Приложение

к приказу Администрации

Тракторозаводского района

города Челябинска

от \_\_\_\_\_\_\_\_\_\_\_\_№\_\_\_\_\_\_\_

Положение

о порядке обработки и обеспечения безопасности персональных данных   
в Администрации Тракторозаводского района города Челябинска

I. Общие положения

1. Настоящее Положение о порядке обработки и обеспечения безопасности персональных данных в Администрации Тракторозаводского района города Челябинска (далее – Положение) устанавливает порядок и требования   
к обработке и обеспечению безопасности персональных данных, регулирует отношения, связанные с обработкой таких персональных данных, осуществляемой в Администрации Тракторозаводского района   
города Челябинска (далее – Администрация района).

2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, федеральными законами от 27.07.2006 № 152-ФЗ  
«О персональных данных» (далее – Федеральный закон № 152-ФЗ), от 02.03.2007 № 25-ФЗ «О муниципальной службе в Российской Федерации», постановлениями Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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», от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3. В сферу действия настоящего Положения попадают отношения, связанные с обработкой персональных данных с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

4. Настоящее Положение устанавливает процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере персональных данных, а также определяющие для каждой цели обработки персональных данных содержание обрабатываемых персональных данных, категории субъектов, персональные данные которых обрабатываются (далее – субъект персональных данных), сроки обработки и хранения таких персональных данных, порядок уничтожения при достижении целей обработки или при наступлении иных законных оснований.

II. Обработка персональных данных

5. Операторами персональных данных (далее – оператор) являются структурные подразделения Администрации района самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Муниципальные служащие и работники структурных подразделений Администрации района, получившие доступ к персональным данным (далее – работник), обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законодательством Российской Федерации.

Типовые формы обязательств лиц, осуществляющих обработку персональных данных, о неразглашении сведений, содержащих персональные данные, утверждаются правовыми актами Администрации района.

6. При обработке персональных данных оператором должны соблюдаться следующие общие требования:

1. при определении объема и содержания обрабатываемых персональных данных оператор руководствуется законодательством Российской Федерации, Челябинской области, муниципальными правовыми актами города Челябинска;
2. при принятии решений, затрагивающих интересы субъектов персональных данных, оператор не вправе основываться на сведениях, полученных исключительно в результате автоматизированной обработки персональных данных субъекта персональных данных;
3. персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на разных материальных носителях;
4. оператор обеспечивает защиту персональных данных субъектов от их неправомерного использования, утраты;
5. субъекты персональных данных (их законные представители) должны быть ознакомлены под подпись с организационно-распорядительными документами Администрации района, устанавливающими порядок обработки и обеспечения безопасности персональных данных, а также об их правах и обязанностях в этой области.

7. Обработка персональных данных включает в себя следующие действия: сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Способы обработки персональных данных в Администрации района включают:

1. копирование оригиналов документов;
2. внесение сведений в учетные формы (на бумажных и электронных носителях);
3. формирование персональных данных в ходе их обработки;
4. внесение персональных данных в информационные системы персональных данных Администрации района (далее – ИСПДн);
5. непосредственное получение оригиналов необходимых документов.

8. Обработка персональных данных в Администрации района осуществляется в рамках осуществления функций, установленных Администрации Тракторозаводского района города Челябинска, утвержденным решением Челябинской городской Думы от 25.06.2024 № 51/13 в целях:

1. реализации норм законодательства Российской Федерации о муниципальной службе и противодействии коррупции;
2. контроля за эффективным и целевым расходованием средств бюджета города Челябинска;
3. предоставления муниципальных услуг;
4. обеспечения размещения муниципальных заказов;
5. организации и проведения культурно-массовых мероприятий;
6. защиты законных прав и интересов жителей города;
7. подготовки документов для наград и поощрений жителей города;
8. обеспечения прав граждан на обращение в органы местного самоуправления города Челябинска;
9. реализации прав граждан на получение информации о деятельности Администрации района, а также справок, копий правовых актов, иных документов Администрации района;
10. исполнения договоров и соглашений, стороной которых является субъект персональных данных;
11. реализации трудовых отношений, ведения бухгалтерского учета и отчетности в Администрации района;
12. реализации кадровой политики в Администрации района, подготовки и ведения кадрового резерва, резерва руководящих кадров руководителей муниципальных предприятий и учреждений;
13. организации воинского учета и бронирования граждан, пребывающих в запасе;
14. иных целях, предусмотренных законодательством Российской Федерации, Челябинской области, муниципальными правовыми актами города Челябинска.

9. Обработка персональных данных должна осуществляться в соответствии с принципами обработки персональных данных, установленными статьей 5 Федерального закона № 152-ФЗ.

10. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных, в соответствии с частью 4  
статьи 21 Федерального закона № 152-ФЗ.

Порядок и условия уничтожения персональных данных утверждаются правовыми актами Администрации района в установленном порядке.

11. Оператором может осуществляться обработка персональных данных, доступ к которым имеет неограниченный круг лиц, в случаях, предусмотренных статьей 8 Федерального закона № 152-ФЗ, с согласия субъекта персональных данных, а также по его просьбе. В целях информационного обеспечения населения в Администрации района могут создаваться общедоступные источники персональных данных.

Сведения о субъекте персональных данных должны быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов.

12. Обработка специальных категорий персональных данных может производиться Администрацией района в случаях и порядке, предусмотренных статьей 10 Федерального закона № 152-ФЗ.

13. Перечень работников Администрации района, ответственных за организацию обработки персональных данных (далее – ответственный за организацию обработки персональных данных), утверждается правовым актом Администрации района.

