Муниципальное казенное учреждение социального обслуживания «Социально-реабилитационный центр для несовершеннолетних»
Ленинского района г. Челябинска
(наименование работодателя)

ПРИКАЗ

Номер	Дата
255-ОД	25.11.2022

Об организации защиты персональных данных
(название приказа)

Основание: Во исполнение требований Федерального закона от 27.06.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»
(документ, его автор (при необходимости), дата, номер, заголовок, или несколько документов)

ПРИКАЗЫВАЮ:

1. Утвердить:
- Положение об организации проведения внутреннего контроля состояния защиты персональных данных;
- Порядок доступа работников в помещения, в которых ведется обработка персональных данных;
- Инструкция пользователя информационных систем персональных данных;
- Инструкция обслуживающего персонала информационных систем персональных данных;
- Форма Акта о результатах проведения внутренних проверок состояния защиты персональных данных;
- Список помещений, где обрабатываются персональные данные и лиц, допущенных в данное помещение;
- План проведения внутренних проверок состояния защиты персональных данных;
- План мероприятий по защите персональных данных;
- Перечень мест хранения материальных носителей персональных данных.
2. Контроль за исполнением настоящего приказа оставляю за собой.

Директор (должность руководителя) _____ (личная подпись) С.Г. Богданова (ФИО)

Приложение
к приказу 255-ОД
от 25.11.2022 №

Положение
об организации проведения внутреннего контроля состояния защиты персональных данных

I. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1. Настоящий документ определяет порядок проведения проверочных мероприятий по контролю соблюдения порядка обработки и защищенности персональных данных в МКУ СО «Социально – реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска.

2. Мероприятия по проверке условий обработки персональных данных и контролю эффективности принятых мер по обеспечению безопасности конфиденциальной информации должны включать:

1) создание комиссии по контролю условий обработки персональных данных и эффективности защиты конфиденциальной информации;

2) установление порядка проведения внутренних проверок условий обработки персональных данных и состояния защиты конфиденциальной информации.

II. ПОРЯДОК КОНТРОЛЯ ЗАЩИЩЕННОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3. Ответственным за организацию проведения проверок условий обработки персональных данных и контроля эффективности защиты конфиденциальной информации является ответственный за организацию обработки персональных данных в МКУ СО «Социально – реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска.

4. Состав комиссии по контролю условий обработки персональных данных и исполнения мероприятий по защите конфиденциальной информации утверждается приказом МКУ СО «Социально – реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска.

5. В целях контроля изучения и оценки фактического состояния защищенности персональных данных, своевременного реагирования на нарушения установленного порядка их обработки, а также для совершенствования порядка обработки и обеспечения его соблюдения, в МКУ СО «Социально – реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска на регулярной основе должны проводиться контрольные мероприятия.

6. Контрольные мероприятия (проверки) проводятся на плановой основе в соответствии с Планом внутренних проверок состояния защиты персональных данных (приложение 1), а также внепланово – по фактам выявления инцидентов в области безопасности персональных данных, а также при изменениях в составе пользователей и при существенных изменениях в сфере обработки персональных данных.

7. Плановые проверки проводятся ежеквартально и включают в себя:

1) проверку системы допуска и учета лиц, допущенных к работе с конфиденциальной информацией;

2) проверку актуальности нормативно-организационных документов;

3) проверку работоспособности и эффективности технических средств информационных систем персональных данных и средств защиты персональных данных;

4) проверку ведения средств защиты информации, в том числе, криптографических;

5) проверку проведения процедуры резервного копирования защищаемой информации;

6) контроль над выполнением парольной защиты;

7) контроль над соблюдением режима обработки персональных данных;

8) проверку отсутствия на автоматизированных рабочих местах пользователей нештатного программного обеспечения;

9) контроль над выполнением антивирусной защиты;

10) организация анализа и пересмотра имеющихся угроз безопасности персональных данных, а также предсказание появления новых, еще неизвестных угроз.

11) обеспечение режима безопасности помещений информационных систем, в которых осуществляется обработка конфиденциальной информации;

12) контроль хранения и уничтожения материальных носителей конфиденциальной информации;

13) иные мероприятия.

