Муниципальное казенное учреждение социального обслуживания
«Социально-реабилитационный центр для несовершеннолетних»
Ленинского района города Челябинска

ПРИКАЗ

от «24» августа 2020 г. № 114-ОД

Об организации защиты персональных данных

В соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Постановления Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»,

П Р И К А З Ы В А Ю:

1. Утвердить политику обработки и защиты персональных данных в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (Приложение №1)
2. Утвердить инструкцию по работе сотрудников Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска в сети Интернет (Приложение №2)
3. Утвердить положение о персональных данных в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (Приложение №3)
4. Утвердить положение о порядке обработки персональных данных без использования средств автоматизации в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (Приложение №4)
5. Утвердить инструкцию по разграничению доступа пользователей к средствам защиты и информационным ресурсам в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (Приложение №5)
6. Утвердить Инструкцию по работе ответственного лица за организацию обработки персональных данных в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (Приложение №6)
7. Утвердить инструкцию по организации парольной защиты в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный

центр для несовершеннолетних» Ленинского района города Челябинска (Приложение №7)

8. Утвердить правила рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (Приложение №8)
9. Утвердить инструкцию пользователя по обеспечению обработки персональных данных в случае возникновения внештатных ситуаций в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (Приложение №9)
10. Утвердить инструкцию по физической охране и контролю доступа в помещения ситуаций в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (Приложение №10)
11. Контроль за исполнением настоящего приказа оставляю за собой.

И.о.директора М.С.Киржацких

Приложение № 1
к приказу №114-о от 24.08.20

УТВЕРЖДАЮ
Директор МКУ СО
«Социально-реабилитационный центр
для несовершеннолетних»
Ленинского района города Челябинска
_____ М.С.Киржацких
«___» _____2020г

Политика обработки и защиты персональных данных в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска

1.Общие сведения

1. Настоящая политика в области обработки и защиты персональных данных в МКУ СО «Социально-реабилитационного центра для несовершеннолетних» Ленинского района города Челябинска. (далее по тексту - Оператор) разработана в целях обеспечения реализации требований законодательства в области обработки и защиты персональных данных.

2. Политика раскрывает категории персональных данных, обрабатываемых Оператором, цели, способы и принципы обработки персональных данных, права и обязанности Оператора при обработке персональных данных, права субъектов персональных данных, а также включает перечень мер, применяемых Оператором в целях обеспечения безопасности персональных данных при их обработке.

3. Настоящая политика является общедоступным документом, декларирующим основы деятельности Оператора при обработке персональных данных.

2. Информация об Операторе

Наименование: Муниципальное казенное учреждение социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска.

ИНН: 7449023101

Адрес местонахождения:

Челябинская область, г. Челябинск, ул. Шота Руставели, д. 15

Тел.: +7(351) 251-47-14

E-mail: SRCLenin15@mail.ru

Сайт: srcleninskiu.eps74.ru

Регистрация в реестре операторов Роскомнадзор

Номер 74-13-000581

Основание внесения оператора в реестр Приказ № 493 от 21.06.2013

Дата начала обработки персональных данных 07.09.1998

Дата и основание внесения записи в реестр Приказ № 64 от 06.04.2018

3. Правовые основания обработки персональных данных

3.1.Политика Оператора в области обработки персональных данных определяется в соответствии со следующими законодательными и нормативными правовыми актами РФ:
3.1.1. ст.ст.23, 24 Конституции Российской Федерации от 12 декабря 1993 года;
3.1.2. ст.ст.35, 85-90 Трудового кодекса Российской Федерации от 30 декабря 2001 года;
3.1.3. Кодексом Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ;
3.1.4. Федеральным законом от 22 октября 2004 г. N 125-ФЗ «Об архивном деле в Российской Федерации»;
3.1.5. Федеральным законом от 27.07.2006 № 152-ФЗ "О персональных данных";
3.1.6. Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
3.1.7. Федеральным законом от 29.12.2012 N 273-ФЗ «Об образовании в Российской Федерации»;
3.1.8. Постановлением Правительства РФ от 18.04.2012 N 343 "Об утверждении Правил размещения в сети Интернет и обновления информации об образовательном учреждении";
3.1.9. Постановлением Правительства Российской Федерации от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации".
3.1.10. Локальными актами Оператора.
3.2. Во исполнение настоящей Политики директором Оператора утверждены локальные акты по вопросам обработки и защиты персональных данных.

4. Цели обработки персональных данных

Оператор обрабатывает персональные данные **работников** Оператора, уволенных работников, кандидатов на замещение вакантных должностей (далее по тексту работники оператора) исключительно в следующих целях:
- прохождения процедуры оформления трудовых отношений;
- реализации основных прав и обязанностей, возложенных на Оператора в рамках трудового законодательства РФ;
- внесения предложений по представлению работников Оператора к государственным наградам и присвоению почетных званий и наград Челябинской области.
- обеспечения соблюдения требований законодательства РФ;
- отражения информации в кадровых документах;
- начисления заработной платы;
- исчисления и уплаты налоговых платежей предусмотренным законодательством РФ;
- представления законодательно установленной отчетности по физическим лицам ИФНС и внебюджетные фонды;
- подачи сведений в банк для оформления банковской карты и последующего перечисления на нее заработной платы, организация и ведение бухгалтерского и налогового учета и отчетности;
- предоставления налоговых вычетов;
- обеспечения безопасных условий труда;
- контроля требований к количеству и качеству выполняемой сотрудником работы;
- предоставления информации в медицинские учреждения, страховые компании;
- обеспечения предоставления сотруднику социального пакета;
- предоставления информации в государственные органы Российской Федерации в порядке, предусмотренным действующим законодательством.

Оператор обрабатывает персональные данные **получателей социальных услуг**, их законных представителей, членов их семей (далее по тексту получатели социальных услуг) исключительно в следующих целях:
- прохождения процедуры приема ребенка в МКУ СО СРЦ;
- организации обратной связи с родителями (законными представителями) в период нахождения ребенка в МКУ СО СРЦ;
- использования данных для формирования учреждением регистра получателей социальных услуг;

- осуществления социальной реабилитации несовершеннолетнего;

- индивидуального учета результатов проведенных реабилитационных мероприятий;

- хранения в архивах сведений о результатах проведенных реабилитационных мероприятий;

- видеонаблюдения, фото и видео съемки во время участия в мероприятиях и проектах, реализуемых в МКУ СО СРЦ;

- устранения угрозы жизни и здоровью несовершеннолетнего;

- оказания социально-педагогических, социально-психологических, социально-бытовых, социально-трудовых и других услуг, оказываемых МКУ СО СРЦ.

5. Объем и категории субъектов обрабатываемых персональных данных

5.1. В зависимости от субъекта персональных данных, Оператор обрабатывает персональные данные следующих категорий субъектов персональных данных
5.1.1.Работники Оператора, уволенные работники, кандидаты на замещение вакантных должностей;
5.1.2. Получатели социальных услуг, их законных представителей, члены их семей.
5.1.3. Физические лица, направившие Оператору устное и /или письменное обращение/заявление/жалобу (далее по тексту физические лица);
5.2. Оперватором осуществляется обработка следующих персональных данных в зависимости от категории субъекта персональных данных:
5.2.1. Персональные данные **работников** Оператора, включают в себя: фамилия, имя, отчество; дата рождения; паспорт или иной документ, удостоверяющий личность; контактный телефон; фактический адрес проживания, адрес проживания по прописке; сведения об образовании, квалификации и о наличии специальных знаний или специальной подготовки; сведения о повышении квалификации и переподготовке; сведения о трудовой деятельности; сведения о номере, серии и дате выдачи трудовой книжки (вкладыша в нее) и записях в ней; документы воинского учета; сведения о семейном положении; справка о наличии (отсутствии) судимости и (или) факта уголовного преследования либо о прекращении уголовного преследования по реабилитирующим основаниям; заключение по результатам предварительного (периодического) медицинского осмотра; сведения о несовершеннолетних детях; справка по инвалидности (при наличии); сведения, отражающие состояние здоровья (заключение врачей при прохождении первичного, периодического медицинского осмотра); сведения о номере и серии страхового свидетельства государственного пенсионного страхования; сведения об идентификационном номере налогоплательщика.

5.2.2. Персональные данные **получателей социальных услуг, не достигших совершеннолетнего возраста**, включают в себя: фамилия, имя, отчество; школа, класс, домашний адрес; дата и место рождения; сведения и доступ к медицинской документации, отражающих состояние здоровья несовершеннолетнего; паспорт (для лиц, достигших четырнадцатилетнего возраста), свидетельство о рождении несовершеннолетнего (иной документ подтверждающий родство с ребенком или законность представления прав ребенка); сведения о выдаче паспорта (свидетельства о рождении), включая дату выдачи и код подразделения; свидетельство о регистрации ребенка по месту жительства или по месту пребывания на закрепленной территории; телефон, адрес электронной почты; результаты участия несовершеннолетнего в различных олимпиадах, смотрах, конкурсах, соревнованиях и т.п.; сведения о размере одежды; дополнительные данные, которые сообщены в заявлении, договоре, других документах заполняемых получателем социальных услуг, его представителя, членами его семьи. Персональные данные **получателей социальных услуг, включают в себя**: фамилия, имя, отчество; дата рождения; паспорт или иной документ, удостоверяющий личность; контактный телефон; фактический адрес проживания, адрес проживания по прописке; сведения о семейном положении; сведения о несовершеннолетних детях; дополнительные сведения, которые я сообщил (а) в заявлении, договоре и заполняемых мною документах.