Ответственный за организацию обработки персональных данных обязан:

1. доводить до сведения работников Администрации района положения законодательства Российской Федерации, Челябинской области, муниципальных правовых актов города Челябинска о персональных данных и требованиях к защите персональных данных;
2. осуществлять внутренний контроль за соблюдением операторами,  
   а также работниками Администрации района, в должностные обязанности которых входит обработка персональных данных, законодательства Российской Федерации о персональные данные и требований к защите персональных данных;
3. осуществлять контроль за приемом и обработкой обращений и запросов субъектов персональных данных или их законных представителей.

Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных утверждаются правовым актом Администрации района в установленном порядке.

14. Перечни персональных данных, обрабатываемых в Администрации района, перечни должностей работников, ответственных за проведение мероприятий по обеспечению безопасности обрабатываемых персональных данных, а также перечни должностей, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к ним, утверждаются правовыми актами Администрации района.

15. В Администрации района ведется учет ИСПДн, оператором которых она является.

III. Согласие субъекта персональных данных

16. Обработка персональных данных осуществляется с согласия субъекта персональных данных. Согласие на обработку персональных данных может быть дано субъектом персональных данных или его законным представителем в любой позволяющей подтвердить факт его получения форме в соответствии со статьей 9 Федерального закона № 152-ФЗ.

17. Обработка персональных данных осуществляется без получения письменного согласия в следующих случаях:

1. обработка персональных данных необходима для исполнения договора (в том числе трудового), стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;
2. обработка персональных данных осуществляется на основании Трудового кодекса Российской Федерации или иного федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также муниципальных правовых актов города Челябинска, определяющих полномочия Администрации района как работодателя;
3. обработка персональных данных осуществляется для статистических или иных научных целей, при условии обязательного обезличивания персональных данных;
4. обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно;
5. персональные данные являются общедоступными;
6. по требованию полномочных государственных органов в случаях, предусмотренных законодательством Российской Федерации.

18. Форма согласия на обработку персональных данных утверждается правовым актом Администрации района в установленном порядке и должна содержать:

1. фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
2. фамилию, имя, отчество, адрес законного представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого законного представителя (при получении согласия от законного представителя субъекта персональных данных);
3. наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;
4. цель обработки персональных данных;
5. перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;
6. наименование (фамилию, имя, отчество) и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
7. перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
8. срок, в течение которого действует согласие на обработку персональных данных, а также порядок его отзыва;
9. подпись субъекта персональных данных.

Типовые формы согласия на обработку персональных данных приведены в приложении 1 «Согласие на обработку персональных данных» и  
в приложении 2 «Согласие на обработку персональных данных, разрешенных субъектом персональных данных для распространения» к настоящему Положению. Для обработки персональных данных в связи с реализацией служебных (трудовых) отношений в Администрации района может быть разработана иная, более расширенная форма согласия.

19. Оператор с согласия субъекта персональных данных вправе поручить обработку персональных данных другому лицу на основании заключаемого муниципального контракта в порядке и случаях, определяемых законодательством Российской Федерации, Челябинской области, муниципальными правовыми актами города Челябинска.

Типовые формы согласия субъекта персональных данных на передачу его персональных данных другому лицу утверждаются правовыми актами Администрации района.

20. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных в порядке и случаях, предусмотренных законодательством Российской Федерации, Челябинской области, муниципальными правовыми актами города Челябинска. Форма отзыва согласия на обработку персональных данных утверждается правовым актом Администрации района в установленном порядке.

21. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий 30 дней с даты поступления указанного отзыва в соответствии со статьей 21 Федерального закона № 152-ФЗ.

22. В случае отказа субъекта персональных данных от дачи согласия на обработку персональных данных работником Администрации района, принимающим заявление, должны быть разъяснены юридические последствия отказа для субъекта персональных данных.

IV. Рассмотрение запросов субъектов персональных данных или их  
законных представителей

23. Сведения, касающиеся обработки персональных данных субъекта персональных данных в составе, указанном в части 7 статьи 14 Федерального закона № 152-ФЗ, предоставляются субъекту персональных данных или его законному представителю оператором при обращении либо при получении запроса субъекта персональных данных или его законного представителя.

24. Запрос должен содержать номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие нахождение субъекта персональных данных в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись субъекта персональных данных или его законного представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

25. В день поступления запроса оператору от субъекта персональных данных указанный запрос регистрируется в установленном порядке. На запросе проставляется штамп, в котором указывается входящий номер и дата регистрации документа, а также осуществляется его проверка на повторность.

После регистрации запрос субъекта персональных данных передается в установленном порядке работнику оператора (непосредственный исполнитель), имеющему доступ к запрашиваемым персональным данным в соответствии с его должностными обязанностями, для подготовки ответа.

26. Исполнитель обеспечивает рассмотрение запроса субъекта персональных данных и подготовку ответа за подписью уполномоченного лица Администрации района в течение 30 дней со дня регистрации запроса оператором. Ответ на запрос после подписания регистрируется в установленном порядке и направляется субъекту персональных данных.

27. Сведения, касающиеся обработки персональных данных субъекта персональных данных в составе, указанном в части 7 статьи 14 Федерального закона № 152-ФЗ, должны быть предоставлены субъекту персональных данных оператором в доступной форме, 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.

