчисляется с момента получения Агентством персональных данных до достижения целей обработки персональных данных.

3.4. Хранение персональных данных:

3.4.1. Пользователи имеют право постоянного хранения файлов с защищаемыми данными на жестком магнитном диске, входящие в состав технических средств. Для хранения файлов, содержащих персональные данные, съемные носители информации (оптические диски, флеш-носители и т.д.) не используются. Учет съемных носителей не ведется.

3.4.2. После достижения цели обработки персональных данных, если это предусмотрено федеральными законами, нормативными актами или в письменном согласии субъекта персональных данных, персональные данные помещаются в архив и хранятся в течение срока, установленного законодательством Российской Федерации. На хранение персональных данных в электронном архиве должно быть получено согласие субъекта.

3.4.3. Если в течение срока архивного хранения субъект персональных данных направил в адрес Агентства заявление об отзыве согласия на обработку персональных данных, Агентство обязано уничтожить персональные данные субъекта с составлением соответствующего акта или обеспечить их уничтожение, если сохранение персональных данных более не требуется для целей обработки персональных данных.

3.5. Передача персональных данных.

Передача персональных данных субъекта любым физическим или юридическим лицам может быть осуществлена только с письменного согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

3.6. Уничтожение персональных данных.

3.6.1. Уничтожение персональных данных осуществляется по истечении соответствующего срока хранения. Для уничтожения персональных данных приказом руководителя Агентства создается комиссия, которая проводит уничтожение персональных данных.

3.6.2. Носители, содержащие персональные данные, уничтожаются таким способом, чтобы после процедуры уничтожения не представилось возможным восстановить данные. По результатам уничтожения составляется акт об уничтожении персональных данных, который подписывается комиссией, созданной для уничтожения персональных данных. В течение пяти рабочих дней после уничтожения и составления акта об уничтожении персональных данных Агентство уведомляет об этом субъекта персональных данных.

3.7. Содержание обрабатываемых персональных данных представлено в Перечне персональных данных, обрабатываемых в Агентстве, в связи с

реализацией служебных или трудовых отношений согласно приложению № 6 настоящего Приказа.

3.8. Категории субъектов, персональные данные которых обрабатываются:

государственные гражданские служащие и иные работники Агентства (в том физические лица, предоставившие сведения в Агентство для участия в конкурсе на замещение вакантных должностей государственной гражданской службы либо для формирования кадрового резерва);

лица замещающие должности руководителей подведомственных учреждений.

4. ПРАВА СУБЪЕКТА ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

подтверждение факта обработки персональных данных Агентством;

правовые основания и цели обработки персональных данных;

цели и применяемые Агентством способы обработки персональных данных;

наименование и место нахождения Агентства, сведения о лицах (за исключением государственных гражданских служащих Агентства), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Агентством или на основании федерального законодательства;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законодательством;

сроки обработки персональных данных, в том числе сроки их хранения;

порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

5. ОБЯЗАННОСТИ ОПЕРАТОРА

5.1. При сборе персональных данных Агентство обязано предоставить субъекту персональных данных по его просьбе информацию, предусмотренную частью 7 статьи 14 Федерального закона № 152-ФЗ,

в сроки, установленные частью 1 статьи 20 Федерального закона № 152-ФЗ.

5.2. Если предоставление персональных данных является обязательным в соответствии с федеральным законодательством, Агентство обязано разъяснить субъекту персональных данных юридические последствия отказа предоставить его персональные данные.

5.3. Если персональные данные получены не от субъекта персональных данных, Агентство, за исключением случаев, предусмотренных частью 4 статьи 18 Федерального закона № 152-ФЗ, до начала обработки таких персональных данных обязано предоставить субъекту персональных данных следующую информацию:

наименование либо фамилия, имя, отчество и адрес оператора или его представителя;

цель обработки персональных данных и ее правовое основание;

предполагаемые пользователи персональных данных;

установленные Федеральным законом № 152-ФЗ права субъекта персональных данных;

источник получения персональных данных.

5.4. Агентство освобождается от обязанности предоставить субъекту персональных данных сведения, предусмотренные пунктом 5.3 настоящих Правил, в случаях, если:

субъект персональных данных уведомлен об осуществлении обработки его персональных данных соответствующим оператором;

персональные данные получены Агентством на основании федерального законодательства или в связи с исполнением договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных;

персональные данные сделаны общедоступным субъектом персональных данных или получены из общедоступного источника;

Агентство осуществляет обработку персональных данных для статистических или иных исследовательских целей, если при этом не нарушаются права и законные интересы субъекта персональных данных;

предоставление субъекту персональных данных сведений, предусмотренных пунктом 5.3 настоящих Правил, нарушает права и законные интересы третьих лиц.

5.5. Агентство самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных законодательством Российской Федерации и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам могут, в частности, относиться:

1) назначение ответственного за организацию обработки персональных данных;

2) издание документов, определяющих политику Агентства в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений

законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 Федерального закона № 152-ФЗ;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Агентства в отношении обработки персональных данных, локальным актам Агентства;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых Агентством мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

6) ознакомление служащих Агентства, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных сотрудников.

5.6. В случае выявления неправомерной обработки персональных данных, осуществляемой Агентством или лицом, действующим по поручению Агентства, Агентство в срок, не превышающий трех рабочих дней с даты этого выявления, обязано прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению Агентства. В случае, если обеспечить правомерность обработки персональных данных невозможно, Агентство в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные или обеспечить их уничтожение. Об устранении допущенных нарушений или об уничтожении персональных данных Агентство обязано 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.

5.7. В случае достижения цели обработки персональных данных Агентство обязано прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению Агентства) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом,

действующим по поручению Агентства) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между Агентством и субъектом персональных данных, либо если Агентство не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных законодательством Российской Федерации.

6. МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Мероприятия по обеспечению безопасности персональных данных являются составной частью деятельности Агентства.

6.2. Перечень должностей государственной гражданской службы, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным, а также порядок доступа должностных лиц Агентства в помещения, в которых ведется обработка персональных данных определяются согласно приложениям к настоящему Приказу.

6.3. Сбой в функционировании элементов ИСПД, предоставляемых пользователям ИСПД, а также потеря защищаемой информации, связанные с нарушением правил обработки персональных данных, может произойти в результате следующих действий (бездействия):

непреднамеренных либо преднамеренных действий сотрудников Агентства и третьих лиц;

в результате возникновения обстоятельств непреодолимой силы.

6.4. По каждому происшествию проводится проверка, для проведения которой назначается комиссия. Порядок проведения проверки устанавливается Правилами осуществления в Агентстве внутреннего контроля соответствия обработки персональных данных требованиям законодательства в сфере защиты персональных данных согласно приложению № 4 к настоящему Приказу. В ходе проверки устанавливаются обстоятельства, виновные лица в совершении нарушений мероприятий по защите информации, причины и условия, способствовавшие нарушению.

По результатам проведенной проверки определяются необходимые мероприятия по устранению выявленных нарушений, а также обстоятельств, способствующих их совершению.

6.5. Процедуры, направленные на выявление нарушений:

осуществление внутреннего контроля соответствия обработки персональных данных законодательству Российской Федерации и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике Агентства в отношении обработки персональных данных, локальным актам Агентства;

иные процедуры, направленные на выявление нарушений.

6.6. Процедуры, направленные на предотвращение нарушений:

назначение ответственного за организацию обработки персональных данных, который осуществляет, в том числе обучение и инструктаж, внутренний контроль, за соблюдением служащими Агентства требований к защите персональных данных;

ознакомление служащих Агентства, непосредственно осуществляющих обработку персональных данных, с положениями действующего законодательства о персональных данных и иными документами по вопросам обработки персональных данных;

определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных Агентства;

применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных Агентства, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;

разграничение прав доступа к персональным данным при их обработке в информационных системах персональных данных Агентства.

6.7. Персональные данные не подлежат разглашению (распространению). Прекращение доступа к такой информации не освобождает служащего Агентства от взятых им обязательств по неразглашению сведений ограниченного распространения.

6.8. При обработке в Агентстве персональных данных на бумажных носителях, в частности, при использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться требования, установленные Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденным Постановлением Правительства РФ от 15.09.2008 № 687.

Необходимо обеспечивать раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ.

6.9. Допускается передача материальных носителей персональных данных на хранение сторонней организации на основании договора, при этом существенным условием договора является обязанность обеспечения указанной организацией конфиденциальности персональных данных и безопасности персональных данных при их обработке (хранении).

6.10. Лица, виновные в нарушении требований настоящих Правил, несут

ответственность в соответствии с действующим законодательством Российской Федерации.

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем  С.Г. Мунцев

Приложение № 2
к приказу агентства труда
и занятости населения
Красноярского края
от 28-08- 2015 г. №83-211

ПРАВИЛА
РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ, ПОСТУПАЮЩИХ В АГЕНТСТВО ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ

1. Правилами рассмотрения запросов субъектов персональных данных или их представителей в агентстве труда и занятости населения Красноярского края (далее - Правила) определяется порядок учета (регистрации), рассмотрения запросов субъектов персональных данных или их представителей (далее - запросы).