5.2.3. Персональные данные **физических лиц**, могут включать в себя: фамилия имя, отчество; почтовый адрес; адрес электронной почты; телефонный номер; иные сведения, необходимые для рассмотрения обращений/заявлений/жалоб.

6. Основные принципы обработки персональных данных

6.1. Оператор в своей деятельности по обработке персональных данных руководствуется следующими принципами:

6.1.1. Обработка персональных данных осуществляется на законной, справедливой и добровольной основе;

6.1.2. Цели обработки персональных данных соответствуют полномочиям Оператора;

6.1.3. Содержание и объем обрабатываемых персональных данных соответствуют целям обработки персональных данных;

6.1.4. Достоверность персональных данных, их актуальность и достаточность для целей обработки, недопустимость обработки избыточных по отношению к целям сбора персональных данных;

6.1.5. Ограничение обработки персональных данных при достижении конкретных и законных целей, запрет обработки персональных данных, несовместимых с целями сбора персональных данных;

6.1.6. Запрет объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

6.1.7. Осуществление хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем это требуют цели обработки персональных данных, если срок хранения персональных данных не установлен действующим законодательством. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

7. Порядок и условия обработки персональных данных

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

7.2. Оператором соблюдаются следующие условия обработки персональных данных:

7.2.1. Обработка персональных данных осуществляется с письменного согласия субъекта персональных данных;

7.2.2. Обработка персональных данных необходима для достижения целей, предусмотренных настоящей Политикой;

7.2.3. Обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно социальных услуг, предусмотренных Федеральным законом от 28.12.2013 г. N 442-ФЗ "Об основах социального обслуживания граждан в Российской Федерации";

7.2.4. Обработка персональных данных необходима для исполнения договора, стороной которого является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться работником Оператора или получателем социальных услуг;

7.2.5. Обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

7.2.6. Обработка персональных данных необходима для осуществления прав и законных интересов оператора или третьих лиц либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта персональных данных.

7.2.7. Обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для

осуществления и выполнения, возложенных законодательством Российской Федерации на Оператора функций, полномочий и обязанностей.

7.3. Сроки обработки персональных данных субъектов персональных данных ограничиваются достижением конкретных, заранее установленных и законных целей.

7.4. Хранение персональных данных осуществляется в форме, позволяющей определить субъекта персональных данных не дольше, чем этого требуют цели обработки персональных данных, кроме случаев, когда срок хранения персональных данных не установлен федеральным законом, договором.

7.5. Сроки хранения персональных данных субъекта персональных данных устанавливается в соответствии с законодательством Российской Федерации.

7.6. Оператором обеспечивается конфиденциальность персональных данных. Лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам, и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено законом.

7.7. По мотивированному запросу исключительно для выполнения возложенных законодательством функций и полномочий персональные данные субъекта персональных данных без его согласия могут быть переданы:

- в судебные органы в связи с осуществлением правосудия;
- в органы государственной безопасности;
- в органы прокуратуры;
- в органы полиции;
- в следственные органы;
-в иные органы и организации в случаях, установленных нормативными правовыми актами, обязательными для исполнения.

7.8. В случае необходимости взаимодействия с третьими лицами в рамках достижения целей, указанных настоящей Политикой, передача персональных данных субъектов осуществляется исключительно по мотивированному запросу и с письменного согласия субъекта.

7.9. Объем передаваемых персональных данных, перечень действий по их обработке и требования к защите обрабатываемых персональных данных при взаимодействии с третьими лицами, соответствуют п. 5.2., п.7.1. 7.2.. п.7.6. настоящей Политики.

7.10. Оператор не осуществляет трансграничную передачу персональных данных на территории иностранных государств;

7.11.Оператор осуществляет обработку персональных данных без использования средств автоматизации, включая передачу информации по внутренней локальной сети и передачу информации по сети Интернет в защищенном режиме.

7.12.Условием прекращения обработки персональных является достижение целей обработки персональных данных, истечение срока действия согласия или отзыв согласия субъекта персональных данных на обработку его персональных данных, а также выявление неправомерной обработки персональных данных.

8. Меры по обеспечению безопасности персональных данных при их обработке

8.1. Оператор при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

8.1.1. Назначением ответственного за организацию обработки персональных данных.

8.1.2. Утверждением 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;

8.1.3.Осуществлением внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ "О персональных данных" и принятыми в соответствии с ним нормативно-правовыми актами, требованиям к защите персональных данных;

8.1.4.Ознакомлением работников Оператора, непосредственно осуществляющих обработку персональных данных, с требованиями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, локальными актами в отношении обработки персональных данных, обучением указанных работников;
8.1.5. Выполнением требований, установленных постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" при обработке персональных данных, осуществляемой без использования средств автоматизации;
8.1.6. Применением прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
8.1.7. Учетом машинных носителей персональных данных;
8.1.8. Выявлением фактов несанкционированного доступа к персональным данным и принятием мер;
8.1.9. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
8.1.10. Установлением правил доступа к персональным данным, обрабатываемым в информационных системах персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых в информационных системах персональных данных.
8.2. Оператор не предоставляет и не раскрывает персональные данные субъектов третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью, для достижения целей предусмотренной настоящей Политикой, а также в случаях, установленных федеральными законами.

9. Права субъектов персональных данных

9.1.Субъект персональных данных имеет право на получение сведений об обработке его персональных данных.
9.2. Субъект персональных данных вправе требовать от Оператора, который их обрабатывает, уточнения этих персональных данных, их блокирования или уничтожения в случае, если они являются неполными, устаревшими, неточными, незаконно полученными или не могут быть признаны необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.
9.3. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с федеральными законами, в том числе в следующих случаях:
9.3.1. Если обработка его персональных данных, включая те, что получены в результате оперативно-розыскной, контрразведывательной и разведывательной деятельности, выполняется в целях укрепления обороны страны, обеспечения безопасности государства и охраны правопорядка;
9.3.2. При условии, что обработка персональных данных по подозрению в совершении преступления, либо предъявившими субъекту персональных данных обвинения по уголовному делу, либо применившими к субъекту персональных данных меру пресечения обвинения, за исключением предусмотренных уголовно-процессуальным законодательством РФ случаев, когда допускается ознакомление подозреваемого или обвиняемого с такими персональными данными;
9.3.3. Если обработка персональных данных выполняется в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
9.3.4. Когда доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.
9.3.5. Если обработка персональных данных осуществляется в случаях, предусмотренных законодательством РФ о транспортной безопасности, в целях обеспечения устойчивого и безопасного функционирования транспортного комплекса, защиты интересов личности, общества и государства в сфере транспортного комплекса от актов незаконного вмешательства;

9.3.6. Для реализации своих прав и защиты законных интересов субъект персональных данных имеет право обратиться к Оператору. Оператор рассматривает любые обращения и жалобы со стороны субъектов персональных данных, тщательно расследует факты нарушений и принимает все необходимые меры для их немедленного устранения, наказания виновных лиц и урегулирования спорных и конфликтных ситуаций в досудебном порядке.

9.4. Субъект персональных данных вправе обжаловать действия или бездействие Оператора путем обращения в уполномоченный орган по защите прав субъектов персональных данных.

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

10. Актуализация, исправление, удаление и уничтожение персональных данных

10.1. В случае подтверждения факта неточности персональных данных или неправомерности их обработки, персональные данные подлежат их актуализации Оператором, с учетом прекращения обработки персональных данных соответственно.

10.2. При достижении целей обработки персональных данных, а также случаев отзыва субъектом персональных данных согласия на их обработку персональные данные подлежат уничтожению.

11. Заключительные положения

12.1. Настоящая Политика утверждается директором МКУ СО СРЦ

12.2. При изменении законодательства и по необходимости данная Политика подлежит пересмотру.

12.3. Настоящая Политика обязательна для соблюдения, и подлежит ознакомлению всех работников, а также публикации на официальном сайте Оператора.

Приложение №2
к приказу №114-ОД от 24.08.20

ИНСТРУКЦИЯ

по работе сотрудников Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска в сети Интернет

Общие положения:

1.1. Настоящая инструкция является дополнением к политике обработки и защиты персональных данных.

1.2. Целью настоящей инструкции является регулирование работы системных администраторов и пользователей, распределения сетевых ресурсов коллективного пользования и поддержания необходимого уровня защиты информации, ее сохранности и соблюдения прав доступа к информации.

Более эффективного использования сетевых ресурсов и уменьшить риск умышленного или неумышленного неправильного их использования.

1.3. К работе в системе допускаются сотрудники, прошедшие инструктаж и зарегистрированные ответственного за работу в сети Интернет.

1.4. Работа в системе каждому работнику разрешена только на определенных компьютерах, в определенное время и только с разрешенными программами и сетевыми ресурсами. Если нужно работать вне указанного времени, на других компьютерах и с другими программами, необходимо получить разрешение системного администратора.

1.5. По уровню ответственности и правам доступа к СЕТИ пользователи СЕТИ разделяются на следующие категории: системные администраторы и пользователи.

1.6.Пользователь подключенного к СЕТИ компьютера - лицо, за которым закреплена ответственность за данный компьютер. Пользователь должен принимать все необходимые меры по защите информации и контролю за соблюдением прав доступа к ней.

1.7.Каждый сотрудник пользуется индивидуальным именем пользователя для своей идентификации в сети.

1.8 Каждый сотрудник САМ создает пароль для входа в компьютерную сеть. При этом пароль должен содержать не менее 8 символов и состоять из букв и цифр.