28. В случае отказа в предоставлении информации о наличии персональных данных о соответствующем субъекте персональных данных при получении повторного запроса оператор обязан дать в письменной форме мотивированный ответ, содержащий ссылку на статью 14 Федерального закона  
№ 152-ФЗ или иной федеральный закон, являющийся основанием для такого отказа, в срок, не превышающий 30 дней со дня обращения субъекта персональных данных либо с даты регистрации повторного запроса.

V. Меры по обеспечению безопасности персональных данных при их обработке

29. Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

30. Обеспечение безопасности персональных данных, обрабатываемых в Администрации района, достигается путем исключения несанкционированного доступа, в том числе случайного, к персональным данным (далее – НСД), а также принятия следующих мер по их защите:

1. определение актуальных угроз безопасности персональных данных, в том числе при их обработке в ИСПДн;
2. применение организационных и технических мер по обеспечению безопасности персональных данных, в том числе при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает необходимый уровень защищенности персональных данных;
3. применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям по безопасности информации;
4. учет машинных носителей персональных данных;
5. обеспечение функционирования средств обработки персональных данных, а также средств защиты информации в соответствии с эксплуатационной и технической документацией;
6. установление правил доступа к персональным данным, в том числе обрабатываемым в ИСПДн, а также обеспечение регистрации и учета действий, совершаемых с персональными данными;
7. обнаружение и регистрация фактов НСД к персональным данным, несанкционированной повторной и дополнительной записи информации после ее извлечения из ИСПДн;
8. восстановление персональных данных, модифицированных или удаленных (уничтоженных) вследствие НСД к ним;
9. контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности ИСПДн.

31. Для персональных данных должен быть определен их уровень защищенности в соответствии с законодательством Российской Федерации.

32. Перечни ИСПДн утверждаются правовыми актами Администрации района.

33. Перечень работников Администрации района, ответственных за обеспечение безопасности персональных данных при их обработке в ИСПДн (далее – ответственный за обеспечение безопасности персональных данных), утверждается правовым актом Администрации района.

34. В должностные обязанности ответственного за обеспечение безопасности персональных данных входит:

1. определение угроз безопасности персональных данных при их обработке в ИСПДн;
2. применение организационных и технических мер по обеспечению безопасности персональных данных, в том числе при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает необходимый уровень защищенности персональных данных;
3. применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям по безопасности информации;
4. оценка эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию ИСПДн;
5. учет машинных носителей персональных данных;
6. обнаружение фактов НСД к персональным данным и принятие соответствующих мер;
7. восстановление персональных данных, модифицированных или уничтоженных вследствие НСД к ним;
8. контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровнем защищенности ИСПДн.

VI. Порядок организации работы в части обеспечения безопасности персональных данных при их обработке в ИСПДн

35. Ответственность за обеспечение безопасности персональных данных при их обработке в ИСПДн возлагается на администраторов информационной безопасности в аппарате Администрации района (далее – администратор ИБ).

36. Допуск работников к персональным данным фиксируется в журнале фактического допуска работников к информации, содержащейся в информационных системах персональных данных Администрации района (приложение 3 к настоящему Положению). Обязанность по ведению данного журнала возлагается на администратора ИБ.

37. Вход работника в ИСПДн должен осуществляться по персональному паролю.

38. Все магнитные, оптические и другие машинные носители персональных данных подлежат обязательному учету. На носители информации наносится маркировка, позволяющая идентифицировать и организовать  
их учет. Машинные носители информации, в том числе с резервными копиями персональных данных, регистрируются в журнале учета машинных  
носителей персональных данных (приложение 4 к настоящему Положению). Обязанность по ведению данного журнала возлагается на администратора ИБ.

39. При работе со съемными машинными носителями информации работник каждый раз перед началом работы обязан проверить их на отсутствие вирусов с использованием штатных антивирусных программ. В случае обнаружения вирусов пользователь автоматизированного рабочего  
места (далее – АРМ) обязан немедленно прекратить их использование и действовать в соответствии с требованиями настоящего Положения.

40. Каждый работник, участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению   
(далее – ПО) и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

1. строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
2. знать и строго выполнять правила работы со средствами защиты информации (далее – СЗИ), установленными на АРМ;
3. хранить в тайне свой пароль (пароли). В соответствии с пунктом 79 настоящего Положения и с установленной периодичностью менять свой пароль (пароли);
4. выполнять требования правил антивирусной защиты в полном объеме;
5. хранить в установленном порядке свое индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);
6. немедленно известить администратора ИБ в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

* несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
* отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования периферийных устройств, а также перебоев в системе электроснабжения;
* некорректного функционирования установленных на АРМ технических средств защиты;
* непредусмотренных отводов кабелей и подключенных устройств.

41. Пользователю АРМ запрещается:

1. использовать компоненты программного и аппаратного обеспечения в неслужебных целях;
2. самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные архивом дистрибутивов установленного ПО АРМ;
3. осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
4. записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации;
5. оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);
6. оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие защищаемую информацию (сведения ограниченного распространения);
7. умышленно использовать недокументированные свойства и ошибки в ПО или в настройках СЗИ, которые могут привести к возникновению кризисной ситуации;
8. размещать средства ИСПДн так, чтобы с них существовала возможность визуального считывания информации.

VII. Порядок резервирования и восстановления работоспособности технических средств и ПО баз данных и СЗИ

42. Целью резервного копирования персональных данных является обеспечение возможности их восстановления в кратчайшие сроки в случае утраты (уничтожения).

Резервное копирование осуществляется путем регулярного создания резервных и архивных копий обрабатываемой в ИСПДн информации.