2. Настоящие Правила разработаны в соответствии Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации», Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее - Федеральный закон № 152-ФЗ), Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 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».

3. Субъект персональных данных имеет право на получение информации, касающейся обработки его персональных данных (часть 7 статьи 14 Федерального закона № 152-ФЗ), в том числе содержащей:

подтверждение факта обработки персональных данных в агентстве труда и занятости населения Красноярского края (далее - Агентство);

правовые основания и цели обработки персональных данных;

цели и применяемые в Агентстве способы обработки персональных данных;

наименование и место нахождения Агентства, сведения о лицах (за исключением служащих Агентства), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с Агентством или на основании федерального

законодательства;

обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом № 152-ФЗ;

сроки обработки персональных данных, в том числе сроки их хранения;

порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом № 152-ФЗ;

информацию об осуществленной или о предполагаемой трансграничной передаче данных;

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

иные сведения, предусмотренные Федеральным законом № 152-ФЗ или другими федеральными законами.

4. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе по основаниям, предусмотренным частью 8 статьи 14 Федерального закона № 152-ФЗ.

5. Субъект персональных данных вправе требовать от Агентства уточнения его 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.

6. Сведения, указанные в части 7 статьи 14 Федерального закона № 152-ФЗ, предоставляются Агентством субъекту персональных данных в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

7. Сведения, указанные в части 7 статьи 14 Федерального закона № 152-ФЗ, представляются субъекту персональных данных или его представителю Агентством при обращении либо при получении запроса субъекта персональных данных или его представителя.

8. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие субъекта персональных данных в отношениях с Агентством (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных в Агентстве, подпись субъекта персональных данных или его представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии

с законодательством Российской Федерации.

9. Все поступившие запросы регистрируются и проверяются на повторность их поступления в день их поступления.

В случае если сведения, указанные в части 7 статьи 14 Федерального закона 152-ФЗ, а также обрабатываемые персональные данные были представлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в Агентство или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона № 152-ФЗ, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса 152-ФЗ, если более короткий срок не установлен федеральным законом, принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных.

Субъект персональных данных вправе обратиться повторно в Агентство или направить повторный запрос в целях получения сведений, указанных в части 7 статьи 14 Федерального закона № 152-ФЗ, а также в целях ознакомления с обрабатываемыми персональными данными до истечения тридцатидневного срока, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в пункте 8 настоящих Правил, должен содержать обоснование направления повторного запроса.

Агентство вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным частями 4 и 5 статьи 14 Федерального закона № 152-ФЗ. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на Агентстве.

10. Обязанности Агентства при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных:

Агентство обязано сообщить в порядке, предусмотренном статьей 14 Федерального закона № 152-ФЗ, субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъекта персональных данных или его представителя в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя;

в случае отказа в представлении информации о наличии персональных

данных о соответствующем субъекте персональных данных или персональных данных субъекту персональных данных или его представителю при их обращении либо при получении запроса субъекта персональных данных или его представителя Агентство обязано дать в письменной форме мотивированный ответ, содержащий ссылку на положение части 8 статьи 14 Федерального закона № 152-ФЗ или иного федерального законодательства, являющимся основанием для такого отказа, в срок, не превышающий тридцати дней со дня обращения субъекта персональных данных или его представителя либо с даты получения запроса субъекта персональных данных или его представителя;

Агентство обязано предоставить безвозмездно субъекту персональных данных или его представителю возможность ознакомления с персональными данными, относящимися к этому субъекту персональных данных. В срок, не превышающий семи рабочих дней со дня предоставления субъектом персональных данных или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, Агентство обязано внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления субъектом персональных данных или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, Агентство обязано уничтожить такие персональные данные;

Агентство обязано уведомить субъекта персональных данных или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого субъекта были переданы;

Агентство обязано сообщить в уполномоченный орган по защите прав субъектов персональных данных по запросу этого органа необходимую информацию в течение тридцати дней с даты получения такого запроса.

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем С.Г. Мунцев

Приложение № 3
к приказу агентства труда
и занятости населения
Красноярского края
от 28-08 2015 г. №83-211

ПРАВИЛА
РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ПЕРСОНАЛЬНЫМИ ДАННЫМИ В АГЕНТСТВЕ ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила работы с обезличенными персональными данными в агентстве труда и занятости населения Красноярского края (далее - Правила) разработаны с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 21.03.2012 № 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» и определяют порядок работы с обезличенными персональными данными в агентстве труда и занятости населения Красноярского края (далее - Агентство).

2. ОСНОВНЫЕ ПОНЯТИЯ

2.1. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» в настоящих Правилах используются следующие понятия:

персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных к конкретному субъекту

персональных данных.

3. УСЛОВИЯ ОБЕЗЛИЧИВАНИЯ

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

3.2. Способы обезличивания при условии дальнейшей обработки персональных данных:

уменьшение перечня обрабатываемых сведений;

замена части сведений идентификаторами;

обобщение - понижение точности некоторых сведений;

деление сведений на части и обработка в разных информационных системах;

другие способы.

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

3.4. Перечень должностей государственных гражданских служащих Агентства, ответственных за проведение мероприятий по обезличиванию обрабатываемых персональных данных, приведен в приложении № 7 к настоящему Приказу.

3.5. Для обезличивания персональных данных используются любые способы, явно не запрещенные действующим законодательством.

3.6. Государственные гражданские служащие Агентства, обслуживающие базы данных с персональными данными совместно с ответственными за организацию работы с персональными данными, осуществляют непосредственное обезличивание выбранным способом.

4. ПОРЯДОК РАБОТЫ С ОБЕЗЛИЧЕННЫМИ ДАННЫМИ

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

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

4.3. 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.

4.4. 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.

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем С.Г. Мунцев

Приложение № 4
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08. 2015 г. №53-211

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ В АГЕНТСТВЕ ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА В СФЕРЕ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Правилами осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в агентстве труда и занятости населения Красноярского края (далее - Правила) определяются процедуры, с целью выявления и предотвращения нарушений законодательства Российской Федерации в сфере персональных данных.

1.2. Правила определяют основания, порядок, формы и методы проведения внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных.

1.3. Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 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» и другими нормативными правовыми актами.

1.4. В Правилах используются основные понятия, определенные в статье 3 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

2. ПОРЯДОК ПРОВЕДЕНИЯ ПРОВЕРКИ

2.1. В целях осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в агентстве труда и занятости населения Красноярского края (далее - Агентство) организовывается проведение проверок условий обработки

персональных данных.

Проверки осуществляются комиссией, образуемой приказом руководителя Агентства.

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

Проверки соответствия обработки персональных данных установленным требованиям (плановые проверки) в Агентстве проводятся 1 раз в 2 года, или на основании поступившего в Агентство письменного заявления (обращения), служебной записки о нарушениях правил обработки персональных данных (внеплановые проверки). Проведение внеплановой проверки организуется в течение трех рабочих дней с момента поступления соответствующего заявления (обращения), служебной записки о нарушениях правил обработки персональных данных.

2.2. При проведении проверки соответствия обработки персональных данных установленным требованиям должны быть полностью, объективно и всесторонне установлены:

порядок и условия применения организационных и технических мер по обеспечению безопасности персональных данных при их обработке, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные уровни защищенности персональных данных;

порядок и условия применения средств защиты информации;

эффективность принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

соблюдение правил доступа к персональным данным;

наличие (отсутствие) фактов несанкционированного доступа к персональным данным и принятие необходимых мер;

мероприятия по восстановлению персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

осуществление мероприятий по обеспечению целостности персональных данных.

2.3. Члены комиссии имеют право:

запрашивать у служащих Агентства информацию, необходимую для проведения проверки;

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

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

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

вносить руководителю Агентства предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении законодательства Российской Федерации в отношении обработки персональных данных.

2.4. В отношении персональных данных, ставших известными в ходе проведения мероприятий внутреннего контроля, должна обеспечиваться конфиденциальность персональных данных.

2.5. Проверка должна быть завершена не позднее чем через месяц со дня издания приказа о ее проведении. По результатам проведенной проверки составляется и подписывается комиссией заключение, в котором отражаются меры, необходимые для устранения выявленных нарушений. Подписанное заключение не позднее дня, следующего за днем завершения проверки, представляется руководителю Агентства.

2.6. По результатам проверки руководитель Агентства принимает необходимые меры, направленные на предотвращение нарушений, а при необходимости привлекает виновных лиц к установленной ответственности.

