АВТОНОМНОЕ УЧРЕЖДЕНИЕ СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ НАСЕЛЕНИЯ ТЮМЕНСКОЙ ОБЛАСТИ
«СОЦИАЛЬНО-ОЗДОРОВИТЕЛЬНЫЙ ЦЕНТР ГРАЖДАН ПОЖИЛОГО ВОЗРАСТА И ИНВАЛИДОВ «КРАСНАЯ ГВОЗДИКА»

ПРИКАЗ

19 декабря 2018 г. № 64

г. Тюмень

Об утверждении ответственных в области обеспечения безопасности персональных данных в АУ СОН ТО «Центр «Красная гвоздика»

В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», Постановлением Правительства РФ 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 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», Указом Президента РФ от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера», Регламентирующими документами ФСТЭК России и ФСБ России об обеспечении безопасности персональных данных,

ПРИКАЗЫВАЮ:

1. Ответственным за организацию обработки персональных данных в АУ СОН ТО «Центр «Красная гвоздика» (далее – Учреждение) назначить работника, замещающего должность специалиста по кадрам, а на время отсутствия этого работника, ответственным за организацию обработки персональных данных в Учреждении назначается начальник отдела правовой, административно – кадровой и закупочной деятельности, юрисконсульт.
2. Ответственным за организацию и обеспечение защиты информации в Учреждении назначить сотрудника, замещающего должность программиста, а на время отсутствия этого работника, ответственным за организацию и обеспечение защиты информации в Учреждении назначить специалиста по охране труда.
3. Утвердить инструкцию ответственного за организацию обработки персональных данных согласно приложению № 1 к настоящему приказу
4. Утвердить инструкцию администратора информационной безопасности согласно приложению № 2 к настоящему приказу.
5. Бологовой О.В., секретарю руководителя, довести настоящий приказ до сведения исполнителей.
6. Контроль исполнения настоящего приказа оставляю за собой.

Директор М.В. Бабушкина

Приложение 1 к приказу
28.12.2018 № 64

УТВЕРЖДЕНО
Директор АУ СОН ТО
«Центр «Красная гвоздика»
_____ М.В. Бабушкина

ИНСТРУКЦИЯ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В АУ СОН ТО «ЦЕНТР «КРАСНАЯ ГВОЗДИКА»

1. Общие положения

1.1. Настоящий документ определяет основные обязанности, права и ответственность сотрудника, назначенного ответственным за организацию обработки персональных данных (далее - ПДн) в АУ СОН ТО «Центр «Красная гвоздика» (далее – Учреждение).

1.2. Инструкция регулирует отношения и порядок взаимодействия между ответственным за организацию работ по обработке персональных данных в Учреждении и структурными подразделениями Учреждения, которые обрабатывают персональные данные, в связи с реализацией трудовых функций, в соответствии с действующим законодательством Российской Федерации, за исключением случаев, перечисленных в части 2 статьи 1 Федерального закона от 27.07.2006 г. N 152-ФЗ «О персональных данных».

1.3. Ответственный за организацию работ по обработке персональных данных в Учреждении в своей деятельности руководствуется локальными нормативными актами Учреждения, Федеральными законами, Конституцией РФ и другими подзаконными актами, регулирующими вопросы обеспечения безопасности ПДн.

2. Права и обязанности

2.1. Ответственный за организацию работ по обработке персональных данных в Учреждении обязан:

2.1.1. Организовывать работу в учреждении по разработке и принятию правовых актов, правил обработки персональных данных, наличие которых предусмотрено действующим законодательством.

2.1.2. Организовывать ознакомление сотрудников учреждения, непосредственно осуществляющих обработку персональных данных, с действующим законодательством Российской Федерации о персональных данных и локальными правовыми актами, определяющими правила обработки персональных данных в учреждение и требования по защите персональных данных.

2.1.3. Руководить осуществлением принятия необходимых правовых, организационных и технических мер для защиты персональных данных в учреждение в соответствии с действующим законодательством Российской Федерации о персональных данных.