1.9. Каждый сотрудник должен пользоваться только своим именем пользователя и паролем для входа в локальную сеть и сеть Интернет, передача их кому-либо запрещена.

1.10. Для работы на компьютере кроме пользователя необходимо разрешение системного администратора. Никто не может давать разрешение на даже временную работу на компьютере, без разрешения системного администратора.

1.11. В случае нарушения правил пользования сетью, связанных с администрируемым им компьютером, пользователь сообщает системному администратору, который проводит расследование причин и выявление виновников нарушений и принимает меры к пресечению подобных нарушений. Если виновником нарушения является пользователь данного компьютера, администратор имеет право отстранить виновника от пользования компьютером или принять иные меры.

1.12. В случае появления у пользователя компьютера сведений или подозрений о фактах нарушения настоящих правил, а в особенности о фактах несанкционированного удаленного доступа к информации, размещенной на контролируемом им компьютере ли каком-либо другом, пользователь должен немедленно сообщить об этом системному администратору.

1.13. Системный администратор и лицо, обслуживающее сервер и следящее за правильным функционированием СЕТИ.

Системный администратор дает разрешение на подключение компьютера к СЕТИ. Самовольное подключение является серьезнейшим нарушением правил пользования СЕТЬЮ.

1.14. Системный администратор информирует пользователей обо всех плановых профилактических работах, могущих привести к частичной или полной неработоспособности СЕТИ на ограниченное время, а также об изменениях предоставляемых сервисов и ограничениях, накладываемых на доступ к ресурсам СЕТИ.

1.15. Системный администратор имеет право отключить компьютер пользователя от СЕТИ в случае, если с данного компьютера производились попытки несанкционированного доступа к информации на других компьютерах, и в случаях других серьезных нарушений настоящей инструкции.

1.16. Пользователь должен ознакомиться с настоящей инструкцией. Обязанность ознакомления пользователя с инструкцией лежит на системном администраторе и начальнике отдела ИТО.

2 Пользователи СЕТИ обязаны:

2.1. Соблюдать правила работы в СЕТИ, оговоренные настоящей инструкцией.

2.2. При доступе к внешним ресурсам СЕТИ, соблюдать правила, установленные системными администраторами для используемых ресурсов.

2.3. Немедленно сообщать системному администратору СЕТИ об обнаруженных проблемах в использовании предоставленных ресурсов, а также о фактах нарушения настоящей инструкции кем-либо. Администраторы, при необходимости, с помощью других специалистов, должны провести расследование указанных фактов и принять соответствующие меры.

2.4. Не разглашать известную им конфиденциальную информацию (имена пользователей, пароли),необходимую для безопасной работы в СЕТИ.

2.5. Немедленно отключать от СЕТИ компьютер, который подозревается в заражении вирусом.

Компьютер не должен подключаться к СЕТИ до тех пор, пока системные администраторы не удостоверятся в удалении вируса.

2.6.Обеспечивать беспрепятственный доступ системному администратору к сетевому оборудованию и компьютерам пользователей.

2.7.Выполнять предписания системного администратора, направленные на обеспечение безопасности СЕТИ.

2.8. В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к системному администратору.

3 Пользователи СЕТИ имеют право:

3.1. Использовать в работе предоставленные им сетевые ресурсы в оговоренных в настоящей инструкции

3.2. Обращаться к администратору СЕТИ по вопросам, связанным с распределением ресурсов компьютера. Какие-либо действия пользователя, ведущие к изменению объема используемых им ресурсов, или влияющие на загруженность или безопасность системы (например, установка на компьютере коллективного доступа), должны санкционироваться системным администратором СЕТИ.

3.3. Обращаться за помощью к системному администратору при решении задач использования ресурсов СЕТИ.

3.4. Вносить предложения по улучшению работы с ресурсом.

4 Пользователям СЕТИ запрещено:

4.1. Разрешать посторонним лицам пользоваться закрепленным за ним компьютером (кроме случаев подключения/отключения ресурсов, выполняемого специалистами ИТО).

4.2. Использовать сетевые программы, не предназначенные для выполнения прямых служебных обязанностей без согласования с системным администратором.

4.3. Самостоятельно устанавливать или удалять установленные системным администратором сетевые программы на компьютерах, подключенных к СЕТИ, изменять настройки операционной системы и приложений, влияющие на работу сетевого оборудования и сетевых ресурсов.

4.4.Повреждать, уничтожать или фальсифицировать информацию, не принадлежащую пользователю.

4.5. Вскрывать компьютеры, сетевое и периферийное оборудование; подключать к компьютеру дополнительное оборудование без ведома системного администратора, изменять настройки, а также производить загрузку рабочих станций с дисков или флеш-карт.

4.6. Самовольно подключать компьютер к СЕТИ, а также изменять IP-адрес компьютера, выданный системным администратором. Передача данных в сеть с использованием

других IP адресов в качестве адреса отправителя является распространением ложной информации и создает угрозу безопасности информации на других компьютерах.
4.7. Работать с каналоемкими ресурсами (real video, real audio, chat и др.) без согласования с системным администратором СЕТИ. При сильной перегрузке канала вследствие использования каналоемких ресурсов текущий сеанс пользователя, вызвавшего перегрузку, будет прекращен.
4.8. Получать и передавать в сеть информацию, противоречащую законодательству и нормам морали общества, представляющую коммерческую или государственную тайну, распространять через сеть информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.
4.9. Обхождение учетной системы безопасности, системы статистики, ее повреждение и по дезинформация.
4.10. Использовать иные формы доступа к сети Интернет, за исключением разрешенных системным администратором; пытаться обходить установленный межсетевой экран при соединении с сетью Интернет.
4.11. Осуществлять попытки несанкционированного доступа к ресурсам СЕТИ, проводить или участвовать в сетевых атаках и сетевом взломе.
4.12. Использовать СЕТЬ для совершения коммерческих сделок, распространения рекламы, коммерческих объявлений, порнографической информации, призывов к насилию, разжиганию национальной или религиозной вражды, оскорблений, угроз и т.п.
4.13. Пользователи должны уважать право других пользователей на личную информацию. Это означает, что пользователь (системный администратор) не имеет права пользоваться чужими именами и паролями для входа в сеть, читать чужую почту, причинять вред данным (кроме случаев, указанных выше), принадлежащих другим пользователям.
4.14. Запрещается производить действия, направленные на взлом (несанкционированное получение привилегированного доступа) рабочих станций и сервера Сети, равно как и любых других компьютеров в Интернет.
4.15. Закрывать доступ к информации паролями без согласования с системным администратором.
5 Работа с электронной почтой:
5.1. Электронная почта предоставляется сотрудникам только для выполнения своих служебных обязанностей. Использование ее в личных целях запрещено.
5.2. Входящие письма должны проверяться на наличие вирусов или других вредоносных программ.
5.3. Необходимо организовать обучение пользователей правильной работе с электронной почтой.
5.4. Справочники электронных адресов сотрудников не могут быть доступны всем и являются конфиденциальной информацией.
5.5. Никто из посетителей, контрактников или временных служащих не имеет права использовать электронную почту.
5.6. Исходящие сообщения могут быть выборочно проверены, чтобы гарантировать соблюдение правил работы с электронной почтой.
5.7. Пользователи не должны позволять кому-либо посылать письма от чужого имени.
5.8. В качестве клиентов электронной почты могут использоваться только утвержденные почтовые программы.
5.9. Конфиденциальная информация не может быть послана с помощью электронной почты.
5.10. Если будет установлено, что сотрудник неправильно использует электронную почту с умыслом, к нему будет применено дисциплинарное взыскание.
5.11. Запрещено открывать или запускать приложения, полученные по электронной почте от неизвестного источника и (или) не затребованные пользователем.
5.12. Запрещено осуществлять массовую рассылку не согласованных предварительно электронных писем. Под массовой рассылкой подразумевается как рассылка множеству получателей, так и множественная рассылка одному получателю (спам).
5.13. Запрещено использовать несуществующие обратные адреса при отправке электронных писем.
6 При работе с веб-ресурсами:

6.1. Пользователи используют программы для поиска информации в WWW только в случае, если это необходимо для выполнения своих должностных обязанностей.
6.2. Использование ресурсы сети Интернет разрешается только в рабочих целях. использование её ресурсов не должно потенциально угрожать информационной системе.
6.3. По использованию Интернет ведется статистика.
6.4. Действия любого пользователя, подозреваемого в нарушении правил пользования Интернетом. могут быть запротоколированы и использоваться для принятия решения о применении к нему дисциплинарных мер.
6.5. Сотрудникам, пользующимся Интернетом, запрещено передавать или загружать на компьютер материал, который является непристойным, порнографическим, фашистским или расистским.
6.6. Все программы, используемые для доступа к сети Internet, должны быть утверждены сетевым администратором и на них должны быть настроены необходимые уровни безопасности.
6.7. Все файлы, загружаемые с помощью сети Internet, должны проверяться на вирусы с помощью утвержденных руководством антивирусных программ.
6.8. Сотрудники, нанятые по контракту, должны соблюдать эту политику после предоставления им доступа к Internet.
6.9. В учреждении должна быть организована фильтрация запрещенных ресурсов Internet. Программы для работы с Internet должны быть сконфигурированы так, чтобы к этим сайтам нельзя было получить доступ.
6.10. Запрещено размещать в гостевых книгах, форумах, конференциях сообщения содержащие грубые и оскорбительные выражения.
6.11.
Запрещено получать и передавать через СЕТЬ информацию. законодательству и нормам морали общества, представляющую распространять информацию, задевающую честь и достоинство граждан, а также рассылать обманные, беспокоящие или угрожающие сообщения.
6.12. Запрещено получать доступ к информационным ресурсам СЕТИ или сети Интернет, не являющихся публичными, без разрешения их собственника.
7 Ответственность:
7.1. Пользователь компьютера отвечает за информацию, хранящуюся на его компьютере. технически исправное состояние компьютера и вверенной техники.
7.2. Системный администратор отвечает за бесперебойное функционирование вверенной ему СЕТИ, качество предоставляемых пользователям сервисов.
7.3. Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в СЕТИ и за ее пределами.
7.4. За нарушение настоящей инструкции пользователь может быть отстранен от работы с СЕТЬЮ.
7.5. Нарушение данной инструкции, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, нарушение работы компьютеров пользователей, системы или СЕТИ компьютеров, может повлечь административную или уголовную ответственность в соответствии с действующим законодательством.