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем С.Г. Мунцев

Приложение № 5
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08. 2015 г. №83-211

ПЕРЕЧЕНЬ
ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ АГЕНТСТВА ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ

№ п/п	Наименование информационных систем персональных данных	Показатель объема обрабатываемых персональных данных	Наличие подключения к сети Интернет	Режим обработки персональных данных	Разграничение доступа пользователей	Нахождение ИСПД (ее составных частей) в пределах Российской Федерации	Тип угроз
1.	1С, версия 8.3. Предприятие «Зарплата и кадры»	до 1000	существует	многопользовательский	присутствует	Все технические средства находятся в пределах Российской Федерации	3
2.	1С, версия 8.3. Предприятие «Бухгалтерия для бюджетных организаций»	до 1000	существует	многопользовательский	присутствует	Все технические средства находятся в пределах Российской Федерации	3

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем С.Г. Мунцев

Приложение № 6
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08 2015 г. №53-211

ПЕРЕЧЕНЬ
ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В АГЕНТСТВЕ ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ В СВЯЗИ С РЕАЛИЗАЦИЕЙ СЛУЖЕБНЫХ ИЛИ ТРУДОВЫХ ОТНОШЕНИЙ

Персональные данные, обрабатываемые в агентстве труда и занятости населения Красноярского края в связи с реализацией служебных или трудовых отношений:

фамилия, имя, отчество, дата и место рождения, гражданство;

прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);

адрес регистрации и фактического проживания;

номер контактного телефона или сведения о других способах связи;

дата регистрации по месту жительства;

информация о паспорте гражданина Российской Федерации (серия, номер, кем и когда выдан паспорт гражданина Российской Федерации) или ином документе, удостоверяющем личность гражданина;

информация о трудовой книжке;

идентификационный номер налогоплательщика;

страховой номер индивидуального лицевого счета застрахованного лица в системе обязательного пенсионного страхования в Российской Федерации;

информация о паспорте гражданина Российской Федерации, удостоверяющем личность гражданина Российской Федерации за пределами Российской Федерации (серия, номер, кем и когда выдан);

информация о государственной регистрации актов гражданского состояния;

информация о владении иностранными языками и языками народов Российской Федерации;

информация об образовании (когда и какие образовательные учреждения окончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);

информация о послевузовском профессиональном образовании (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);

информация о дополнительном профессиональном образовании;

информация о профессиональной переподготовке или повышении

квалификации.

информация о выполняемой работе с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность и т.п.), в том числе:

информация о замещаемой должности;

информация о ранее замещаемой должности (последнем месте работы, службы);

информация об общем трудовом стаже, стаже государственной гражданской службы;

информация о классном чине федеральной государственной гражданской службы, гражданской службы субъекта Российской Федерации, муниципальной службы, дипломатическом ранге, воинском, специальном звании, классном чине правоохранительной службы (кем и когда присвоены);

информация о государственных наградах, иных наградах и знаках отличия (кем награжден и когда);

информация о степени родства, фамилиях, именах, отчествах, датах рождения близких родственников (отца, матери, братьев, сестер и детей), а также супруга (супруги), бывшего супруга (супруги);

информация о местах рождения, местах работы и домашних адресах близких родственников (отца, матери, братьев, сестер и детей), а также супруга (супруги), бывшего супруга (супруги);

информация о пребывании за границей (когда, где, с какой целью);

информация о близких родственниках (отец, мать, братья, сестры и дети), а также супругах, в том числе бывших, постоянно проживающих за границей и (или) оформляющих документы для выезда на постоянное место жительства в другое государство (фамилия, имя, отчество, с какого времени проживают за границей);

информация об отношении к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);

информация о наличии (отсутствии) судимости;

информация о допуске к государственной тайне, оформленном за период работы, службы, учебы (форма, номер и дата);

информация о наличии (отсутствии) заболевания, препятствующего поступлению на государственную гражданскую службу Российской Федерации или ее прохождению, подтвержденная заключением медицинского учреждения;

информация о наличии (отсутствии) медицинских противопоказаний для работы с использованием сведений, составляющих государственную тайну, подтвержденная заключением медицинского учреждения;

результаты обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований);

полис обязательного медицинского страхования;

денежное содержание и условия оплаты труда;

сведения о доходах, о расходах, об имуществе и обязательствах

имущественного характера, а также о доходах, о расходах, об имуществе и обязательствах имущественного характера членов семьи;

информация об отпусках и командировках;

информация о прохождении аттестации и сдаче квалификационного экзамена;

информация об участии в конкурсных процедурах, включении в кадровый резерв;

информация о проведении служебных проверок;

информация о наложении дисциплинарных взысканий, их снятии (отмене);

информация о поощрении;

информация о размере денежного содержания и иных выплат;

информация, содержащаяся в служебном контракте, дополнительных соглашениях к служебному контракту (в трудовом договоре, дополнительных соглашениях к трудовому договору);

иная информация, содержащаяся в анкете, личной карточке государственного гражданского служащего (личной карточке работника);

фотография гражданина;

информация о составе семьи, месте нахождения занимаемого им жилого помещения и его общей площади;

информация о наличии либо об отсутствии зарегистрированных прав на недвижимое имущество;

информация о банковских реквизитах расчетного счета.

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем С.Г. Мунцев

Приложение № 7
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08. 2015 г. №83-211

ПЕРЕЧЕНЬ
ДОЛЖНОСТЕЙ ГОСУДАРСТВЕННЫХ ГРАЖДАНСКИХ СЛУЖАЩИХ АГЕНТСТВА ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ, ОТВЕТСТВЕННЫХ ЗА ПРОВЕДЕНИЕ МЕРОПРИЯТИЙ ПО ОБЕЗЛИЧИВАНИЮ ОБРАБАТЫВАЕМЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Главный бухгалтер - заведующий отделом бухгалтерского учета и отчетности (в части обезличивания персональных данных, связанных с выплатой денежного содержания, обязательным страхованием, выполнением функции налогового агента в отношении налога на доходы физических лиц).

2. Заместитель главного бухгалтера (в части обезличивания персональных данных, связанных с выплатой денежного содержания, обязательным страхованием, выполнением функции налогового агента в отношении налога на доходы физических лиц).

3. Старший бухгалтер отдела бухгалтерского учета и отчетности (в части обезличивания персональных данных, связанных с выплатой денежного содержания, обязательным страхованием, выполнением функции налогового агента в отношении налога на доходы физических лиц).

4. Начальник отдела персонала и документационного обеспечения управления (в части обезличивания персональных данных, связанных с ведением кадровой работы).

5. Главный специалист отдела персонала и документационного обеспечения управления (в части обезличивания персональных данных, связанных с ведением кадровой работы).

6. Ведущий специалист отдела персонала и документационного обеспечения управления (в части обезличивания персональных данных, связанных с ведением кадровой работы).

7. Специалист 1 категории отдела персонала и документационного обеспечения управления (в части обезличивания персональных данных, связанных с ведением кадровой работы).

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем С.Г. Мунцев

Приложение № 8
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08 2015 г. №83-211

ПОЛОЖЕНИЕ
ОБ АДМИНИСТРАТОРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АГЕНТСТВЕ ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об администраторе информационной безопасности агентства труда и занятости населения Красноярского края (далее - Положение) разработано в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Настоящие Положение определяет основные задачи, функции, обязанности, права и ответственность администратора информационной безопасности агентства труда и занятости населения Красноярского края (далее - Агентство).

1.2. Администратор информационной безопасности - лицо, выполняющее функции по настройке и сопровождению всех программных и технических средств защиты информации (далее - СЗИ) автоматизированной системы (далее - АС) от несанкционированного доступа (далее - НСД).

1.3. Администратор информационной безопасности назначается руководителем Агентства.

1.4. Администратор информационной безопасности в пределах своих функциональных обязанностей обеспечивает безопасность информации, обрабатываемой и хранимой в АС.

1.5. Администратор информационной безопасности в своей работе руководствуется положениями нормативных правовых актов Российской Федерации, руководящими документами по безопасности информации, положениями, а так же приказами и нормативными актами ФСТЭК и ФСБ России и настоящим Положением.

2. ОСНОВНЫЕ ЗАДАЧИ И ФУНКЦИИ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Основными задачами администратора информационной безопасности являются:

2.1.1. Назначение прав доступа пользователей операционной системы и приложений (задач, функционального программного обеспечения) к объектам защиты (файлам, директориям).

2.1.2. Управление ресурсами и объектами операционной системы и приложений (например, размещение на физических носителях) АС.

2.1.3. Управление регламентом предоставления ресурсов операционной системы и приложений пользователям АС.

2.1.4. Управление резервированием и восстановлением операционных систем в АС.

2.1.5.Управление инсталляцией системного и прикладного программного обеспечения в АС.

2.1.6. Организация эксплуатации технических и программных средств и систем защиты информации в АС.

2.1.7. Текущий контроль работы средств и систем зашиты информации в АС.

2.1.8. Контроль за работой пользователей АС, выявление попыток несанкционированного доступа к АС и защищаемым информационным ресурсам.

2.1.9. Анализ системных журналов безопасности и выявление подозрительных событий в АС.

2.1.10. Составление и поддержание в актуальном состоянии списка прав доступа и полномочий сотрудников по доступу к средствам вычислительной техники, с использованием которых обрабатывается, хранится и передается информация ограниченного доступа.