2.1.4. Осуществлять согласование мероприятий при создании в учреждение новых информационных систем персональных данных.

2.1.5.Координировать работу в структурных подразделениях учреждения по формированию и ведению перечней:

- должностей сотрудников Учреждения, замещение которых предусматривает осуществление обработки персональных данных;
- персональных данных, обрабатываемых в Учреждении;

2.1.6.Организовывать своевременное направление в территориальный орган Роскомнадзора уведомления об обработке персональных данных в

Учреждении, информации о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных и прочей информации, направление которой предусмотрено законодательством.

2.1.7.Организовывать и руководить проведением внутренних проверок организации состояния работ по вопросам информационной безопасности в Учреждении для осуществления периодического контроля:

- условий обработки персональных данных в Учреждении и их соответствие требованиям действующего законодательства Российской Федерации о персональных данных и принятыми в соответствии с ним приказами учреждения;

- организации приема и обработки в Учреждении обращений и запросов субъектов персональных данных или их представителей;

- выполнения установленных в соответствии с действующим законодательством Российской Федерации и локальными актами Учреждения требований к защите персональных данных, обрабатываемых в учреждение;

2.1.8.Представлять доклады директору Учреждения о результатах проведенных внутренних проверок организации состояния работ по вопросам информационной безопасности в учреждение и мерах, необходимых для устранения выявленных нарушений.

2.1.9.Координировать работу в структурных подразделениях Учреждения на принятие мер, направленных на совершенствование защиты персональных данных, обрабатываемых в Учреждении.

2.1.10.Осуществлять методическое руководство при разработке условий обработки персональных данных и эффективности мер по защите персональных данных в Учреждении.

2.1.11.Организовывать работу по планированию прохождения обучения сотрудников Учреждения по вопросам обеспечения защиты персональных данных, обрабатываемых в Учреждении.

2.2. Ответственный за организацию работ по обработке персональных данных в учреждение имеет право:

2.2.1.Запрашивать в структурных подразделениях Учреждения, в которых ведется обработка персональных данных или планируется ведение обработки персональных данных, любые сведения, необходимые для организации условий обработки персональных данных и принятия необходимых правовых, организационных и технических мер для защиты персональных данных в учреждение.

2.2.2.Принимать участие в рассмотрении жалоб и обращений граждан или юридических лиц по вопросам, связанным с обработкой персональных данных в Учреждении, а также вырабатывать предложения для принятия в пределах своих полномочий решений по результатам рассмотрения указанных жалоб и обращений.

2.2.3.Участвовать в расследовании нарушений в области защиты персональных данных в Учреждении и разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений.

2.2.4.Требовать от структурных подразделениях Учреждения уточнения, блокирования или уничтожения недостоверных или полученных незаконным путем персональных данных, при обращении (запросе) субъекта персональных данных или его представителя либо уполномоченного органа по защите прав субъектов персональных данных либо по результатам проведенной внутренней проверки организации состояния работ по вопросам информационной безопасности в учреждение.

2.2.5.Принимать меры по приостановлению или прекращению обработки персональных данных в Учреждении, осуществляемой с нарушением требований действующего законодательства Российской Федерации о персональных данных.

2.2.6.Вносить предложения о совершенствовании нормативного правового регулирования обработки и защиты персональных данных в Учреждении.

3. Ответственность

3.1. Ответственный за организацию обработки персональных данных в Учреждении несет ответственность за ненадлежащее выполнение возложенных на него обязанностей, прописанных в настоящей инструкции, в соответствии с действующим законодательством Российской Федерации и локальными актами Учреждения.

Приложение 2 к приказу
12.11.2018 № 64

УТВЕРЖДЕНО
Директор АУ СОН ТО «Центр «Красная гвоздика»
_____ /М.В. Бабушкина/

ИНСТРУКЦИЯ АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АУ СОН ТО «ЦЕНТР «КРАСНАЯ ГВОЗДИКА»

1. Общие положения

1.1. В настоящей инструкции под администратором информационной безопасности понимается ответственный за организацию и обеспечение защиты информации в АУ СОН ТО «Центр «Красная гвоздика» (далее – Учреждение).