Приложение № 3
к приказу №[illegible] от 24.08.20

Положение о персональных данных

1. Общие положения

1.1. Настоящее Положение о персональных данных Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (далее – Положение) разработано на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 27.07.2006 № 152- ФЗ «О персональных данных» и других нормативных правовых актов Российской Федерации.

1.2. Настоящим Положением определяется порядок обработки персональных данных субъектов персональных данных как с использованием средств автоматизации, так и без использования таковых.

1.3. Целью настоящего Положения является обеспечение защиты прав и свобод сотрудников Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска и иных граждан, предоставивших свои персональные данные, при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.4. Положение распространяется также на персональные данные любых иных лиц, содержащихся в документах, полученных Муниципальным казенным учреждением социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска из других организаций, в обращениях граждан и иных источниках персональных данных.

1.5. Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, а также затруднения реализации прав и свобод граждан Российской Федерации.

1.6. Персональные данные защищаются от несанкционированного доступа в соответствии с нормативно-правовыми актами Российской Федерации, нормативно-распорядительными актами и рекомендациями регулирующих органов в области защиты информации, а также утвержденными положениями и инструкциями Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска.

1.7. Персональные данные относятся к категории конфиденциальной информации. Обработка персональных данных субъекта персональных данных без письменного его согласия не допускается, если иное не определено законом. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении сроков хранения, если иное не определено законом.

1.8. Должностные лица Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска, в обязанности которых входит обработка персональных данных субъектов, обязаны обеспечить каждому субъекту возможность ознакомления в установленном порядке, со своими персональными данными, если иное не предусмотрено законом.

1.9. Настоящее Положение утверждается директором Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска и является обязательным для исполнения всеми сотрудниками _____, имеющими доступ к персональным данным субъектов персональных данных.

2. Основные понятия, применяемые в настоящем Положении:

2.1. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, определяемая нормативно-правовыми актами Российской Федерации, Перечнем ПДн, обрабатываемых в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска, настоящим Положением и другими локальными правовыми актами.

2.2. Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

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

2.4. Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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

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

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

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

2.9. Конфиденциальность персональных данных – обязательное для соблюдения любым сотрудником или иным получившим доступ к персональным данным лицом требование, не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

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

2.11. Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

2.12. К субъектам персональных данных (далее – субъекты) относятся сотрудники Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска, включая совместителей и лиц, выполняющие работы по договорам гражданско-правового характера, персональные данные которых переданы (как на добровольной основе, так и в рамках выполнения требований нормативно-правовых актов) для обработки, а также иные лица, предоставляющие персональные данные.

3. Правила обработки персональных данных

3.1. Обработка персональных данных осуществляется на основе следующих принципов:

3.1.1. Законности целей и способов обработки персональных данных и добросовестности;

3.1.2. Соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям предприятия;

3.1.3. Соответствия объема, характера и способов обработки персональных данных целям обработки;

3.1.4. Достоверности и достаточности персональных данных для целей обработки;

3.1.5. Недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

3.1.6. Недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных.

3.2. Собственником своих персональных данных является субъект персональных данных и он самостоятельно решает вопрос передачи своих персональных данных.

3.3. Необходимым условием обработки персональных данных субъекта персональных данных является его письменное согласие.

3.4. Субъект персональных данных обязан передать комплекс достоверных, документированных персональных данных, состав которых установлен трудовым законодательством, иными законами Российской Федерации, включая сведения об образовании, специальных знаниях, стаже работы, отношении к воинской обязанности, гражданстве, месте жительства и др.

3.5. Муниципальное казенное учреждение социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска имеет право проверять достоверность указанных сведений в порядке, не противоречащем законодательству России.

3.6. Субъект персональных данных имеет право на свободный и бесплатный доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных федеральными законами, а также получать информацию, касающуюся обработки его персональных данных.

3.7. Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, производится не дольше, чем этого требуют цели их обработки.

3.8. Уничтожение персональных данных производится при достижении целей обработки или в случае утраты необходимости в их обработке.

3.9. Согласие на обработку персональных данных может быть отозвано субъектом персональных данных в соответствии с положением статьи 6 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

3.10. В случае отзыва субъектом согласия на обработку своих персональных данных, оператор обязан прекратить обработку персональных данных и уничтожить персональные данные. Об уничтожении персональных данных оператор обязан уведомить субъекта персональных данных.

3.12. В целях информационного обеспечения функционирования могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги). В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться фамилия, имя, отчество, адрес, абонентский номер, сведения о должности и иные персональные данные, предоставленные субъектом.

3.12. Перечень должностей, замещение которых предусматривает доступ к обработке персональных данных, определяется приказом директора Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска

3.13. Муниципальное казенное учреждение социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска обязан сообщить в уполномоченный орган по защите прав субъектов персональных данных по его запросу информацию, необходимую для осуществления деятельности указанного органа в установленные нормативно-правовыми актами Российской Федерации сроки.

3.14. Внутренний доступ (доступ внутри Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска) к персональным данным субъектов имеют сотрудники, которым эти данные необходимы для выполнения должностных обязанностей.

3.14. Внешний доступ к персональным данным субъектов имеют массовые потребители персональных данных и контрольно-надзорные органы.

3.16. Надзорно-контрольные органы имеют доступ к информации исключительно в сфере своей компетенции.

3.17. Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе деятельности Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска

3.18. При обработке персональных данных принимаются необходимые организационные и технические меры, в том числе используются криптографические средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования и распространения, а также от иных неправомерных действий.

3.19. Мероприятия по технической защите персональных данных проводятся в соответствии с Приказом ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», требованиями приказа ФСТЭК 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», постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказом ФСБ России от 10.07.2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

4. Ответственность за разглашение конфиденциальной информации

4.1. За разглашение информации лицом, получившим доступ к персональным данным в связи с исполнением служебных обязанностей, предусмотрена ответственность в соответствии с действующим законодательством Российской Федерации.

4.2. За неправомерный отказ в предоставлении субъекту персональных данных доступа к своим персональным данным или в получении информации, касающейся обработки его персональных данных, предусмотрена административная ответственность.

4.3. Муниципальное казенное учреждение социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска как юридическое лицо, должностные лица и иные сотрудники Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска, в соответствии со своими полномочиями владеющие персональными данными субъектов, получающие и использующие их, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

4.4. Нарушение неприкосновенности частной жизни (в том числе незаконный сбор или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), совершенные лицом с использованием своего служебного положения, влечет наложение наказания в порядке, предусмотренном Уголовным кодексом Российской Федерации.

Приложение № 4

к приказу №114-ОТ от 24.08.20

ПОЛОЖЕНИЕ
О ПОРЯДКЕ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Правила обработки персональных данных, осуществляемой без использования средств автоматизации в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска, установленные настоящим Положением, должны применяться с учетом требований Постановления Правительства Российской Федерации "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" от 15 сентября 2008 года № 687, а также требований нормативных правовых актов федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации.

II. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2. Несанкционированный доступ (далее – НСД) - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

3. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

4. Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

5. 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.

6. Обработка персональных данных без использования средств автоматизации – обработка персональных данных, при которой такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

7. Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

8. Уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

III. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

9. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

10. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

11. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе работники Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска или лица, осуществляющие такую обработку по договору с Муниципальным казенным учреждением социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска.

12. При использовании форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться следующие условия:

1) типовая формулировки (далее – форма) или связанные с ними документы должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, наименование и адрес Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых Муниципальным казенным учреждением социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска способов обработки персональных данных;

2) форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

3) форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

13. При ведении журналов (журналов регистрации, журналов посещений), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных в помещение Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска или в иных аналогичных целях, должны соблюдаться следующие условия:

1) необходимость ведения такого журнала должна быть предусмотрена нормативно-правовым актом, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных данных. Перечень лиц, имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных определены должностной инструкцией работника «Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска.

2) копирование содержащейся в таких журналах информации не допускается.

14. По истечении срока хранения документы, содержащие персональные данные, должны быть уничтожены без возможности восстановления.

15. Уничтожение персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

16. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

IV. МЕРЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ, ОСУЩЕСТВЛЯЕМОЙ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

17. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

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

19. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются приказом начальника Муниципального казенного учреждения социального обслуживания «Социально-

реабилитационный центр для несовершеннолетних» Тракторозаводского района города Челябинска.

V. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ НОРМ, РЕГУЛИРУЮЩИХ ОБРАБОТКУ И ЗАЩИТУ ПЕРСОНАЛЬНЫХ ДАННЫХ

20. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на работников Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска, имеющих доступ к персональным данным, администратора безопасности информационных систем персональных данных Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска и ответственного за организацию обработки персональных данных Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска.