2.2. Основными функциями администратора информационной безопасности являются:

2.2.1. Поддержание функционирования средств и систем защиты информации в пределах возложенных на него обязанностей.

2.2.2. Обучение персонала и пользователей вычислительной техники правилам работы с СЗИ от НСД.

2.2.3. Формирование и распределение списка реквизитов полномочий пользователей, определяемых эксплуатационной документацией на средства и системы защиты информации.

2.2.4. Организация антивирусного контроля, включая контроль съемных носителей информации.

2.2.5. Участие в проведении служебных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации.

2.2.6. Организация учета и хранения носителей информации, содержащих резервные копии общесистемных программных средств и систем.

2.2.7. Текущий контроль технологического процесса обработки защищаемой информации.

2.2.8. Текущий контроль работоспособности средств и систем защиты информации.

2.2.9. Текущий контроль за соблюдением требований положения при эксплуатации средств и систем защиты информации.

2.2.10. Контроль целостности эксплуатируемого на средствах вычислительной техники (далее – СВТ) программного обеспечения с целью выявления несанкционированных изменений в нем.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Знать перечень установленных программ в подразделениях АС и перечень задач, решаемых с их использованием.

3.2. Обеспечивать постоянный контроль за выполнением служащими установленного комплекса мероприятий по обеспечению безопасности информации в АС.

3.3. Управлять средствами и системами защиты информации АС и поддерживать их функционирование.

3.4. Немедленно сообщать начальнику отдела информационных технологий и эксплуатации автоматизированных систем об имевших место в подразделениях попытках несанкционированного доступа к информации и техническим средствам АС, а также принимать необходимые меры по устранению нарушений.

3.5. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания технических средств АС и отправке их в ремонт.

3.6. Контролировать соответствие аппаратно-программной конфигурации АС, приведенной в документации реальной конфигурации АС.

3.7. Генерировать ключи, личные идентификаторы, а так же пароли для пользователей АС.

3.8. Назначать права доступа и полномочий пользователей к объектам доступа (программам, файлам, каталогам, портам и устройствам ввода-вывода).

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

3.10. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования АС и осуществления НСД к информации и техническим средствам СВТ. При выявлении таковых сообщать о них начальнику отдела информационных технологий и эксплуатации автоматизированных систем.

3.11. Проводить инструктаж служащих Агентства (пользователей СВТ) по правилам работы с используемыми средствами и системами защиты

информации.

4. ПРАВА АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. Требовать от пользователей АС выполнения установленной технологии обработки информации и выполнения инструкций по обеспечению информационной безопасности и защите информации в АС.

4.2. Останавливать обработку информации в АС в случаях подтвержденных нарушений установленной технологии обработки данных, приводящих к нарушению функционирования СЗИ.

4.3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов АС.

4.4. Обращаться к начальнику отдела информационных технологий и эксплуатации автоматизированных систем с требованием прекращения работы в АС при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

4.5. Вносить предложения по совершенствованию технологических мер защиты.

5. ОТВЕТСТВЕННОСТЬ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. На администратора информационной безопасности возлагается персональная ответственность за качество и полноту проводимых им работ по обеспечению защиты информации в соответствии с его функциональными обязанностями.

5.2. Администратор информационной безопасности несет ответственность в соответствии с действующим законодательством за разглашение сведений ограниченного доступа, за нарушение требований нормативных методических документов и настоящего Положения.

6. ПОРЯДОК ДЕЙСТВИЙ В СЛУЧАЕ ВЫЯВЛЕНИЯ НАРУШЕНИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. В случае выявления фактов нарушений информационной безопасности администратор информационной безопасности принимает меры, необходимые для предотвращения негативных последствий нарушения в АС и информирует непосредственно начальника отдела информационных технологий и эксплуатации автоматизированных систем о факте нарушения и принятых мерах.

6.2. Администратор информационной безопасности анализирует и устанавливает причины возникшего нарушения и принимает меры по предотвращению подобных нарушений в дальнейшем.

6.3. В случае создания комиссии по расследованиям причин нарушения администратор информационной безопасности принимает участие в ее работе.

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем С.Г. Мунцев

Приложение № 9
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08. 2015 г. № 83-211

ПЕРЕЧЕНЬ ДОЛЖНОСТЕЙ ГОСУДАРСТВЕННЫХ ГРАЖДАНСКИХ СЛУЖАЩИХ АГЕНТСТВА ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ, ЗАМЕЩЕНИЕ КОТОРЫХ ПРЕДУСМАТРИВАЕТ ОСУЩЕСТВЛЕНИЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ЛИБО ОСУЩЕСТВЛЕНИЕ ДОСТУПА К ПЕРСОНАЛЬНЫМ ДАННЫМ

№ п/п	Наименование структурного подразделения	Наименование должности
1	Руководство	Руководитель
2		Заместитель руководителя
3		Секретарь руководителя
4	Отдел персонала и документационного обеспечения управления	Начальник отдела
5		Главный специалист
6		Ведущий специалист
7		Специалист 1 категории
8	Отдел информационных технологий и эксплуатации автоматизированных систем	Начальник отдела
9		Консультант
10		Ведущий специалист
11		Системный администратор
		Программист
12	Отдел бухгалтерского учета и отчетности	Заведующий отделом – главный бухгалтер
13		Заместитель главного бухгалтера

14		Старший бухгалтер
15		Бухгалтер

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем С.Г. Мунцев

Приложение № 10
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08. 2015 г. № 83-211

Типовое обязательство государственного гражданского служащего агентства труда и занятости населения Красноярского края, непосредственно осуществляющего обработку персональных данных, в случае расторжения с ним служебного контракта или трудового договора прекратить обработку персональных данных, ставших известными ему в связи с исполнением должностных обязанностей

Я,_____
(Фамилия, имя, отчество)

_____
(Должность)

_____
обязуюсь прекратить обработку персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, в случае расторжения со мной служебного контракта, освобождения меня от замещаемой должности и увольнения с государственной гражданской службы.

В соответствии со статьей 7 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» я уведомлен (а) о том, что персональные данные являются конфиденциальной информацией, и я обязан(а) не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, ставших известными мне в связи с исполнением должностных обязанностей, если иное не предусмотрено федеральным законом.

Я понимаю, что разглашение указанных сведений может нанести ущерб и вред субъектам персональных данных.

Ответственность, предусмотренная законодательством Российской Федерации в случае нарушения требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», мне разъяснена в полном объеме.

«__» _____20 __ г. _____/_____
подпись расшифровка Ф.И.О.

Приложение № 11
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08. 2015 г. №83-211

Типовая форма согласия на обработку персональных данных государственного гражданского служащего агентства труда и занятости населения Красноярского края, иных субъектов персональных данных

Я, _____
(Фамилия, имя, отчество)

проживающий (ая) по адресу:_____
_____
_____
(область, край, город, улица, дом, кв.)

_____
паспорт (другой документ, удостоверяющий личность) серия, номер, когда и кем выдан

_____

выражаю свое согласие на обработку своих персональных данных в соответствии со статьями 86 – 90 Трудового кодекса Российской Федерации, Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», главой 7 Федерального закона от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации», пунктом 1 части 1 статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в агентстве труда и занятости населения Красноярского края (далее - Оператор), расположенного по адресу: 660021, г. Красноярск, ул. Дубровинского, д. 110.

Согласие дается Оператору на обработку моих персональных данных, которые установлены в Перечне персональных данных, обрабатываемых оператором в связи с реализацией служебных и трудовых отношений.

Настоящее согласие представляется на осуществление любых правомерных действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу и трансграничную передачу), обезличивание, блокирование, уничтожение персональных данных, а также осуществление любых иных действий с моими персональными данными в соответствии с действующим законодательством Российской Федерации.

В случае моего поступления (прохождения) на государственную гражданскую службу Красноярского края настоящее согласие действует бессрочно, в случае включения в кадровый резерв на государственной

гражданской службе Красноярского края настоящее согласие действует до истечения пяти лет со дня включения в кадровый резерв на государственной гражданской службе Красноярского края. В иных случаях настоящее согласие действует в течение одного календарного года, если иное не предусмотрено законодательством Российской Федерации.

Мне известно, что по истечении срока действия согласия документы, содержащие мои персональные данные, подлежат уничтожению.

Настоящим согласием я признаю и подтверждаю, что в случае необходимости представления моих персональных данных для достижения указанных выше целей третьим лицам (в том числе иным государственным органам, государственным и муниципальным учреждениям здравоохранения, Красноярскому краевому фонду обязательного медицинского страхования, Пенсионному фонду Красноярского края, территориальным органам федеральной налоговой службы, страховым медицинским организациям и т.д.), а также в случае передачи функций и полномочий от Оператора другим лицам, Оператор вправе в необходимом объеме раскрывать для достижения указанных выше целей мои персональные данные таким третьим лицам, а также представлять таким третьим лицам документы, содержащие информацию о моих персональных данных. Настоящим согласием я признаю и подтверждаю, что настоящее согласие считается данным мною любым третьим лицам, указанным выше, и любые такие третьи лица имеют право на обработку моих персональных данных на основании настоящего согласия в целях и в объеме, указанных в настоящем согласии.