1.2. Настоящий документ определяет основные обязанности, права и ответственность администратора информационной безопасности (далее - ИБ) Учреждения.

1.3. Администратор информационной безопасности руководствуется локальными нормативными актами Учреждения, Федеральными законами, Конституцией РФ и другими подзаконными актами, регулирующими вопросы обеспечения безопасности персональных данных (далее – ПДн).

2. Права и обязанности

2.1. Администратор ИБ обязан:

2.1.1. Решать вопросы обеспечения информационной безопасности Учреждения;

2.1.2. Знать перечень установленных в подразделениях Учреждения объектов вычислительной техники (далее - ОВТ) и перечень задач, решаемых с их использованием;

2.1.3. Осуществлять учет и периодический контроль за составом и полномочиями пользователей различных ОВТ и информационных систем;

2.1.4. Осуществлять периодический контроль внесения изменений в конфигурацию (модификации) аппаратно-программных средств защищенных ОВТ и серверов, устанавливать и осуществлять контроль за настройкой средств защиты ОВТ;

2.1.5. Периодически проверять состояние используемых систем защиты информации (далее - СЗИ) от несанкционированного доступа (далее – НСД), осуществлять проверку правильности их настройки (выборочное тестирование);

2.1.6. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИС и осуществления НСД к информации и ОВТ;

2.1.7. Докладывать организацию обработки персональных данных в Учреждении об имевших место попытках несанкционированного доступа к информации и ОВТ;

2.1.8. При необходимости проводить занятия с пользователями различных ОВТ по правилам работы на ОВТ, оснащенных СЗИ от НСД;

2.1.9. При необходимости разрабатывать инструкции и памятки для пользователей, обрабатывающих персональные данные;

2.1.10. При необходимости разрабатывать регламенты проведения работ по обеспечению безопасности персональных данных;

2.1.11. Проводить работы по установке и настройке межсетевых экранов;

2.1.12. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД;

2.1.13. Проводить периодическое тестирование функций систем защиты ПДн (далее – СЗПДн) при изменении программной среды и персонала информационных систем персональных данных (далее – ИСПДн), с помощью тест-программ, имитирующих попытки НСД;

2.1.14. При наличии технической возможности обеспечить автоматическое резервное копирование всех данных содержащих ПДн, программных модулей ИСПДн и средств защиты.

2.1.15. Соблюдать требования режима конфиденциальности информации, содержащей персональные данные работников, обучающихся, а также третьих лиц, ставшей ему известной в связи с исполнением своих должностных обязанностей, и не использовать ее в интересах, не связанных с исполнением указанных обязанностей.

2.2. Администратор ИБ имеет право:

2.2.1. Требовать от пользователей различных ОВТ выполнения инструкций по обеспечению безопасности и защите информации;

2.2.2. Доступа к любым программным и аппаратным ресурсам и любой информации на рабочих станциях пользователей (за исключением информации, закрытой с использованием средств криптозащиты) и средствам их защиты;

2.2.3. Участвовать в проведении служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС;

2.2.4. Непосредственно обращаться к руководителям подразделений с требованием прекращения работы в ИС при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности;

2.2.5. Вносить свои предложения по совершенствованию мер защиты информации в Учреждении.

3. Ответственность

3.1. На администратора ИБ возлагается персональная ответственность за работу программно - технических и криптографических средств защиты информации и за качество проводимых работ по обеспечению защиты информации на ОВТ в соответствии с функциональными обязанностями;

3.2. Администратор ИБ несет ответственность по действующему законодательству за разглашение сведений, составляющих (государственную, банковскую, коммерческую, медицинскую) тайну, и сведений ограниченного распространения, ставших известными ему по роду работы;

3.3. Администратор ИБ несет ответственность за реализацию принятой в Учреждение политики безопасности.