21. Работники Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Тракторозаводского района города Челябинска, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

22. Разглашение персональных данных субъекта (передача их посторонним лицам, в том числе другим сотрудникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих персональные данные субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами (приказами, распоряжениями) Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска, влечет наложение на работника, имеющего доступ к персональным данным, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска, имеющий доступ к персональным данным субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (в соответствии с п.7 ст. 243 Трудового кодекса РФ).

23. В отдельных случаях, при разглашении персональных данных, работник Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска, совершивший указанный проступок, несет ответственность в соответствии со статьей 13.14 Кодекса об административных правонарушениях РФ.

24. В случае незаконного сбора или публичного распространения информации о частной жизни лица (нарушения неприкосновенности частной жизни), предусмотрена ответственность в соответствии со ст. 137 Уголовного кодекса РФ.

25. Начальник Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска за нарушение норм, регулирующих получение, обработку и защиту персональных данных субъектов, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает субъекту ущерб, причиненный неправомерным использованием информации, содержащей персональные данные этого субъекта.

Приложение № 5

к приказу №114/2 от 24.08.20

Инструкция
по разграничению доступа пользователей к средствам защиты и информационным ресурсам

1.Общие положения

1. Данная Инструкция определяет порядок организации работ по разграничению доступа пользователей к средствам защиты и информационным ресурсам, обрабатываемым в информационных системах персональных данных (далее – ИСПДн) в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска
2. Основными видами угроз безопасности информационных систем являются:
   - противоправные действия посторонних лиц;
   - ошибочные действия пользователей ИСПДн;
   - отказы и сбои технических средств ИСПДн, приводящие к ее модификации, блокированию, уничтожению или несанкционированному копированию, а также нарушению правил эксплуатации ЭВМ и сетевого оборудования.
3. Целью защиты информации является:
   - предотвращение утечки, хищения, утраты, подделки информации, а также неправомерных действий по уничтожению, модификации, искажению, несанкционированному копированию, блокированию информации, предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы обеспечения правового режима документированной информации как объекта собственности;
   - защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в ИСПДн;
   - сохранение конфиденциальности информации в соответствии с законодательством Российской Федерации;
   - обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.
4. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИСПДн, администратора безопасности (далее – АБ) и ответственного за обеспечение безопасности персональных данных.
5. Субъекты доступа, получающие доступ к базам данных и другим информационным ресурсам, должны изучить Инструкцию пользователя информационных систем персональных данных и оставить письменное подтверждение (подпись) о неразглашении ими информации, к которой они имеют доступ, паролей, а также в том, что за нарушение правил информационной безопасности и данной Инструкции они несут персональную ответственность в соответствии с законодательством Российской Федерации.

Термины и определения

1. Информация – сведения (сообщения, данные) независимо от формы их представления.
2. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.
3. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.
4. Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.
5. Доступ к информации – возможность получения информации и ее использования.
6. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

Разграничение доступа пользователей к информационным ресурсам и средствам защиты информации

1. Защита от несанкционированного доступа осуществляется:
   - идентификацией и проверкой подлинности пользователей ИСПДн при доступе к информационным ресурсам;
   - разграничением доступа к обрабатываемым базам данных. Для осуществления доступа к информационным ресурсам, АБ назначает конкретному пользователю ИСПДн идентифицирующее имя пользователя, кодирует персональный идентификатор (при его наличии) и предоставляет возможность задать пароль;
   - АБ должен осуществлять мероприятия по обеспечению защиты информационных ресурсов от несанкционированного доступа и непреднамеренных изменений и разрушений, а также иметь в наличии средства восстановления, резервные копии, предусматривающие процедуру восстановления свойств информационных ресурсов после сбоев и отказов оборудования.

Обеспечение сохранности информации

1. Для обеспечения сохранности электронных информационных ресурсов необходимо соблюдать следующие требования:
   - АБ должен иметь не менее двух резервных копий программного обеспечения для работы с информационными ресурсами, хранимых в разных помещениях, а также методику восстановления данных;
   - резервное копирование информационных ресурсов должно производиться в соответствии с документацией на используемое программное обеспечение;
   - в случае сбоя или порчи восстановление информационных ресурсов из резервных копий производится в соответствии с документацией на используемое программное обеспечение с составлением акта;
   - для копирования информации должны использоваться только проверенные на наличие компьютерных вирусов и других вредоносных программ носители информации.
2. Субъектам доступа запрещается:
   - установка и использование при работе с компьютерами вредоносных программ, ведущих к блокированию работы системы;

- самовольное изменение сетевых адресов;
- самовольное вскрытие блоков компьютеров, модернизация или модификация компьютеров и программного обеспечения;
- несанкционированная передача компьютеров с прописанными сетевыми настройками. Передача компьютеров производится только АБ с предварительно удаленными сетевыми настройками.

3. Сведения, содержащиеся в электронных документах, и базы данных должны использоваться только в служебных целях в рамках полномочий работника, работающего с соответствующими материалами.

Приложение № 6
к приказу №1140 от 24.08.20

Инструкция
по работе ответственного лица за организацию обработки персональных данных

1.Общие положения

1.1. Данная Инструкция определяет основные обязанности, права и ответственность ответственного лица за организацию обработки персональных данных в «Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (далее – СРЦ)

1.2. Ответственное лицо за организацию обработки персональных данных является штатным работником СРЦ и назначается директором СРЦ.

1.3. Ответственное лицо за организацию обработки персональных данных (далее – Ответственный) – лицо, отвечающее за организацию обработки персональных данных с использованием средств автоматизации и без использования таких средств.

1.4. Решение вопросов организации защиты персональных данных в СРЦ входит в прямые служебные (трудовые) обязанности Ответственного.

1.5. Ответственный отвечает за поддержание необходимого уровня безопасности объектов защиты, является уполномоченным на проведение соответствующих работ.

1.6. Ответственный в своей работе руководствуется Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлениями Правительства, а также другими нормативными правовыми актами, действующими на территории Российской Федерации, настоящей Инструкцией и иными регламентирующими документами СРЦ.

1.7. Требования Ответственного, связанные с выполнением им своих служебных (трудовых) обязанностей, обязательны для исполнения всеми работниками, имеющими санкционированный доступ к персональным данным.

1.8. Ответственный обладает правами доступа к любым программным и аппаратным ресурсам СРЦ, а также к любым носителям персональных данных СРЦ.

2. Термины и определения

2.1. Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных).

2.2. Доступ к информации – возможность получения информации и ее использования.

2.3. Защита информации – деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на информацию, то есть процесс, направленный на достижение информационной безопасности.

2.4. Информация – сведения (сообщения, данные) независимо от формы их представления.

2.5. Информационная система персональных данных (далее - ИСПДн) – совокупность содержащихся в базах данных персональных данных и

обеспечивающих их обработку информационных технологий и технических средств.

2.6. Несанкционированный доступ (далее – НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

2.7. Носитель информации – любой материальный объект или среда, используемый для хранения или передачи информации.

2.8. 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.

2.9. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.10. Пользователь – работник СРЦ, участвующий в рамках своих функциональных обязанностей в процессах обработки персональных данных.

2.11. Средство защиты информации (далее – СЗИ) – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

2.12. Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных.

3. Обязанности ответственного

3.1. В области автоматизированной обработки персональных данных Ответственный обязан:

3.1.1. взаимодействовать с администратором безопасности ИСПДн по вопросам обеспечения и выполнения требований обработки персональных данных (далее – администратор безопасности);

3.1.2. контролировать осуществление мероприятий по установке и настройке СЗИ;

3.1.3. осуществлять контроль за порядком учета, создания, хранения и использования резервных копий и машинных носителей, содержащих персональные данные.

3.2. В области обработки персональных данных без использования средств автоматизации Ответственный обязан:

3.2.1. контролировать порядок обработки бумажных носителей персональных данных;

3.2.2. осуществлять проверки наличия документов, содержащих персональные данные.

3.3. В области информирования работников Ответственный обязан:

3.3.1. доводить до сведения работников положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

3.3.2. осуществлять методическое руководство работников, имеющих санкционированный доступ к персональным данным, в вопросах обеспечения безопасности персональных данных;

3.3.3. организовывать повышение квалификации работников в области защиты персональных данных.

3.4. В области работы с субъектами персональных данных Ответственный обязан:

3.4.1. разъяснять субъекту персональных данных юридические последствия отказа предоставления его персональных данных;

3.4.2. организовывать прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществлять контроль за приемом и обработкой обращений и запросов.

3.5. В области контроля работников Ответственный обязан:

3.5.1. осуществлять внутренний контроль за соблюдением оператором и его работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

3.5.2. планировать мероприятия по организации обеспечения безопасности персональных данных;

3.5.3. организовывать и осуществлять периодический контроль пользователей по соблюдению ими режима конфиденциальности, правил работы со съемными машинными носителями информации, выполнению организационных мер по защите информации, а также принимать участие в проведении проверок уполномоченными структурами;

3.5.4. организовывать работы по плановому контролю работоспособности технических средств защиты персональных данных, охраны объекта, средств защиты информации от НСД;

3.5.5. контролировать соблюдение пользователями локальных документов, регламентирующих порядок работы с программными, техническими средствами ИСПДн и персональными данными.

3.6. В области учета лиц, имеющих доступ к персональным данным, Ответственный обязан:

3.6.1. знать и предоставлять на утверждение директору СРЦ изменения в перечень должностей работников СРЦ, замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным в информационных системах.