43. Для создания резервных копий могут использоваться сервер резервного копирования, компактные (сменные) носители информации (CD/DVD-диски, внешние жесткие диски и другие), иные внешние носители информации, зарегистрированные в установленном порядке.

44. Резервному копированию и хранению подлежат персональные данные, обрабатываемые в ИСПДн, а также иная информация, определяемая как критичная для обеспечения бесперебойной работы ИСПДн.

45. Резервное копирование данных, обрабатываемых в ИСПДн, осуществляется уполномоченным работником, в должностные обязанности которого входят функции по обеспечению работоспособности данной ИСПДн или функции по резервному копированию информации.

46. Сеансы резервного копирования настраиваются на внерабочее время с учетом возможности ИСПДн поддерживать работу с копируемыми данными, а также длительности выполнения процедуры резервного копирования.  
Полная резервная копия, являющаяся основным источником восстановления персональных данных, производится на внешнее хранилище информации,  
по возможности отдаленное от ресурсов, на которых хранятся и обрабатываются резервируемые персональные данные. Частичная резервная копия  
производится при необходимости и предназначена для восстановления  
части ИСПДн.

47. Полная резервная копия содержит:

1. информацию, необходимую для восстановления работоспособности ИСПДн;
2. информацию, содержащуюся в ИСПДн;
3. рабочие копии установочных компонентов (дистрибутивов) ПО рабочих станций;
4. файлы конфигурации ИСПДн;
5. прочую необходимую информацию.

48. Восстановление информации из резервных копий может осуществляться в случаях:

1. потери данных;
2. необходимости исправления ошибочных операций с данными;
3. тестового восстановления.

VIII. Контроль защиты информации в ИСПДн

49. Контроль защиты информации в ИСПДн – комплекс организационных и технических мероприятий, проводимых в целях предупреждения и пресечения возможности получения техническими средствами охраняемых сведений, выявления и предотвращения утечки информации по техническим каналам, исключения или существенного затруднения НСД к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение целостности информации или работоспособности систем информатизации.

50. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн и в защищаемом помещении, в котором расположены АРМ, входящие в ИСПДн, (далее – объект информатизации). Контроль защиты информации осуществляется по объектовому принципу, при котором на объекте информатизации одновременно проверяются все варианты защиты информации.

51. Основными задачами контроля защиты информации на объекте информатизации являются:

1. проверка организации выполнения мероприятий по защите информации с учетом требований по защите информации в разрабатываемых плановых и распорядительных документах;
2. уточнение зон перехвата информации, обрабатываемой на объектах информатизации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
3. проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
4. проверка выполнения требований по защите ИСПДн от НСД к информации;
5. проверка выполнения требований по антивирусной защите автоматизированных систем и АРМ;
6. проверка знаний работников по вопросам защиты информации и соответствия их уровня подготовки требованиям защиты информации для конкретного АРМ;
7. оперативное принятие мер по пресечению нарушений требований защиты информации в ИСПДн.

52. В ходе контроля защиты информации проверяются:

1. соответствие принятых мер по обеспечению безопасности персональных данных уровню защищенности ИСПДн;
2. своевременность и полнота выполнения требований правовых актов Администрации района и настоящего Положения в области защиты персональных данных;
3. возможные технические каналы утечки информации, НСД к ней и программно-технических воздействий на информацию;
4. эффективность применения организационных и технических мероприятий по защите информации;
5. устранение ранее выявленных недостатков.

Кроме того, могут проводиться необходимые измерения и расчеты приглашенными для этих целей специалистами организации-лицензиата Федеральной службы по техническому и экспортному контролю  
(далее – организация-лицензиат).

53. Основными видами технического контроля на объекте информатизации являются контроль эффективности защиты информации от утечки по техническим каналам, контроль НСД к информации и программно-технических воздействий на информацию.

54. Полученные в ходе контроля защиты информации результаты обрабатываются и анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений требований по защите информации администратор ИБ докладывает ответственному за обеспечение безопасности персональных данных о том, где допущены нарушения, для принятия им решения о прекращении обработки информации и проведения соответствующих организационных и технических мероприятий по устранению нарушения. Результаты контроля защиты информации оформляются актами либо заносятся в соответствующие журналы учета результатов контроля.

55. Невыполнение предписанных мероприятий по защите персональных данных считается предпосылкой к утечке информации. По каждой такой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований проводится расследование.

Для проведения расследования назначается комиссия с привлечением администратора ИБ. Комиссия обязана установить, имела ли место утечка сведений, обстоятельства ей сопутствующие, лиц, виновных в нарушении предписанных мероприятий по защите информации, причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению.

56. Ведение контроля защиты информации осуществляется путем проведения плановых и внеплановых проверок ИСПДн. Плановые и внеплановые проверки ИСПДн проводятся, как правило, силами администратора ИБ в соответствии с утвержденным планом.

57. Одной из форм контроля защиты информации является обследование ИСПДн. Оно проводится не реже 1 раза в год рабочей группой по обследованию ИСПДн, возглавляемой ответственным за организацию обработки персональных данных.

58. Обследование объекта информатизации проводится с целью определения соответствия объекта информатизации, основных и вспомогательных технических средств и систем объекта информатизации требованиям по защите информации, установленным в аттестате объекта информатизации на соответствие требованиям безопасности информации  
(далее – аттестат соответствия) при наличии.