Я оставляю за собой право отозвать настоящее согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае назначения на должность государственной гражданской службы Красноярского края я выражаю также свое согласие на включение в общедоступные источники персональных данных следующих сведений: фамилия, имя, отчество, дата, месяц, год рождения, фотография, номера служебных телефонов, служебные адреса электронной почты.

В случае включения меня в кадровый резерв на государственной гражданской службе Красноярского края я выражаю также свое согласие на включение в общедоступные источники персональных данных следующих сведений: фамилия, имя, отчество, дата, месяц, год рождения, номера контактного телефона, адреса электронной почты, об образовании (когда и какие учебные заведения окончил (а), специальность и квалификация по диплому), о трудовой деятельности.

Я признаю, что общедоступные источники персональных данных могут размещаться в информационно-телекоммуникационной сети Интернет, издаваться в виде справочников, передаваться по электронной почте и по иным каналам связи.

Мне известно, что в соответствии с Федеральным законом

от 27.07.2006 № 152-ФЗ «О персональных данных» мои персональные данные могут быть в любое время исключены из общедоступных источников персональных данных по моему требованию либо по решению суда или иных уполномоченных государственных органов.

Мне известно, что обработка Оператором моих персональных данных осуществляется в информационных системах, с применением электронных и бумажных носителей информации.

«__» _____ 20__ г. _____ /_____

подпись расшифровка Ф.И.О.

Приложение № 12
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08. 2015 г. №83-211

Типовая форма согласия на обработку персональных данных директора краевого государственного учреждения службы занятости населения, иных субъектов персональных данных

Я, _____
(Фамилия, имя, отчество)

проживающий (ая) по адресу:_____
_____
_____
(область, край, город, улица, дом, кв.)

_____
паспорт (другой документ, удостоверяющий личность) серия, номер, когда и кем выдан

_____
выражаю свое согласие на обработку своих персональных данных в соответствии со статьями 86 – 90 Трудового кодекса Российской Федерации, Федеральным законом от 02.05.2006 № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» в агентстве труда и занятости населения Красноярского края (далее - Оператор), расположенного по адресу: 660021, г. Красноярск, ул. Дубровинского, д. 110.

Согласие дается Оператору на обработку моих персональных данных, которые установлены в Перечне персональных данных, обрабатываемых оператором в связи с реализацией служебных и трудовых отношений.

Настоящее согласие представляется на осуществление любых правомерных действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу и трансграничную передачу), обезличивание, блокирование, уничтожение персональных данных, а также осуществление любых иных действий с моими персональными данными в соответствии с действующим законодательством Российской Федерации.

В случае моего назначения на должность _____
_____
(наименование должности и учреждения.)

настоящее согласие действует бессрочно, в случае включения в резерв управленческих кадров Красноярского края настоящее согласие действует до истечения пяти лет со дня включения в резерв управленческих кадров

Красноярского края. В иных случаях настоящее согласие действует в течение одного календарного года, если иное не предусмотрено законодательством Российской Федерации.

Мне известно, что по истечении срока действия согласия документы, содержащие мои персональные данные, подлежат уничтожению.

Настоящим согласием я признаю и подтверждаю, что в случае необходимости представления моих персональных данных для достижения указанных выше целей третьим лицам (в том числе иным государственным органам, государственным и муниципальным учреждениям здравоохранения, Красноярскому краевому фонду обязательного медицинского страхования, Пенсионному фонду Красноярского края, территориальным органам федеральной налоговой службы, страховым медицинским организациям и т.д.), а также в случае передачи функций и полномочий от Оператора другим лицам, Оператор вправе в необходимом объеме раскрывать для достижения указанных выше целей мои персональные данные таким третьим лицам, а также представлять таким третьим лицам документы, содержащие информацию о моих персональных данных. Настоящим согласием я признаю и подтверждаю, что настоящее согласие считается данным мною любым третьим лицам, указанным выше, и любые такие третьи лица имеют право на обработку моих персональных данных на основании настоящего согласия в целях и в объеме, указанных в настоящем согласии.

Я оставляю за собой право отозвать настоящее согласие посредством составления соответствующего письменного документа, который может быть направлен мной в адрес Оператора по почте заказным письмом с уведомлением о вручении либо вручен лично под расписку представителю Оператора.

В случае назначения на должность я выражаю также свое согласие на включение в общедоступные источники персональных данных следующих сведений: фамилия, имя, отчество, дата, месяц, год рождения, фотография, номера служебных телефонов, служебные адреса электронной почты.

В случае включения меня в кадровый резерв управленческих кадров Красноярского края я выражаю также свое согласие на включение в общедоступные источники персональных данных следующих сведений: фамилия, имя, отчество, дата, месяц, год рождения, номера контактного телефона, адреса электронной почты, об образовании (когда и какие учебные заведения окончил (а), специальность и квалификация по диплому), о трудовой деятельности.

Я признаю, что общедоступные источники персональных данных могут размещаться в информационно-телекоммуникационной сети Интернет, издаваться в виде справочников, передаваться по электронной почте и по иным каналам связи.

Мне известно, что в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» мои персональные данные могут быть в любое время исключены из общедоступных источников персональных данных по моему требованию либо по решению суда или иных

уполномоченных государственных органов.

Мне известно, что обработка Оператором моих персональных данных осуществляется в информационных системах, с применением электронных и бумажных носителей информации.

«__» _____ 20__ г. _____ /_____

подпись расшифровка Ф.И.О.

Приложение № 13
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08 2015 г. №53-211

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

Мне, _____,
(Фамилия, имя, отчество)

разъяснены юридические последствия отказа предоставить свои персональные данные в агентство труда и занятости населения Красноярского края.

В соответствии со статьями 26, 42 Федерального закона от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации», Положением о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела, утвержденного Указом Президента Российской Федерации от 30.05.2005 № 609, определен перечень персональных данных, которые субъект персональных данных обязан предоставить в связи с поступлением или прохождением государственной гражданской службы.

Согласно статьям 57, 65, 69 Трудового кодекса Российской Федерации субъект персональных данных, поступающий на работу или работающий, обязан представить определенный перечень информации о себе.

Без предоставления субъектом персональных данных, обязательных для заключения служебного контракта (трудового договора) сведений, служебный контракт (трудовой договор) не может быть заключен.

На основании пункта 11 части 1 статьи 33 Федерального закона от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации» служебный контракт прекращается вследствие нарушения установленных обязательных правил его заключения, если это нарушение исключает возможность замещения должности гражданской службы.

«__» _____ 20__ г. _____ / _____
подпись расшифровка Ф.И.О.

Приложение № 14
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08. 2015 г. №83-211

ПОРЯДОК ДОСТУПА ГОСУДАРСТВЕННЫХ ГРАЖДАНСКИХ СЛУЖАЩИХ АГЕНТСТВА ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ В ПОМЕЩЕНИЯ, В КОТОРЫХ ВЕДЕТСЯ ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Настоящий Порядок разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановлением Правительства Российской Федерации от 21.03.2012 № 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» и другими нормативными правовыми актами.

2. Персональные данные относятся к конфиденциальной информации. Государственные гражданские служащие (далее - служащие) агентства труда и занятости населения Красноярского края (далее - Агентство), получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

3. Обеспечение безопасности персональных данных от уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных достигается, в том числе установлением правил доступа в помещения, где обрабатываются персональные данные.

4. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется в охраняемых помещениях. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

5. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только сотрудники Агентства, уполномоченные на обработку персональных данных, утвержденные приказом руководителя.

6. Ответственным за организацию доступа в помещения, в которых ведется обработка персональных данных, является ответственный за организацию обработки персональных данных Агентства.

7. Нахождение лиц в помещениях Агентства, не являющихся уполномоченными служащими на обработку персональных данных, возможно только в сопровождении уполномоченного служащего Агентства на время, ограниченное необходимостью решения вопросов, связанных с исполнением должностных обязанностей.

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем С.Г. Мунцев

Приложение № 15
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08. 2015 г. №83-211

ПОЛОЖЕНИЕ
ОБ ЭКСПЕРТНОЙ КОМИССИИ В АГЕНСТВЕ ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об экспертной комиссии агентства труда и занятости населения Красноярского края (далее - Положение) разработано в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К).

Экспертная комиссия агентства труда и занятости населения Красноярского края (далее – «комиссия») является коллегиальным органом, координирующим деятельность структурных и подчиненных подразделений по реализации задач в сфере защиты информации ограниченного доступа в Агентстве.

1.2. Основными задачами комиссии являются:

1.2.1. Оценка эффективности принимаемых структурными и подведомственными подразделениями мер по защите информации ограниченного доступа и организация разработки предложений по ее совершенствованию.

1.2.2. Определение (уточнение) степени секретности сведений, относящихся к компетенции агентства труда и занятости населения Красноярского края (далее – Агентства).