3.6.2. участвовать в определении полномочий пользователей ИСПДн (оформлении разрешительной системы доступа), минимально необходимых им для выполнения служебных (трудовых) обязанностей.

3.7. Иные обязанности Ответственного:

3.7.1. проводить разбирательства и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных;

3.7.2. по указанию руководства своевременно и точно отражать изменения в локальных нормативных правовых актах по правилам обработки персональных данных;

3.7.3. знать перечень и условия обработки персональных данных в СРЦ;

3.7.4. осуществлять организацию учета документов, содержащих персональные данные, их уничтожение, либо контроль процедуры их уничтожения;

3.7.5. блокировать доступ к персональным данным при обнаружении нарушений порядка их обработки;

3.7.6. реагировать на попытки НСД к информации в установленном ст. 5 настоящей Инструкции порядке;

3.7.7. представлять интересы СРЦ при проверках надзорных органов в

сфере обработки персональных данных;

3.7.8. участвовать в работе комиссий СРЦ по пересмотру планов защиты персональных данных.

3.7.9. знать законодательство РФ о персональных данных, следить за его изменениями;

3.7.10. выполнять иные мероприятия, требуемые нормативными документами по защите персональных данных.

4. Права ответственного

4.1. Ответственный имеет право:

4.1.1. запрашивать и получать необходимые материалы для организации и проведения работ по вопросам организации обработки и обеспечения безопасности персональных данных;

4.1.2. требовать от всех пользователей выполнения установленной технологии обработки персональных данных, инструкций и других нормативных правовых документов по обеспечению безопасности персональных данных;

4.1.3. инициировать блокирование доступа работников к персональным данным, если это необходимо для предотвращения нарушения режима защиты персональных данных;

4.1.4. инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несоблюдения условий хранения носителей персональных данных, нарушения правил работы с документами, содержащими персональные данные, НСД, утраты, порчи защищаемых носителей персональных данных и технических средств из состава информационных систем или по другим нарушениям, которые могут привести к снижению уровня защищенности персональных данных;

4.1.5. обращаться к директору СРЦ с предложением о приостановке процесса обработки персональных данных или отстранению от работы пользователя в случаях нарушения установленной технологии обработки персональных данных или нарушения режима конфиденциальности;

4.1.6. подавать свои предложения по совершенствованию мер защиты персональных данных в ИСПДн, разработке и принятии мер по предотвращению возможных опасных последствий нарушений, приводящих к снижению уровня защищенности персональных данных.

5. Действия при обнаружении попыток НСД

5.1. К попыткам НСД относятся:

5.1.1. сеансы работы с персональными данными незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, или срок действия полномочий которых истек, или превышающих свои полномочия по доступу к данным;

5.1.2. действия постороннего лица, пытающегося получить доступ (или уже получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, методом подбора пароля, использования пароля, разглашенного владельцем учетной записи или любым другим методом.

5.2. Защита от несанкционированного доступа осуществляется:

5.2.1. идентификацией и проверкой подлинности пользователей ИСПДн при доступе к информационным ресурсам СРЦ;

5.2.2. разграничением доступа к обрабатываемым базам данных. Пользователь ИСПДн допускается только к тем ресурсам, которые разрешены для него.

5.3. При выявлении факта НСД Ответственный обязан:

5.3.1. по возможности пресечь дальнейший НСД к персональным данным;

5.3.2. доложить директору СРЦ служебной запиской о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

5.3.3. известить руководителя структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

5.3.4. известить администратора безопасности о факте НСД.

6. Ответственность

6.1. Ответственный несет персональную ответственность за:

6.1.1. соблюдение требований настоящей Инструкции;

6.1.2. правильность и объективность принимаемых решений;

6.1.3. качество и своевременность проводимых им работ по обеспечению безопасности персональных данных;

6.1.4. за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учетной записи.

6.2. Ответственный при нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несет дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 7
к приказу №1105 от 24.08.20

Инструкция по организации парольной защиты

1.Общие положения

1.1. Настоящая инструкция разработана в соответствии нормативными документами по безопасности информации и регламентирует процессы генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн) Муниципального казенного учреждения социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (далее - «СРЦ»), а также контроль над действиями пользователей и обслуживающего персонала при работе с паролями.

1.2. Осуществление процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на администратора безопасности ИСПДн.

2. Термины и определения

2.1. Информация – сведения (сообщения, данные) независимо от формы их представления.

2.2. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу.

2.3. Информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.4. Пароль – секретная комбинация цифр, знаков, слов, или осмысленное предложение, служащие для защиты информации от несанкционированного доступа к информационным ресурсам.

2.5. Компрометация пароля – раскрытие, обнаружение или утеря пароля.

3. Правила формирования паролей

3.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями информационной системы самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя имя пользователя, легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков

(111, qwerty, абвгд и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на информации о пользователе;

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в шести позициях.

3.2. Работникам допускается использовать пароли, составленные из первых букв слов запоминающихся высказываний в разном регистре, смешанные в произвольном порядке со специальными символами (например Кожзгсф7!).

3.3. В случае если формирование личных паролей пользователей осуществляется централизованно, ответственность за правильность их формирования и распределения возлагается на администратора безопасности ИСПДн.

3.4. Для обеспечения возможности использования имен и паролей некоторых работников в их отсутствие (например, в случае возникновении нештатных ситуаций, форс-мажорных обстоятельств и т.п.), работники обязаны сразу же после установки своих паролей передавать их на хранение вместе с именами своих учетных записей администратору безопасности ИСПДн в запечатанном конверте или опечатанном пенале. Опечатанные конверты (пеналы) с паролями работников должны храниться в сейфе, к которому исключен доступ других работников «СРЦ» и посторонних лиц. Для опечатывания конвертов (пеналов) должны применяться личные печати владельцев паролей (при их наличии), либо печать администратора безопасности ИСПДн. Все конверты (пеналы) с паролями в обязательном порядке фиксируются в Журнале учета паролей пользователей (Приложение).

4. Ввод пароля

4.1. При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его просмотра посторонними лицами и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

4.2. При неверном вводе пароля более 5 раз, учетная запись пользователя должна блокироваться не менее чем на 3 минуты и не более чем на 15 минут.

5. Порядок смены личных паролей

5.1. Смена паролей должна проводиться регулярно, не реже одного раза в 12 месяцев.

5.2. В случае прекращения полномочий пользователя (увольнение, переход на другую работу и т.п.) должно производиться немедленное удаление его учетной записи сразу после окончания последнего сеанса работы данного пользователя с системой.

5.3. Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и т.п.) ответственного за обеспечение безопасности персональных данных, администратора безопасности и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

5.4. Администратор безопасности ИСПДн ведет Журнал учета паролей пользователей, в котором он отмечает причины внеплановой смены паролей пользователей.

5.5. Временный пароль, заданный администратором безопасности ИСПДн при регистрации нового пользователя, должен действовать в течение ограниченного срока времени. Пользователь должен изменить временный пароль при первом входе в систему.

6. Хранение пароля

6.1. Запрещается записывать пароли на бумаге, в файле, электронной записной книжке, мобильном телефоне и любых других предметах и носителях информации.

6.2. Запрещается сообщать свой пароль полностью или частично другим пользователям, запрещается спрашивать или подсматривать пароль других пользователей.

6.3. Запрещается регистрировать других пользователей в ИСПДн со своим личным паролем, запрещается входить в ИСПДн под учетной записью и паролем другого пользователя.

7. Действия в случае утери и компрометации пароля

7.1. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя должна быть немедленно проведена внеплановая процедура смены пароля.

8. Ответственность

8.1. Каждый пользователь ИСПДн несет персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учетной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения компрометации пароля его учетной записи.

8.2. Ответственность за контроль проведения мероприятий по организации парольной защиты возлагается на ответственного за организацию обработки персональных данных.

8.3. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, обрабатывающими персональные данные, работники могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение № 8
к приказу №114-ОД от 24.08.20

ПРАВИЛА
РАССМОТРЕНИЯ ЗАПРОСОВ СУБЪЕКТОВ ПЕРСОНАЛЬНЫХ ДАННЫХ
ИЛИ ИХ ПРЕДСТАВИТЕЛЕЙ

1. Настоящие Правила определяют порядок рассмотрения запросов субъектов персональных данных или их представителей в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (далее – СРЦ)

2. Право на получение информации, касающейся обработки своих персональных данных в СРЦ, имеют следующие субъекты персональных данных:

1) работники СРЦ;

2) граждане, претендующие на замещение должностей в СРЦ;

3) Субъекты персональных данных, обработка персональных данных которых осуществляется СРЦ в связи с предоставлением государственных услуг и осуществлением государственных функций.

3. Субъекты персональных данных, указанные в пункте 1 настоящих Правил, имеют право на получение информации, касающейся обработки их персональных данных, в том числе содержащей:

1) подтверждение факта обработки персональных данных в СРЦ;

2) правовые основания и цели обработки персональных данных;

3) применяемые в СРЦ способы обработки персональных данных;

4) наименование и место нахождения СРЦ, сведения о гражданах (за исключением гражданских служащих СРЦ), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с СРЦ или на основании законодательства Российской Федерации;

5) обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких персональных данных не предусмотрен законодательством Российской Федерации в области персональных данных;

6) сроки обработки персональных данных, в том числе сроки их хранения в СРЦ;

7) порядок осуществления субъектом персональных данных прав, предусмотренных Федеральным законом от 27 июля 2006 г. N 152-ФЗ "О персональных данных" (Собрание законодательства Российской Федерации, 2006, N 31, ст. 3451; 2017, N 31, ст. 4772);

8) сведения об осуществленной или предполагаемой трансграничной передаче персональных данных;

9) наименование организации или фамилию, имя, отчество (при

наличии) и адрес лица, осуществляющего обработку персональных данных по поручению СРЦ, если обработка поручена или будет поручена такой организации или лицу;

10) иные сведения, предусмотренные законодательством Российской Федерации в области персональных данных.