59. В ходе обследования объекта информатизации проверяется:

1. соответствие уровня защищенности обследуемого объекта информатизации условиям, сложившимся на момент проверки;
2. соблюдение организационно-режимных требований объекта информатизации;
3. сохранность печатей, пломб на технических средствах передачи и обработки информации, а также на устройствах их защиты, отсутствие повреждений экранов корпусов аппаратуры, оболочек кабелей и их соединений с шинами заземления;
4. наличие электробытовой, радио- и телевизионной аппаратуры и устройств непромышленного изготовления, которые могут способствовать возникновению каналов утечки информации;
5. выполнение требований предписаний на эксплуатацию основных технических средств, систем по их размещению относительно вспомогательных технических средств, систем организации электропитания и заземления;
6. соответствие выполняемых на объекте информатизации мероприятий по защите информации данным, изложенным в техническом паспорте данного объекта информатизации;
7. выполнение требований по защите автоматизированных систем от НСД;
8. выполнение требований по антивирусной защите.

60. Периодический контроль состояния защиты персональных данных осуществляется Администрацией города Челябинска не реже 1 раза в 3 года в соответствии с планом проведения проверок. При необходимости Администрация города Челябинска может привлекать на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

IX. Обязанности работников, допущенных к обработке персональных данных

61. Работники, допущенные к обработке персональных данных, обязаны:

1. знать и выполнять требования настоящего Положения;
2. осуществлять обработку персональных данных в целях, определенных законодательством Российской Федерации, Челябинской области, муниципальными правовыми актами города Челябинска;
3. знакомиться только с теми персональными данными, к которым им разрешен доступ;
4. не разглашать известные им персональные данные, информировать своего непосредственного начальника о фактах нарушения порядка обработки персональных данных и о попытках НСД к ним;
5. предупреждать лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены;
6. выполнять требования по защите полученных персональных данных;
7. соблюдать правила пользования документами, содержащими персональные данные, порядок их обработки и защиты;
8. предоставлять письменные объяснения о допущенных нарушениях установленного порядка обработки персональных данных, а также о фактах их разглашения или утраты.

62. Первичные инструктажи и ознакомление с законодательством в области защиты персональных данных проводятся администратором ИБ при поступлении на работу работника в соответствующее структурное подразделение, где происходит обработка конфиденциальной информации в ИСПДн.

X. Правила регистрации событий безопасности и учета действий с персональными данными в ИСПДн

63. Под событием безопасности в ИСПДн понимается любое  
событие, которое может повлиять на безопасность ИСПДн (далее – событие безопасности).

64. Целью регистрации событий безопасности является обнаружение несанкционированных действий, связанных с обработкой персональных данных. Мониторинг автоматизированных систем следует проводить с целью проверки эффективности применяемых мер и средств контроля и управления.

65. Перечень событий безопасности, подлежащих регистрации в ИСПДн (при наличии технической возможности):

1. вход (выход), а также попытки входа пользователя АРМ в ИСПДн;
2. попытка удаленного доступа в ИСПДн;
3. запуск (остановка) ИСПДн;
4. подключение машинных носителей информации к средствам обработки информации;
5. вывод информации на носители информации (в том числе на печать);
6. запуск (завершение) программ и процессов (заданий, задач), связанных с обработкой персональных данных;
7. заведение пользователя АРМ ИСПДн;
8. блокирование пользователя АРМ ИСПДн;
9. аннулирование (постоянное блокирование) пользователя АРМ ИСПДн;
10. удаление пользователя АРМ ИСПДн;
11. редактирование пользователя АРМ ИСПДн (без изменения полномочий);
12. изменение полномочий пользователя АРМ ИСПДн;
13. ошибка ввода пароля пользователя АРМ ИСПДн;
14. изменение пароля пользователя АРМ ИСПДн;
15. сброс пароля пользователя АРМ ИСПДн;
16. изменение прав доступа к защищаемым объектам ИСПДн;
17. удаление (очистка) журнала событий безопасности ИСПДн;
18. невозможность (ошибка) записи в журнал событий безопасности ИСПДн;
19. нарушение (попытка нарушения) политик доступа;
20. предупреждение или отказ ИСПДн и их компонентов;
21. изменение (попытка) параметров настройки системы безопасности, а также мер и средств контроля и управления.

66. В ИСПДн, где установлены СЗИ, проверка журнала событий безопасности производится в соответствии с прилагаемым к указанным СЗИ руководством. Журнал событий безопасности ведется в электронном виде.

В ИСПДн, где защита от НСД реализована организационными мероприятиями, проверка журнала событий безопасности проводится внутренними средствами операционной системы.

67. В большинстве случаев записи журналов безопасности хранятся не менее 3 месяцев, причем в оперативном доступе (онлайн) – не менее 2 недель. Для различных событий безопасности ИСПДн сроки хранения соответствующих записей могут отличаться.

68. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить следующие возможности по идентификации:

1. даты и времени события безопасности;
2. типа и описания события безопасности;
3. субъекта доступа (пользователь и (или) процесс), связанного с данным событием безопасности;
4. объекта доступа (защищаемый ресурс, внешнее устройство и другие);
5. способа, средства доступа, используемых технологий доступа;
6. результата события безопасности (успешно или неуспешно).

69. Если в ходе плановых или внеплановых проверок ИСПДн выявлены случаи НСД к информации конфиденциального характера, то Администратор ИБ действует в соответствии с пунктом 54 настоящего Положения.

XI. Правила антивирусной защиты

70. К использованию на АРМ допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств, сертифицированные Федеральной службой по техническому и экспортному контролю.

71. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, CD-ROM, другие). Антивирусный контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

72. На АРМ запрещается установка ПО, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

73. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление  
сообщений о системных ошибках) работник самостоятельно (или вместе  
с администратором ИБ) должен провести внеочередной антивирусный контроль своего АРМ.