1.2.3. Экспертиза ценности документов, содержащих сведения, ограниченного доступа, их отбор для передачи в специальный фонд Агентства, или уничтожения.

1.3. В своей деятельности комиссия руководствуется Конституцией Российской Федерации, федеральными законами и иными нормативными актами Российской Федерации, регулирующими вопросы защиты информации ограниченного доступа, а также настоящим Положением.

1.4. Комиссию возглавляет председатель – заместитель

руководителя Агентства.

1.5. В состав комиссии включаются лица из числа руководителей и наиболее подготовленных сотрудников Агентства, имеющих соответствующую форму допуска к работе со сведениями ограниченного доступа. Персональный состав комиссии утверждается приказом руководителя агентства.

1.6. Организационно-техническое обеспечение деятельности комиссии осуществляет отдел персонала и документационного обеспечения управления, отдел информационных технологий и эксплуатации автоматизированных систем, в части своей компетенции.

2. ОСНОВНЫЕ ПОЛНОМОЧИЯ КОМИССИИ

2.1. В пределах своей компетенции рассматривать вопросы о защите информации ограниченного доступа в Агентстве.

2.2. Вносить руководству Агентства предложения по совершенствованию данной работы.

2.3. Заслушивать начальников отделов Агентства о состоянии защиты информации ограниченного доступа.

2.4. Давать рекомендации по внедрению в практическую деятельность положительного опыта работы других организаций, научных достижений по обеспечению защиты информации ограниченного доступа.

2.5. Рассматривать в пределах компетенции в порядке, установленном законодательством Российской Федерации, вопросы о возможности передачи сведений ограниченного доступа сторонним организациям.

2.6. Координировать деятельность Агентства по специальной подготовке и (или) повышению квалификации специалистов по вопросам защиты информации ограниченного доступа.

2.7. Рассматривать вопросы и согласовывать акты об уничтожении отдельных документов, дел, учетных форм, нормативных правовых актов, утративших практическое значение и не имеющих научной и практической ценности.

2.8. Участвовать по поручению руководителя Агентства в проверках наличия документов с информацией ограниченного доступа, дел с такими документами и других носителей сведений ограниченного доступа, независимо от времени их поступления (изготовления). Рассматривать результаты проверок, разрабатывать меры по устранению выявленных нарушений и недостатков в обеспечении режима безопасности.

2.9. Участвовать по поручению руководителя Агентства в ежегодных проверках наличия информации ограниченного доступа.

2.10. Рассматривать по поручению руководителя Агентства другие вопросы в области защиты информации ограниченного доступа.

3. ОРГАНИЗАЦИЯ И ОБЕСПЕЧЕНИЕ ДЕЯТЕЛЬНОСТИ КОМИССИИ

3.1. Основной формой работы комиссии являются плановые заседания, которые проводятся не реже одного раза в год. В случае необходимости председатель комиссии может назначать внеочередные заседания комиссии.

3.2. План работы комиссии формируется председателем комиссии на полугодие и включает перечень вопросов, подлежащих рассмотрению на заседаниях комиссии, с указанием по каждому вопросу месяца его рассмотрения, членов комиссии, подразделений Агентства, ответственных за подготовку вопроса. Проект плана работы комиссии на полугодие, согласованный с ответственными исполнителями и подписанный председателем комиссии, представляется на утверждение руководителя Агентства соответственно.

3.3. Утвержденный план работы комиссии в десятидневный срок направляется отделом персонала и документационного обеспечения управления членам комиссии, указанным в плане.

3.4. Решение об изменении утвержденного плана работы комиссии в части формулировки рассматриваемого вопроса, переноса срока его рассмотрения либо снятия вопроса с обсуждения принимается руководителем Агентства по обращению ответственного исполнителя, согласованному с председателем комиссии. Копия заявления, рассмотренного руководителем Агентства, передается председателю комиссии для дальнейшего исполнения.

3.5. При необходимости включения в повестку очередного заседания комиссии дополнительных вопросов инициатором готовятся предложения, которые сообщаются председателю комиссии и по результатам рассмотрения направляются в отдел персонала и документального обеспечения управления не позднее чем за месяц до предполагаемого срока проведения заседания комиссии.

3.6. Заседание комиссии и принятые на нем решения считаются правомочными, если на заседании присутствует не менее половины членов комиссии. Решения комиссии принимаются большинством голосов членов комиссии. Право решающего голоса предоставлено только членам комиссии. Приглашенные должностные лица имеют право совещательного голоса. При равенстве голосов принятым считается решение, за которое проголосовал председательствующий на заседании.

3.7. Решение комиссии оформляется протоколом и вступает в силу после его подписания председательствующим и секретарем комиссии.

3.8. В случае несогласия с принятым решением каждый член комиссии имеет право изложить в письменном виде свое особое мнение по рассматриваемому вопросу, которое подлежит обязательному

приобщению к протоколу заседания.

3.9. Решения комиссии, принятые в соответствии с ее полномочиями, обязательны для исполнения членами комиссии и подразделениями Агентства.

3.10. Председатель комиссии:

3.10.1. Организует деятельность комиссии и обеспечивает контроль исполнения ее решений.

3.10.2. Организует выполнение комиссией поручений руководителя Агентства.

3.10.3. Докладывает руководителю Агентства по вопросам, отнесенным к компетенции комиссии.

3.10.4. Определяет порядок рассмотрения комиссией отдельных вопросов, входящих в ее компетенцию.

3.10.5. Определяет персональный состав групп, создаваемых для определения степени секретности сведений и проведения экспертиз степени секретности сведений, содержащихся в утраченных документах или разглашенной информации, и при необходимости утверждает подготовленные этими группами соответствующие заключения.

3.11. Председатель комиссии имеет право:

3.11.1. Принимать решение, о привлечении должностных лиц подразделений Агентства для выполнения аналитических и экспертных работ.

3.11.2. Запрашивать и получать в установленном порядке от подразделений Агентства, должностных лиц органов государственной власти субъектов Российской Федерации, органов местного самоуправления, предприятий, учреждений и организаций необходимую для осуществления деятельности комиссии информацию.

3.11.3. Поручать заместителю (одному из заместителей) председателя подготовку и проведение отдельных заседаний комиссии.

3.12. Секретарь комиссии:

3.12.1. Осуществляет сбор предложений для включения в проект плана работы комиссии и в повестку дня очередного заседания.

3.12.2. Контролирует своевременность представления материалов на рассмотрение комиссии.

3.12.3. По указанию председателя (заместителей председателя) комиссии организует работу по подготовке экспертными группами заключений о степени секретности носителей информации, а также заключений экспертов.

3.12.4. При необходимости детальной проработки заключений о степени секретности носителей информации по согласованию с председателем (заместителями председателя) комиссии продлевает сроки их подготовки.

3.12.5. Проверяет соответствие заключений о степени секретности и заключений экспертов формам, установленным федеральным законодательством Российской Федерации.

3.12.6. Обеспечивает членов комиссии необходимыми документами, информирует их о сроках проведения заседаний.

3.12.7. Доводит решения комиссии до сведения должностных лиц в части, их касающейся.

3.12.8. Организует делопроизводство комиссии, хранение и использование ее документов.

3.13. Комиссия в лице председателя, его заместителей или секретаря имеет право не принимать к рассмотрению и возвращать для доработки документы, исполненные с нарушением правил их подготовки и оформления.

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем  С.Г. Мунцев

Приложение № 16
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08. 2015 г. № 83-211

ИНСТРУКЦИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ПОДКЛЮЧЕНИИ И ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ОБЩЕГО ПОЛЬЗОВАНИЯ В АГЕНТСТВЕ ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция по обеспечению информационной безопасности при подключении и использовании информационно-вычислительной сети общего пользования в агентстве труда и занятости населения Красноярского края (далее - Инструкция) разработана в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К).

1.2. Инструкция по обеспечению информационной безопасности при подключении и использовании информационно-вычислительной сети общего пользования агентства труда и занятости населения Красноярского края (далее - Агентство) устанавливает требования к работе в сети «Интернет» служащих Агентства.

1.3. В настоящей Инструкции используются следующие термины и определения:

Интернет - глобальная информационная система, имеющая логически взаимосвязанное единое адресное пространство, являющаяся совокупностью общедоступных информационных сетей и основанная на использовании стека протоколов TCP/IP (протокол управления передачей/Интернет – протокол);

Администратор – лицо, ответственное за использование, техническое обеспечение и функционирование средств вычислительной техники, имеющих выход в сеть «Интернет»;

Пользователь – лицо, допущенное к работе в сети «Интернет»;

Логин – регистрационное имя пользователя, выраженное комбинацией цифр, букв и (или) знаков;

Пароль – кодовая комбинация, состоящая из букв, цифр и (или) знаков, подтверждающая правомочность пользователя на осуществление входа в сеть «Интернет» с определенным для него логином;

Ресурс (сайт) – логическая и (или) физическая часть вычислительной системы и совокупность информационных ресурсов, предназначенных для общего доступа пользователю, подключенному к сети «Интернет», имеющему соответствующие технические средства получить доступ к части или всей информации на платной или бесплатной основе;

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

1.3. Работники, использующие ресурсы сети «Интернет» подразделяются на следующие категории: администратор и пользователь.

2. ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К ПОРЯДКУ ПОДКЛЮЧЕНИЯ И ОРГАНИЗАЦИИ РАБОТЫ В СЕТИ «ИНТЕРНЕТ»

2.1. Приказом руководителя Агентства назначается администратор информационной безопасности.

2.2. Подключение работников к сети «Интернет» проводится с обоснованной служебной необходимостью.

2.3. Подключение к информационным ресурсам сети «Интернет» технических средств, информационных систем, сетей связи и автономных персональных компьютеров, в которых обрабатывается информация, содержащая сведения, составляющие служебную и иную охраняемую законом тайну, а также для которых установлены особые правила доступа, без технических средств защиты информации запрещается.

2.4. Включение технических средств, информационных систем, сетей связи и автономных персональных компьютеров, проводится при обязательном использовании сертифицированных средств защиты информации, обеспечивающих ее целостность и доступность, в том числе криптографических, для подтверждения достоверности информации (антивирусное программное обеспечение, система защиты от несанкционированного доступа, межсетевые экраны и другие средства защиты).

2.5. Размещение технических средств, подключаемых к открытым информационным системам и сетям связи, включая сеть «Интернет», используемым при информационном обмене в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, ограниченного доступа, осуществляется только при наличии сертификата, разрешающего эксплуатацию таких средств в указанных помещениях.

2.6. Контроль доступа к ресурсам сети «Интернет» служащих Агентства возлагается на администратора информационной безопасности.

3. ФУНКЦИИ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОРГАНИЗАЦИИ РАБОТЫ В СЕТИ «ИНТЕРНЕТ»

3.1. Администратор информационной безопасности выполняет следующие функции:

3.1.1. Организует допуск пользователей к работе в сети «Интернет»;

3.1.2. Обеспечивает инсталляцию, настройку, обновление программного обеспечения систем защиты от несанкционированного доступа и реализацию требований информационной безопасности и автоматического учета времени работы пользователей на технических средствах, подключенных к сети «Интернет»;

3.1.3. Обеспечивает работоспособность и актуализацию системы антивирусной защиты рабочих мест, подключенных к сети «Интернет»;

3.1.4. Незамедлительно докладывает начальнику отдела информационных технологий и эксплуатации автоматизированных систем о фактах нарушения требований настоящей Инструкции и попытках несанкционированного доступа к техническим средствам, за которые он несет ответственность;

3.1.5. В случае нарушения требований настоящей Инструкции, по указанию руководства Агентства, прекращает допуск пользователей к использованию ресурсов сети «Интернет».

4. ТРЕБОВАНИЯ К ИСПОЛЬЗОВАНИЮ СЕТИ «ИНТЕРНЕТ»

4.1. Пользователи обязаны:

4.1.1. Соблюдать требования настоящих Правил;

4.1.2. Соблюдать при доступе к ресурсам сети «Интернет» правила, установленные владельцами используемых ресурсов;

4.1.3. Сообщать администратору информационной безопасности о сбоях, возникших в процессе работы в сети «Интернет».

4.2. Пользователям запрещается:

4.2.1. Оставлять без присмотра рабочее место, подключенное к сети «Интернет»;

4.2.2. Предоставлять логин и пароль другим лицам для работы в сети «Интернет»;

4.2.3. Использовать доступ к сети «Интернет» в личных целях, не связанных с выполнением служебных обязанностей;

4.2.4. Осуществлять несанкционированный доступ к информационным ресурсам сети «Интернет», а также повреждать, уничтожать или фальсифицировать ее информационные ресурсы;

4.2.5. Самостоятельно устанавливать или удалять программы на компьютерах, подключенных к сети «Интернет», изменять настройки

операционной системы и приложений, влияющих на работу сетевого оборудования и сетевых ресурсов;

4.2.6. Изменять техническую конфигурацию средств электронной вычислительной техники, сетевого и периферийного оборудования и подключать дополнительное оборудование;

4.2.7. Передавать в сеть «Интернет» информацию, содержащую информацию ограниченного доступа, и (или) иные сведения, охраняемые законодательством Российской Федерации;

4.2.8. Нарушать регламент учетной системы и системы статистики, в том числе повреждать или дезинформировать вышеуказанные системы;

4.2.9. Осуществлять рассылку информации, не имеющей отношения к служебной деятельности.

4.3. В случае выявления нарушения требований настоящей Инструкции запрещается использование сети «Интернет» на рабочем месте до момента устранения нарушения и причин их возникновения.

4.4. Пользователь несет личную ответственность за информационный обмен, совершаемый от его имени (с его логином и паролем) и нарушение требований Инструкции.

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем С.Г. Мунцев

Приложение № 17
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08. 2015 г. № 83-211

ИНСТРУКЦИЯ ПО УЧЕТУ, МАРКИРОВКЕ, ОЧИСТКЕ И УТИЛИЗАЦИИ ОТЧУЖДАЕМЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ И ЖЕСТКИХ МАГНИТНЫХ ДИСКОВ В АГЕНТСТВЕ ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ

Инструкция по учету, маркировке, очистке и утилизации отчуждаемых носителей информации и жестких магнитных дисков (далее - Инструкция) разработана в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К).

1. Все находящиеся на хранении и в обращении в агентстве труда и занятости населения Красноярского края (далее - Агентство) съемные носители с персональными данными и жесткие магнитные диски подлежат учёту. Каждый съемный носитель и жесткий магнитный диск с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

2. Учет и выдачу съемных носителей и жестких магнитных дисков персональных данных по форме (Приложение №1) осуществляет администратор информационной безопасности Агентства, на которого возложены функции хранения носителей персональных данных. Служащие Агентства получают учтенный съемный носитель от администратора информационной безопасности для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

3. Служащим Агентства запрещается:

хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

выносить съемные носители с персональными данными

из служебных помещений для работы с ними на дому и т. д.

4. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные. Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленным для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения начальника отдела.

5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений немедленно ставится в известность начальник соответствующего структурного подразделения. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы персонального учета съемных носителей персональных данных.

6. Съемные носители персональных данных, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется уполномоченной комиссией. По результатам уничтожения носителей составляется акт по форме (Приложение №2).

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем С.Г. Мунцев

Приложение №1
к Инструкции по учету,
маркировке, очистке и
утилизации отчуждаемых
носителей информации
и жестких магнитных дисков

ЖУРНАЛ

учета съемных носителей персональных данных

Начат « »_____ г.

Окончен « »_____ г.

№ п/п	Метка съемного носителя	Фамилия исполнителя	Действие (получил, вернул, передал)	Дата записи информации	Подпись исполнителя	Примечание

Приложение №2
к Инструкции по учету,
маркировке, очистке
и утилизации отчуждаемых
носителей информации и
жестких магнитных дисков

АКТ

уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом_____
№ _____от_____в составе:
1.
2.
3.
провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер съемного носителя	Пояснения

Всего съемных носителей_____(цифрами и прописью).
На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации.
Перечисленные съемные носители уничтожены путем _____ (разрезания, измельчения, сжигания и т.п.) и сданы для уничтожения предприятию по утилизации вторичного сырья

_____
(наименование предприятия) (Дата)

Председатель комиссии

Члены комиссии

Приложение № 18
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08 2015 г. №83-211

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ В АГЕНТСТВЕ ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Инструкция по организации антивирусной защиты информационных систем в агентстве труда и занятости населения Красноярского края (далее - Инструкция) разработана в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К).

1.1. Настоящая Инструкция предназначена для организации порядка проведения антивирусного контроля в агентстве труда и занятости населения Красноярского края (далее - Агентство), с целью предотвращения несанкционированных вредоносных воздействий на информационные ресурсы и возникновения фактов заражения программного обеспечения (далее - ПО) компьютерными вирусами.

1.2. В настоящей Инструкции использованы следующие термины и определения:

a) Антивирусное ПО – набор программ для обнаружения компьютерных вирусов и других вредоносных программ и лечения инфицированных файлов, а также для профилактики, предотвращения заражения файлов или операционной системы вредоносным кодом;

b) Антивирусные базы – файлы, используемые антивирусным ПО при поиске вредоносных программ, периодически обновляемые разработчиком антивирусного ПО;

c) Антивирусный контроль – проверка информации (файла, сообщения и т.п.) на предмет наличия вредоносных программ;

d) Вредоносная программа – компьютерная программа, предназначенная для осуществления несанкционированного доступа и (или)

воздействия на информационные ресурсы;

e) Защищаемый компьютер – электронно-вычислительная машина (персональный компьютер или сервер), используемая для обработки данных;

f) Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу, в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

g) Пользователь – служащий Агентства или другое лицо, использующее в работе средства электронно-вычислительной техники Агентства;

h) Съемный носитель информации – носитель информации, предназначенный для ее автономного хранения, независимо от места использования (съемные винчестеры, флэш-память, CD, DVD, дискеты и др.).