4. Субъект персональных данных вправе требовать от СРЦ 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 законодательством Российской Федерации меры по защите своих прав.

5. Сведения, указанные в пункте 3 настоящих Правил, должны быть предоставлены субъекту персональных данных СРЦ 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.

6. Сведения, указанные в пункте 3 настоящих Правил, предоставляются субъекту персональных данных или его представителю уполномоченным должностным лицом СРЦ, осуществляющим обработку персональных данных, при обращении либо при получении запроса субъекта персональных данных или его представителя.

7. Запрос должен содержать:

1) вид, серию, номер документа, удостоверяющего личность субъекта персональных данных или его представителя;

2) сведения о дате выдачи указанного документа и о выдавшем его органе;

3) сведения, подтверждающие участие субъекта персональных данных в отношениях с СРЦ (документ, подтверждающий прием документов на замещение вакантных должностей федеральной государственной гражданской службы в СРЦ» и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных в СРЦ;

4) 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.

8. Если сведения, указанные в пункте 3 настоящих Правил, а также обрабатываемые персональные данные были предоставлены для ознакомления субъекту персональных данных по его запросу, субъект персональных данных вправе обратиться повторно в СРЦ лично или направить повторный запрос в целях получения указанных сведений и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, 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.

9. Субъект персональных данных вправе обратиться повторно в СРЦ лично или направить повторный запрос в целях получения сведений, указанных в пункте 3 настоящих Правил, а также в целях ознакомления с

обрабатываемыми персональными данными до истечения срока, указанного в 8 настоящих Правил, 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 7 настоящих Правил, должен содержать обоснование направления повторного запроса.

10. СРЦ вправе отказать субъекту персональных данных в выполнении повторного запроса, не соответствующего условиям, предусмотренным пунктами 8 и 9 настоящих Правил. Такой отказ должен быть мотивированным.

11. Право субъекта персональных данных на доступ к его персональным данным может быть ограничено в соответствии с законодательством Российской Федерации в области персональных данных, в том числе если доступ субъекта персональных данных к его персональным данным нарушает права и законные интересы третьих лиц.

Приложение № 9
к приказу №1140 от 24.08.20

ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В СЛУЧАЕ ВОЗНИКНОВЕНИЯ ВНЕШТАТНЫХ СИТУАЦИЙ

I. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ

1. Настоящая Инструкция определяет возможные внештатные ситуации, связанные с функционированием информационных систем персональных данных (далее – ИСПДн), меры и средства поддержания непрерывности работы и восстановления работоспособности ИСПДн после внештатных ситуаций.

2. Целью настоящего документа является превентивная защита элементов ИСПДн от прерывания работы в случае реализации рассматриваемых угроз.

3. Задачами данной Инструкции являются:

1) определение мер защиты от прерывания;

2) определение действий восстановления в случае прерывания.

4. Действие настоящей Инструкции распространяется на всех работников, имеющих доступ к ресурсам ИСПДн (далее – пользователи ИСПДн), а также основные системы обеспечения непрерывности работы и восстановления ресурсов при возникновении внештатных ситуаций, в том числе:

1) системы жизнеобеспечения;

2) системы обеспечения отказоустойчивости;

3) системы резервного копирования и хранения данных;

4) системы контроля физического доступа.

5. Пересмотр настоящего документа осуществляется по мере необходимости.

II. ПОРЯДОК РЕАГИРОВАНИЯ НА ВНЕШТАТНЫЕ СИТУАЦИИ

6. В настоящей Инструкции под внештатной ситуацией понимается некоторое происшествие, связанное со сбоем в функционировании элементов ИСПДн, предоставляемых пользователям ИСПДн. Внештатная ситуация становится возможной в результате реализации одной из угроз, приведенных в таблице 1.

Таблица 1

№ п/п	Тип угрозы	Виды угроз
1	2	3
1.	Технологические угрозы	1) пожар в здании; 2) сбой системы кондиционирования; 3) повреждение водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения); 4) взрыв (бытовой газ, теракт, взрывчатые вещества или приборы, работающие под давлением); 5) химический выброс в атмосферу

№ п/п	Тип угрозы	Виды угроз
1	2	3
2.	Внешние угрозы	1) массовые беспорядки; 2) сбои общественного транспорта; 3) эпидемия; 4) массовое отравление персонала
3.	Стихийные бедствия	1) удар молнии; 2) сильный снегопад; 3) сильные морозы; 4) просадка грунта (подмыв грунтовых вод, подземные работы) с частичным обрушением здания; 5) затопление водой в период паводка; 6) наводнение, вызванное проливным дождем; 7) торнадо; 8) подтопление здания (воздействие подпочвенных вод, вызванное внезапным и непредвиденным повышением уровня грунтовых вод).
4.	Информационные угрозы	1) сбой в работе информационных систем; 2) несанкционированный доступ.
5.	Угроза, связанная с человеческим фактором	1) ошибка персонала, имеющего доступ к серверной; 2) нарушение конфиденциальности, целостности и доступности конфиденциальной информации.
6.	Угрозы, связанные с внешними поставщиками	1) отключение электроэнергии; 2) сбой в работе Интернет-провайдера; 3) физический разрыв внешних каналов связи.

7. При возникновении внештатных ситуаций пользователи ИСПДн немедленно оповещают ответственного за организацию защиты персональных данных (далее – ответственные за реагирование), для предпринятия срочных действий.

8. В кратчайшие сроки, не превышающие одного рабочего дня, ответственные за реагирование предпринимают меры по восстановлению работоспособности ИСПДн и ликвидации последствий внештатных ситуаций.

9. Все действия в процессе реагирования на внештатные ситуации должны документироваться ответственными за реагирование в Журнале учета внештатных ситуаций

10. При реагировании на инцидент, важно, чтобы пользователь ИСПДн правильно классифицировал критичность инцидента. Критичность оценивается на основе следующей классификации:

уровень 1 – **незначительный инцидент**. Незначительный инцидент определяется как локальное событие с ограниченным воздействием, которое не влияет на общую доступность элементов ИСПДн и средств защиты. Эти инциденты решаются ответственными за реагирование;

уровень 2 – **авария**. Любой инцидент, который приводит или может привести к прерыванию работоспособности отдельных элементов ИСПДн и средств защиты. Эти инциденты выходят за рамки разбирательства ответственными за реагирование. К авариям, которые могут привести к отказу элементов ИСПДн и средств защиты, относятся следующие инциденты:

– повреждения водой (прорыв системы водоснабжения, канализационных труб, систем охлаждения), а также подтопления в период паводка или продолжительных дождей;

– сбой системы кондиционирования;

– химический выброс в атмосферу;

– эпидемии;

– массовое отравление персонала;

– стихийные бедствия;

уровень 3 – **катастрофа**. Любой инцидент, приводящий к полному прерыванию работоспособности всех элементов ИСПДн и средств защиты, а также к угрозе жизни пользователей ИСПДн, классифицируется как катастрофа. Обычно к катастрофам относят обстоятельства непреодолимой силы, которые могут привести к неработоспособности ИСПДн и средств защиты на сутки и более. К катастрофам относятся следующие инциденты:

– пожар в здании;

– взрыв;

– просадка грунта с частичным обрушением здания;

– массовые беспорядки в непосредственной близости.

III. МЕРЫ ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ РАБОТЫ ДЛЯ ПРЕДОТВРАЩЕНИЯ ВОЗНИКНОВЕНИЯ ВНЕШТАТНЫХ СИТУАЦИЙ

11. К техническим мерам обеспечения непрерывной работы и восстановления относятся программные, аппаратные и технические средства и системы, используемые для предотвращения возникновения внештатных ситуаций, такие как:

1) Системы жизнеобеспечения. Системы жизнеобеспечения ключевых элементов ИСПДн включают:

- систему пожарной сигнализации;

- системы кондиционирования зон дислокации ключевых элементов ИСПДн;

- резервирование электроснабжения.

2) Системы обеспечения отказоустойчивости. Обеспечение отказоустойчивости ключевых элементов ИСПДн достигается подключением сервера к системе бесперебойного питания. Контроль за данными оборудованием осуществляют ответственные за реагирование в случае возникновения внештатных ситуаций.

3) Системы резервного копирования данных. Функционирование системы резервного копирования должно осуществляться согласно Положению о резервном копировании персональных данных.

4) Системы контроля физического доступа. Контроль физического доступа достигается использованием во всех помещениях расположения элементов ИСПДн системы охранной сигнализации.

12. Пользователи ИСПДн должны быть ознакомлены с настоящей Инструкцией в 3-дневный срок со дня поступления на работу начальником своего структурного подразделения.

13. Должно быть проведено обучение работников, имеющих доступ к ресурсам ИСПДн, порядку действий при возникновении внештатных ситуаций. Работники должны получить базовые знания в следующих областях:

1) оказание первой медицинской помощи;

2) пожаротушение;

3) эвакуация людей;

4) защита материальных и информационных ресурсов;

5) методы оперативной связи со службами спасения и внешними поставщиками;

6) выключение оборудования, электричества, водоснабжения, газоснабжения.