74. В случае обнаружения при проведении антивирусной проверки зараженных вирусами файлов работник обязан:

1. приостановить обработку данных в ИСПДн;
2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора ИБ, владельца зараженных файлов, если файлы принадлежат другому работнику (по возможности), а также работников структурных подразделений, использующих эти файлы в работе;
3. совместно с администратором ИБ и владельцем файлов, если файлы принадлежат другому работнику, провести анализ зараженных вирусом файлов и выявить возможность их дальнейшего использования;
4. провести лечение или уничтожение зараженных файлов.

75. Ответственность за организацию антивирусного контроля в ИСПДн в соответствии с требованиями настоящего Положения возлагается на администратора ИБ.

76. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на администратора ИБ и всех работников, использующих данную ИСПДн.

XII. Правила парольной защиты

77. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями работников при работе с паролями возлагается на администратора ИБ.

78. Личные пароли должны выбираться работниками самостоятельно с учетом следующих требований:

1. пароль должен включать не менее 6 символов;
2. в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и (или) специальные символы (@, #, $, &, \*, %, другие);
3. символы паролей для рабочих станций, на которых установлено СЗИ от НСД, должны вводиться в режиме латинской раскладки клавиатуры;
4. пароль не должен содержать в себе легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ), а также общепринятые сокращения (ЭВМ, ЛВС, USER, подобные);
5. при смене пароля новое значение должно отличаться от предыдущего;
6. пользователь не имеет права сообщать личный пароль другим лицам.

Владельцы паролей должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

79. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже 1 раза в течение 180 дней.

80. Удаление учетной записи пользователя в случае прекращения его полномочий (увольнение, переход на другую работу внутри Администрации района и другие обстоятельства) должна производиться администратором ИБ немедленно после окончания последнего сеанса работы данного пользователя с системой.

81. В случае компрометации личного пароля работника в ИСПДн должен быть немедленно поставлен в известность администратор ИБ для принятия мер по восстановлению парольной защиты.

82. Контроль за действиями пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на   
администратора ИБ.

XIII. Правила обновления общесистемного и прикладного ПО,

технического обслуживания ИСПДн

83. Право внесения изменений в конфигурацию аппаратных и программных средств, защищенных АРМ предоставляется исключительно:

* администратору ИБ – в отношении системных и прикладных программных средств;
* Комиссии – в отношении аппаратных средств, программно-аппаратных СЗИ.

Изменение конфигурации аппаратных и программных средств АРМ  
другими кроме указанных в настоящем пункте лицами запрещено.

84. Все изменения конфигураций технических и программных средств АРМ ИСПДн должны производиться только на основании заявки работника, назначенного ответственным за эксплуатацию конкретного АРМ  
(далее – ответственный за эксплуатацию АРМ).

85. В заявке могут указываться следующие виды необходимых изменений в составе аппаратных и программных средств АРМ ИСПДн:

1. установка (развертывание) на АРМ программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи) в ИСПДн;
2. обновление (замена) на АРМ программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи, программ);
3. удаление с АРМ программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на АРМ).

86. Заявку ответственного за эксплуатацию АРМ, в которой требуется произвести изменения конфигурации аппаратных и программных средств АРМ, рассматривает администратор ИБ и подтверждает или не подтверждает производственную необходимость проведения указанных в заявке изменений для непосредственного исполнения работ по внесению изменений в конфигурацию АРМ, указанного в заявке.

87. Подготовка обновления, модификации общесистемного  
и прикладного ПО ИСПДн, тестирование, стендовые испытания (при необходимости) и передача исходных текстов, документации и дистрибутивных носителей программ в архив дистрибутивов установленного ПО,  
внесение необходимых изменений в настройки средств защиты от НСД  
и средств контроля целостности файлов на АРМ (обновление) и удаление системных и прикладных программных средств производятся уполномоченными работниками. Работы производятся в присутствии ответственного за эксплуатацию АРМ.

88. Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

89. Установка и обновление ПО на АРМ производится только с оригинальных лицензионных дистрибутивных носителей информации, полученных в установленном порядке, прикладного ПО – с эталонных  
копий программных средств, полученных из архива дистрибутивов установленного ПО.

90. Все добавляемые программные и аппаратные компоненты должны быть предварительно в установленном порядке проверены на работоспособность и отсутствие не предусмотренных разработчиком программных и аппаратных компонентов функций.

91. После установки (обновления) ПО администратор ИБ должен настроить средства управления доступом к компонентам АРМ, проверить работоспособность ПО, правильность их настройки и произвести соответствующую запись в журнале учета нештатных ситуаций, выполнения профилактических работ, установки и модификации программных средств автоматизированных рабочих мест (приложение 5 к настоящему Положению), сделать отметку о выполнении на обратной стороне заявки. Также необходимо сделать отметку в техническом паспорте объекта информатизации   
(при наличии).

Оригиналы заявок, на основании которых вносились изменения в состав программных средств АРМ, с отметками о внесении изменений, должны храниться вместе с техническим паспортом объекта информатизации и журналом учета нештатных ситуаций АРМ, выполнения профилактических работ, установки и модификации программных средств АРМ у администратора ИБ.

92. При возникновении ситуаций, требующих передачи АРМ в ремонт, ответственный за эксплуатацию АРМ ставит в известность об этом администратора ИБ и предпринимает необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.  
При наличии аттестата соответствия администратор ИБ связывается со специалистами организации-лицензиата для согласования ремонта.