1.3. Требования настоящей Инструкции обязательны для выполнения всеми пользователями.

1.4. Общее и методическое руководство обеспечением антивирусной защиты информационной системы персональных данных в Агентстве осуществляется отделом информационных технологий и эксплуатации автоматизированных систем.

1.5. Пользователь отвечает за обеспечение устойчивой работоспособности и информационной безопасности вверенного ему объекта вычислительной техники при обработке персональных данных и выполнения других видов работ.

1.6. Техническое обслуживание средств вычислительной техники, уборка помещения и т.п. проводятся под контролем пользователя или уполномоченного лица.

1.7. В качестве средства антивирусной защиты в Агентстве применяется программное обеспечение Dr.Web (далее - антивирусное ПО).

2. УСТАНОВКА АНТИВИРУСНОГО ПО

2.1. Установку антивирусного ПО производит администратор информационной безопасности Агентства.

2.2. В Агентстве может использоваться только лицензионное антивирусное ПО, сертифицированное ФСТЭК России.

2.3. Установка антивирусного ПО производится индивидуально на каждый защищаемый компьютер с обязательным предохранением настроек от изменения паролем.

2.4. Пользователям запрещается отключать средства антивирусной защиты и самостоятельно вносить изменения в настройки антивирусного ПО.

2.5. Ярлык для запуска антивирусного ПО должен быть вынесен на «Рабочий стол» операционной системы.

3. ПОРЯДОК ОБНОВЛЕНИЯ АНТИВИРУСНЫХ БАЗ

3.1. Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети Агентства, должна осуществляться ежедневно в автоматическом режиме через специальный сервер обновлений (по рабочим дням).

3.2. Обновление антивирусных баз на защищаемых компьютерах, не подключенных к локальной сети Агентства, должно осуществляться с использованием маркированных съемных носителей информации, в обязательном порядке проверяемых антивирусным ПО перед их использованием или принудительным подключением к локальной сети служащими отдела информационных технологий и эксплуатации автоматизированных систем.

3.3. Проверка критических областей защищаемого компьютера, заражение которых вредоносными программами может привести к серьезным последствиям, должна проводиться автоматически при каждой его загрузке.

3.4. Актуализация антивирусных баз на защищаемых компьютерах, подключенных к локальной сети Агентства, контролируется пользователем самостоятельно ежедневно и в случае нарушения пользователь должен не принимать никаких мер и срочно сообщить администратору информационной безопасности.

4. ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ АНТИВИРУСНОГО КОНТРОЛЯ

4.1. Пользователь осуществляет контроль за целевым использованием автоматизированного рабочего места, а также всех его внешних устройств.

4.2. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, сообщения электронной почты и т.д.), получаемая и передаваемая по телекоммуникационным каналам, а также данные на съемных носителях информации. Контроль входящей и исходящей информации на защищаемых компьютерах должен осуществляться непрерывно посредством постоянно работающего компонента антивирусного ПО («монитора»).

4.3. Всё программное обеспечение, устанавливаемое на защищаемые компьютеры, должно предварительно проверяться на наличие вредоносных программ.

4.4. Не реже одного раза в две недели должна проводиться полная проверка всех файлов, хранящихся на жестких дисках защищаемого компьютера.

4.5. Внеочередной антивирусный контроль всех дисков и файлов защищаемого компьютера должен выполняться:

сразу после установки или изменения ПО;

после подключения автономного компьютера к локальной сети;

при возникновении подозрения на наличие вредоносных программ

(нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

4.6. В сомнительных случаях для определения факта наличия или отсутствия вредоносных программ к проверке необходимо привлечь администратора информационной безопасности.

5. ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ ПРИ ОБНАРУЖЕНИИ ВРЕДОНОСНЫХ ПРОГРАММ

5.1. В случае обнаружения при проведении антивирусной проверки вредоносных программ пользователи обязаны:

приостановить все операции, связанные с обработкой файлов на защищаемом компьютере;

немедленно поставить в известность о факте обнаружения вредоносных программ непосредственного начальника отдела, владельцев зараженных или поврежденных вредоносными программами файлов, другие отделы, использующие эти файлы в работе;

совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

провести лечение зараженных файлов совместно с администратором информационной безопасности;

в случае обнаружения не поддающегося лечению вируса, пользователь обязан удалить инфицированный файл в соответствующую папку антивирусного ПО, и проверить работоспособность компьютера совместно с администратором информационной безопасности.

6. ОТВЕТСТВЕННОСТЬ ЗА ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ИНСТРУКЦИИ

6.1. Ответственность за организацию антивирусной защиты информации на компьютерах несет начальник отдела информационных технологий и эксплуатации автоматизированных систем.

6.2. Ответственность за соблюдение требований настоящей Инструкции несут пользователи.

6.3. Ответственность за своевременное обновление антивирусных баз на сервере обновлений несет администратор информационной безопасности.

6.4. Ответственность за своевременное обновление антивирусных баз и получение новых лицензионных ключей при истечении их срока действия несет администратор информационной безопасности.

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем  С.Г. Мунцев

Приложение № 19
к приказу агентства труда
и занятости населения
Красноярского края
от 28.08. 2015 г. № 53-211

ИНСТРУКЦИЯ ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ В АГЕНТСТВЕ ТРУДА И ЗАНЯТОСТИ НАСЕЛЕНИЯ КРАСНОЯРСКОГО КРАЯ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Инструкция по организации парольной защиты информационных систем в агентстве труда и занятости населения Красноярского края (далее - Инструкция) разработана в соответствии с Федеральным законом Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСТЭК России от 11.02.2013 №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К).

1.1. Настоящая Инструкция определяет порядок защиты ресурсов автоматизированных систем, обрабатывающей конфиденциальной информации, с использованием подсистемы парольной защиты от несанкционированного доступа в автоматизированных системах объекта информатизации агентства труда и занятости населения Красноярского края (далее - Агентство), предназначенных для обработки конфиденциальной информации.

1.2. Парольная защита при работе на объекте информатизации осуществляется с целью предотвращения несанкционированного доступа к информации, содержащей сведения ограниченного доступа.

1.3. Парольная защита объекта информатизации является составной частью подсистемы управления доступом общей системы защиты от несанкционированного доступа.

1.4. К основным видам паролей относятся:

пароли доступа к локальным ресурсам отдельного компьютера объекта информатизации;

пароли доступа к прикладным программам, обеспечивающим доступ к информации;

пароль доступа средств защиты от несанкционированного доступа;

пароли систем доступа встроенных в используемые операционные

системы.

2. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

2.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в защищаемых автоматизированных системах возлагается на администратора информационной безопасности.

2.3. Личные пароли доступа к ресурсам в автоматизированных системах, системе защиты от несанкционированного доступа, а также пароли встроенных в операционные системы доступа выбираются пользователями самостоятельно, но при этом необходимо руководствоваться следующими требованиями:

длина пароля должна быть не менее 8 символов;

в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры и специальные символы;

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

пароль не должен включать в себя легко вычисляемые (угадываемые) сочетания символов (имена, фамилии, отчества, наименования АРМ организации и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, ADM и т.п.) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об ответственном исполнителе;

не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, QWERTY, 123456 или 1йфячыц2 и т.п.);

не использовать ранее использованные пароли;

минимальное время применения пароля - не менее 2 дней;

максимальное время применения пароля - не более чем 90 дня.

2.3. Лица, использующие парольную защиту, обязаны:

четко знать и строго выполнять требования настоящей Инструкции;

своевременно сообщать администратору информационной безопасности обо всех нештатных ситуациях, нарушениях работы подсистем защиты от несанкционированного доступа, возникающих при работе с паролями.

2.4. При организации парольной защиты запрещается:

записывать свои пароли в очевидных местах (внутренние стенки ящика стола, на передней панели монитора, на обратной стороне клавиатуры и т.д.);

хранить пароли в записанном виде в рабочих тетрадях, на отдельных листах бумаги;

сообщать посторонним лицам свои пароли, а так же сведения о применяемой системе защиты от несанкционированного доступа.

3.6. Компрометация действующих паролей является чрезвычайным происшествием, о чем пользователь сообщает администратору информационной безопасности.

3.7. Скомпрометированные пароли выводятся из действия немедленно.

3.8. Пользователь в случае компрометации действующих паролей принимает меры по предотвращению работы с АРМ, где используются скомпрометированные пароли, до ввода новых паролей, сообщив немедленно о случившимся администратору информационной безопасности.

3.9. С получением информации о случае компрометации паролей администратор информационной безопасности проводит анализ и оценку данного случая, после чего, изменяет пароли в системе защиты информации от несанкционированного доступа.

3.10. По каждому случаю, связанному с компрометацией действующих паролей, администратор информационной безопасности организует и проводит служебную проверку. По результатам расследования к лицам, допустившим разглашение паролей, применяются необходимые административные или дисциплинарные меры.

Временно замещающий должность
начальника отдела информационных
технологий и эксплуатации
автоматизированных систем С.Г. Мунцев