IV. ПЕРЕЧЕНЬ НАИБОЛЕЕ РАСПРОСТРАНЁННЫХ ВНЕШТАТНЫХ СИТУАЦИЙ И ДЕЙСТВИЯ ПРИ ИХ ВОЗНИКНОВЕНИИ

14. Сбой программного обеспечения. Ответственные за реагирование, выясняют причину сбоя программного обеспечения (далее – ПО). Если исправить ошибку своими силами (в том числе после консультации с разработчиками ПО) не удалось, копия акта и сопроводительных материалов (а также файлов, если это необходимо) направляются разработчику ПО.

15. Отключение электричества. Ответственные за реагирование проводят анализ на наличие потерь и (или) разрушения данных и ПО, а также проверяют работоспособность оборудования. В случае необходимости, производится восстановление ПО и данных из последней резервной копии.

16. Выход из строя сервера. Ответственные за реагирование проводят меры по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы. При необходимости производятся работы по восстановлению ПО и данных из резервных копий.

17. Потеря данных. При обнаружении потери данных ответственные за реагирование проводят мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и так далее). При необходимости производится восстановление ПО и данных из резервных копий.

18. Обнаружен вирус. При обнаружении вируса следует руководствоваться Инструкцией по организации антивирусной защиты.

19. Обнаружена утечка информации (уязвимость в системе защиты). При обнаружении утечки информации ставятся в известность ответственные за реагирование. Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищённости системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.

20. Попытка несанкционированного доступа. При попытке либо подозрении в попытке несанкционированного доступа ответственными за реагирование проводится анализ ситуации. По результатам анализа, в случае необходимости, принимаются меры по предотвращению НСД, если есть реальная угроза НСД. Также рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

21. Компрометация ключей. При компрометации ключей следует руководствоваться Инструкцией по организации и обеспечению безопасности эксплуатации шифровальных (криптографических) средств. Проводится служебное расследование.

22. Компрометация пароля. При компрометации пароля необходимо руководствоваться Инструкцией по организации парольной защиты. Проводится служебное расследование.

23. Физическое повреждение ЛВС или персональной электронной вычислительной машины (далее – ПЭВМ). Ставятся в известность ответственные за реагирование. Проводится анализ на утечку или повреждение информации. Определяется причина повреждения ЛВС или ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на

целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий.

Приложение № 10
к приказу №111-ОД от 24.08.20

Инструкция
по физической охране и контролю доступа в помещения

1. Общие положения

1.1. Данная Инструкция регламентирует условия и порядок осуществления доступа лиц в помещения со средствами информационных систем персональных данных (далее – ИСПДн) в целях обеспечения предотвращения несанкционированного доступа к сведениям, содержащим персональные данные в Муниципальном казенном учреждении социального обслуживания «Социально-реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска (далее – СРЦ). При обеспечении доступа лиц соблюдаются требования законодательства РФ по защите персональных данных.

1.2. Обеспечение доступа лиц в помещения предусматривает комплекс специальных мер, направленных на поддержание и обеспечение установленного порядка деятельности СРЦ и определяет порядок пропуска в помещения работников СРЦ и посетителей.

1.3. В помещениях исключено неконтролируемое пребывание посторонних лиц.

1.4. Контроль за порядком обеспечения доступа лиц в помещения возлагается на начальников соответствующих отделов.

2. Термины и определения

2.1. Информация - сведения (сообщения, данные) независимо от формы их представления.

2.2. Носитель информации - любой материальный объект или среда, используемый для хранения или передачи информации.

2.3. Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

2.4. Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.5. Доступ к информации – возможность получения информации и ее использования.

2.6. Несанкционированный доступ (НСД) – доступ к информации, хранящейся на различных типах носителей (бумажных, магнитных, оптических и т. д.) в компьютерных базах данных, файловых хранилищах, архивах, секретных частях и т. д. различных организаций путем изменения (повышения, фальсификации) своих прав доступа.

2.7. Автоматизированное рабочее место (АРМ) – персональный компьютер и подключенные к нему периферийные устройства – принтер, многофункциональные устройства, сканеры и т.п.

3. Порядок доступа в помещения работников и посетителей

3.1. Не допускается нахождение работников СРЦ в помещениях в

нерабочее для них время.

3.2. Нахождение посетителей СРЦ в помещениях допускается только в рабочее время.

3.3. В помещения ИСПДн пропускаются:

3.3.1. беспрепятственно – начальник СРЦ и работники, имеющие допуск к работе с персональными данными и с целью выполнения служебных (трудовых) обязанностей;

3.3.2. при наличии удостоверения, с разрешения начальника СРЦ, и сопровождении ответственного за обеспечение безопасности персональных данных или администратора безопасности – сотрудники контролирующих органов, сотрудники пожарных и аварийных служб, сотрудники полиции;

3.3.3. ограниченно – работники, не имеющие допуска к работе с персональными данными или не имеющие функциональных обязанностей в помещении, работники сторонних организаций и учреждений для выполнения договорных отношений.

3.4. Посетители пропускаются в помещения ИСПДн СРЦ в рабочее время в сопровождении работников, допущенных к обработке персональных данных.

3.5. В помещениях, в которых происходит обработка и хранение персональных данных, запрещено использование не предусмотренных служебными (трудовыми) обязанностями технических устройств, фотографирование, видеозапись, звукозапись, в том числе с использованием мобильных телефонов.

4. Организация и порядок производства ремонтно-строительных работ в помещениях

4.1. Рабочие и специалисты ремонтно-строительных организаций пропускаются в помещения для проведения ремонтно-строительных работ на основании заявок, подписанных директором СРЦ.

4.2. В целях предотвращения несанкционированного доступа к сведениям, содержащим персональные данные, работы проводятся только под контролем ответственного за обеспечение безопасности персональных данных или администратора безопасности.

5. Организация охраны и доступа в помещения

5.1. Для исключения возможности бесконтрольного проникновения в помещения и к установленному в них оборудованию посторонних лиц, двери в отсутствие штатных работников запираются на ключ. Помещения должны быть оборудованы специальными инженерными средствами, такими как усиленные двери, охранная сигнализация и т.п.

5.2. Контроль за состоянием технических средств охраны должен осуществляться не реже одного раза в квартал с отметкой в соответствующем журнале.

5.3. Работники по окончании рабочего дня обязаны убрать все документы в столы, шкафы и сейфы, закрыть окна и форточки, отключить от сети аппаратуру, радиоточки, электроприборы и освещение.

5.4. По окончании рабочего дня помещение должно закрываться на ключ.

5.5. Ключи от входных дверей должны быть пронумерованы, учтены и выданы работникам, имеющим право доступа в режимные помещения, под расписку в соответствующем журнале. Дубликаты ключей от входных дверей таких помещений хранятся в сейфе.

5.6. При утрате ключа от помещения замок заменяется или передается его секрет с изготовлением к нему новых ключей с документальным оформлением.

5.7. Если перед вскрытием помещения будут обнаружены признаки неправомерного вскрытия или проникновения, ответственный за помещение принимает меры по охране помещения, немедленно ставя в известность об этом администратора безопасности. До его прибытия помещение не вскрывается. По результатам вскрытия помещения, его осмотра и проведения при необходимости комиссионной проверки наличия ценностей и документов составляется акт, который представляется начальнику СРЦ.

5.8. Обо всех случаях неправомерного вскрытия помещения или вскрытия его в экстремальных ситуациях докладывается начальнику СРЦ.

5.9. В случае служебной необходимости вскрытия помещения в отсутствие ответственного за него лица, оно может быть вскрыто по указанию начальника СРЦ.

5.10. Оборудование в помещениях должно размещаться таким образом, чтобы исключить возможность бесконтрольного доступа к нему посторонних лиц. Мониторы компьютеров должны быть ориентированы таким образом, чтобы исключить возможность просмотра отображаемой на них информации лицами, не имеющими допуска к обработке персональных данных.

5.11. Окна помещений, в которых ведется обработка персональных данных, должны быть оборудованы шторами или жалюзи.

5.12. Режим работы охраны устанавливается штатным расписанием и должностными инструкциями.

6. Уборка помещений

6.1. Уборка помещений ИСПДн должна производиться под контролем работника, допущенного к обработке персональных данных в этом помещении.

6.2. Во время уборки в помещении должна быть приостановлена работа с персональными данными, должны быть выключены или заблокированы все АРМ, на которых обрабатываются персональные данные. Носители, содержащие персональные данные, должны быть убраны в закрытые шкафы или сейфы.

7. Требования по техническому укреплению

7.1. Необходимо обеспечить обязательное выполнение мероприятий по техническому укреплению и оборудованию специальными техническими средствами охраны, системами пожарной безопасности и руководствоваться следующими основными требованиями:

7.1.1. двери и окна должны иметь прочные и надежные петли, шпингалеты, крючки или задвижки и быть плотно подогнаны к рамам и дверным коробам. Допускается применение электромеханических, электромагнитных замков и задвижек;

7.1.2. оконные проемы первых этажей зданий должны быть укреплены металлическими решетками, запираемыми с внутренней стороны, если это не противоречит требованиям пожарной безопасности.

7.2. Конструкция оконных рам должна исключать возможность демонтажа с наружной стороны оконного проема стекол.

7.3. Стекла в рамах должны быть надежно закреплены в пазах.

7.4. Рамы указанных оконных проемов оборудуются запорными устройствами.