93. Факт уничтожения данных, находившихся на дисках компьютера, оформляется актом за подписью администратора ИБ и ответственного за эксплуатацию данной АРМ.

XIV. Контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ

94. Порядок работы с техническими СЗИ определен в соответствующих инструкциях, руководстве по настройке и использованию СЗИ, обязательных для исполнения как работниками, обрабатывающими конфиденциальную информацию, так и администратором ИБ.

95. Право проверки соблюдения условий использования СЗИ имеет администратор ИБ.

96. Работникам запрещается обработка конфиденциальной информации в ИСПДн с отключенными СЗИ.

97. При наличии аттестата соответствия администратору ИБ запрещается менять настройки программно-аппаратных СЗИ, предустановленные специалистами организации-лицензиата в ходе настройки системы обеспечения безопасности персональных данных при аттестации ИСПДн.

98. Если в ходе проведения плановых или внеплановых проверок ИСПДн выявлено нарушение требований пункта 91 настоящего Положения, то вступают в силу пункты 52, 53 настоящего Положения.

99. При осуществлении контроля работоспособности, параметров настройки и правильности функционирования ПО и СЗИ производится:

1. контроль работоспособности (неотключения) ПО и СЗИ;
2. проверка правильности функционирования (тестирование на  
   тестовых данных, приводящих к известному результату) ПО и СЗИ, объем и содержание которой определяется администратором ИБ;
3. контроль соответствия настроек ПО и СЗИ параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации;
4. восстановление работоспособности (правильности функционирования) и параметров настройки ПО и СЗИ (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов.

XV. Требования по учёту машинных носителей персональных данных

100. Во всех ИСПДн должен быть обеспечен учет машинных  
носителей информации, используемых для хранения и обработки персональных данных.

Обязательному учету подлежат:

1. съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
2. машинные носители информации, встроенные в средства вычислительной техники (накопители на жестких дисках, твердотельные накопители);
3. портативные вычислительные устройства со встроенными носителями информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства).

101. Учет машинных носителей включает присвоение им регистрационных номеров. Для идентификации машинных носителей персональных данных  
могут использоваться серийные номера, присвоенные производителями, номера инвентарного учета, в том числе инвентарные номера технических  
средств, имеющих встроенные носители информации, и иные номера. Регистрационный номер наносится на несъемную часть корпуса носителя информации.

102. Учет всех типов машинных носителей персональных данных, использующихся в ИСПДн, или, при невозможности, целиком портативных вычислительных устройств, ведется в журнале учета машинных носителей персональных данных (приложение 4 к настоящему Положению).

103. При регистрации носителей персональных данных (до первой записи на них персональных данных) должна указываться следующая информация:

1. ограничительная пометка доступа («Персональные данные (ПДн)» или «Для служебного пользования (ДСП)»);
2. ответственный за использование или владелец носителя информации;
3. идентификатор носителя информации.

104. Контроль за соблюдением правил хранения носителей персональных данных и ведение журнала учета машинных носителей персональных данных возлагается на администратора ИБ.

105. Регулярный контроль за наличием учтенных машинных носителей информации осуществляется Комиссией.

106. Все персональные данные и их носители уничтожаются в порядке, предусмотренном для уничтожения документов с пометкой ДСП, по достижении цели, для которой они собирались и использовались, если иное не установлено законодательством Российской Федерации.

XVI. Порядок обработки персональных данных, осуществляемой  
без использования средств автоматизации

107. Порядок обработки персональных данных, осуществляемой без использования средств автоматизации, утверждается правовым актом Администрации района.

Исполняющий обязанности

главы Администрации

Тракторозаводского района города Челябинска Т. А. Букреева

Приложение 1

к Положению о порядке обработки   
и обеспечения безопасности персональных данных в Администрации Тракторозаводского района города Челябинска

Форма

Согласие

на обработку персональных данных

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(фамилия, имя, отчество (при наличии)

зарегистрированный(ая) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

паспорт серия \_\_\_\_\_\_ номер \_\_\_\_\_\_\_\_\_\_\_\_, выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(дата, кем выдан)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

в соответствии со статьей 9 Федерального закона от 27.07.2006 № 152-ФЗ   
«О персональных данных» даю свое согласие оператору \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (далее – Оператор), расположенному по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

на обработку моих нижеуказанных персональных данных в целях \_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Действие согласия распространяется на следующую информацию, относящуюся к моим персональным данным: фамилия, имя, отчество, дата и место рождения, пол, гражданство, паспортные данные или данные иного документа, удостоверяющего личность (серия, номер, когда и кем выдан), сведения, характеризующие мои физиологические особенности (изображение лица), адрес места жительства, контактная информация, сведения об образовании, квалификации и о наличии специальных знаний и специальной подготовки, сведения о трудовой деятельности, заработной плате и иных доходах и расходах, сведения о воинском учете, семейном положении, сведения страховых полисов обязательного и (или) добровольного медицинского страхования, идентификационный номер налогоплательщика, иные сведения.

Настоящее согласие предоставляется на совершение любых необходимых действий (операций) с моими персональными данными, включая сбор (в том числе у определенного круга третьих лиц, без уведомления меня об этом), систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение, осуществляемых как с использованием средств автоматизации (автоматизированная обработка), так и без использования таких средств (неавтоматизированная обработка).

Настоящее согласие действует в течение всего периода хранения моих персональных данных у Оператора, если иное не предусмотрено законодательством Российской Федерации.

Я уведомлен(a), что вправе отозвать согласие на обработку своих персональных данных путем направления мною соответствующего письменного запроса в адрес Оператора, но не менее чем за 1 (один) месяц до момента прекращения обработки Оператором моих персональных данных.

В случае изменения моих персональных данных я обязуюсь уведомить Оператора о таких изменениях не позднее 14 (четырнадцати) календарных дней с момента изменения.

В случае если сведения об изменении моих персональных данных были получены от третьих лиц, то Оператор вправе не уведомлять меня об этом.

Оператор вправе получить мои персональные данные у третьей стороны, если получение персональных данных от меня невозможно. При этом Оператор обязуется сообщить мне о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
| (дата) |  | (подпись) |  | (фамилия и инициалы) |

Приложение 2

к Положению о порядке обработки   
и обеспечения безопасности персональных данных в Администрации Тракторозаводского района города Челябинска

Форма

Согласие

на обработку персональных данных,

разрешенных субъектом персональных данных для распространения

г. Челябинск «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ г.

Я, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(фамилия, имя, отчество (при наличии)

зарегистрированный(ая) по адресу \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

паспорт серия \_\_\_\_\_\_\_\_\_ номер \_\_\_\_\_\_\_\_\_\_\_\_, выдан \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

(дата, кем выдан)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,

в соответствии со статьей 10.1 Федерального закона от 27.07.2006 № 152-ФЗ   
«О персональных данных» даю свое согласие оператору \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
(далее – Оператор), расположенному по адресу:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_,  
на распространение подлежащих обработке персональных данных в целях \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Действие настоящего согласия распространяется на следующую информацию, относящуюся к моим персональным данным:

|  |  |  |  |
| --- | --- | --- | --- |
| Категория персональных данных | Перечень  персональных данных | Разрешение к распространению (да/нет) | Условия и запреты |
| 1 | 2 | 3 | 4 |
| Общие | фамилия |  |  |
|  | имя |  |  |
|  | отчество |  |  |
|  | должность |  |  |
|  | год рождения |  |  |
|  | месяц рождения |  |  |
|  | дата рождения |  |  |
|  | место рождения |  |  |
|  | семейное положение |  |  |
|  | образование |  |  |
| 1 | 2 | 3 | 4 |
|  | наличие ученой степени, ученого звания |  |  |
|  | классный чин |  |  |
|  | выполняемая работа с указанием периодов |  |  |
|  | государственные награды, иные награды и знаки отличия |  |  |
|  | кем и когда выданы награды и знаки отличия |  |  |
|  | контактный рабочий телефон |  |  |
|  | интересы |  |  |
| Биометрические | цветное цифровое фотографическое изображение лица |  |  |
| Иные сведения, которые субъект желает сообщить о себе |  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Предоставление доступа неограниченному кругу лиц должно осуществляться путем размещения моих персональных данных на официальном сайте Оператора в сети Интернет, находящемся по адресу: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Настоящее согласие дано на период трудовых отношений с Оператором.

Я ознакомлен(а), что:

1) настоящее согласие действует с даты его подписания в течение всего срока службы, работы в \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_;

2) настоящее согласие может быть отозвано на основании требования согласно

части 12 статьи 10.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

3) в случае отзыва настоящего согласия Оператор вправе продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2–11  
части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006  
№ 152-ФЗ «О персональных данных»;

4) после увольнения со службы, прекращения трудовых отношений персональные данные работника, разрешенные для распространения, удаляются с официального сайта Оператора в течение срока, предусмотренного законодательством Российской Федерации.

Дата начала обработки персональных данных \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

(число, месяц, год)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(подпись) (фамилия и инициалы)

Приложение 3

к Положению о порядке обработки и обеспечения безопасности персональных данных в Администрации Тракторозаводского района города Челябинска

Форма

Журнал[[1]](#footnote-1)

фактического допуска работников к информации, содержащейся в информационных системах персональных данных Администрации Тракторозаводского района города Челябинска

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Фамилия, имя, отчество работника | Должность, структурное подразделение | Наименование информационной системы персональных данных | Перечень прав доступа | Дата предоставления прав | Дата аннулирования прав |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Приложение 4

к Положению о порядке обработки и обеспечения безопасности персональных данных в Администрации Тракторозаводского района города Челябинска

Форма

Журнал

учета машинных носителей персональных данных

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| № п/п | Регистрационный номер, дата | Тип, емкость машинного носителя персональных данных | Номер экземпляра/ количество экземпляров | Место установки (использования)/ дата установки | Ответственное должностное лицо (фамилия, имя, отчество), использующее машинный носитель персональных данных | Расписка в получении машинного носителя персональных данных (подпись получателя, дата) | Расписка в возврате машинного носителя персональных данных (фамилия, имя, отчество, подпись получателя, дата) | Место хранения машинного носителя персональных данных | Сведения об уничтожении машинного носителя персональных данных, стирании информации (подпись, дата) |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

Приложение 5

к Положению о порядке обработки и обеспечения безопасности персональных данных в Администрации Тракторозаводского района города Челябинска

Форма

Журнал

учета нештатных ситуаций, выполнения профилактических работ, установки и модификации программных средств автоматизированных рабочих мест

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Дата | Краткое описание выполненной работы (нештатной ситуации) | Фамилия, имя, отчество исполнителя, подпись | Фамилия, имя, отчество, ответственного за эксплуатацию автоматизированного рабочего места, подпись | Подпись администратора информационной безопасности | Примечание (ссылка на заявку) |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. Журнал ведется в электронном виде. [↑](#footnote-ref-1)