8. План внутренних проверок состояния защиты персональных данных и конфиденциальной информации составляется ежегодно и утверждается начальником «Название учреждения» не позднее первого февраля нового отчетного года.

9. Результаты проверок оформляются актами (приложение 2). Акт составляется и подписывается председателем и членами комиссии.

10. Выявленные в ходе проверок нарушения, а также отметки об их устранении, фиксируются в Журнале учета проведения внутренних проверок состояния защиты персональных данных (приложение 3).

11. Члены комиссии, осуществляющие проверку, имеют право вносить начальнику «Название учреждения» предложения о совершенствовании правового, технического, и организационного регулирования обеспечения безопасности персональных данных при их обработке, а также предложения о привлечении к дисциплинарной ответственности лиц, виновных в нарушении действующего законодательства Российской Федерации о персональных данных.

12. Выявленные нарушения расследуются, результаты расследования направляются на имя начальника МКУ СО «Социально – реабилитационный центр для несовершеннолетних» Ленинского района города Челябинска. При необходимости принятия решений по результатам проверок готовятся соответствующие докладные записки.

Приложение к приказу
МКУ СО «СРЦ для несовершеннолетних»
Ленинского района
от 25.11.22 № 255-ОД

п4

Инструкция
обслуживающего персонала информационных систем персональных данных

1.Общие положения

Настоящая инструкция разработана в соответствии с нормативными документами по безопасности информации, и определяет порядок обеспечения информационной безопасности при проведении работ обслуживающим персоналом в информационных системах персональных данных (далее – ИСПДн) МКУ СО «СРЦ для несовершеннолетних» Ленинского района.

1.1. Субъектами доступа к ресурсам ИСПДн являются пользователи, администратор безопасности и обслуживающий персонал (работники, осуществляющие техническое обслуживание, ремонт) в соответствии с утвержденным перечнем.

1.2. Обрабатываемая в ИСПДн информация относится к сведениям, составляющим персональные данные (далее – ПДн).

1.3. Работники, осуществляющие ремонт и обслуживание компонентов ИСПДн (обслуживающий персонал) получают доступ к ресурсам ИСПДн по согласованию с администратором безопасности (далее – АБ).

1.4. Обслуживающий персонал осуществляет плановые и внеплановые мероприятия по обеспечению работоспособности основных и вспомогательных технических средств и систем (далее – ОТСС и ВТСС), входящих в состав ИСПДн.

1.5. Методическое руководство по информационной безопасности объектов вычислительной техники (далее – ОВТ) осуществляет АБ.

1.6. Обслуживающий персонал имеет право вносить предложения по изменению и дополнению данной Инструкции.

1.7. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

1.8. Право толкования положений настоящей Инструкции возлагается руководителяа МКУ СО «СРЦ для несовершеннолетних» Ленинского района.

2. Требования к обслуживающему персоналу

2.1. Обслуживающий персонал, не ознакомленный с данной Инструкцией, а также с изменениями и дополнениями к ней, к работе в ИСПДн не допускается.

2.2. Обслуживающий персонал обязан выполнять требования АБ.

2.3. Обслуживающий персонал обязан периодически (согласно утвержденному плану) производить проверку работоспособности технических средств.

2.4. Обслуживающий персонал обязан немедленно реагировать на сообщения АБ о любых неисправностях в работе ИСПДн.

2.5. Обслуживающий персонал обязан отчитаться АБ по факту выполнения работ в ИСПДн.

3. Доступ к ресурсам ИСПДн

3.1. Обязательным условием получения доступа к ресурсам ИСПДн обслуживающего персонала является знание технологии обработки информации в ИСПДн с учетом требований информационной безопасности.

3.2. Все работы выполняются в присутствии работника, имеющего право доступа к ресурсам ИСПДн.

3.3. Обслуживающий персонал не имеет права требовать у пользователей раскрытия их паролей и/или передачи персональных идентификаторов.

3.4. Обслуживающий персонал не имеет право требовать у пользователей распечатывать и/или выводить информацию на экран монитора.

3.5. Обслуживающий персонал не имеет права требовать у пользователей предоставления любых машинных носителей информации, в т.ч. во временное использование.

4. Порядок работы обслуживающего персонала

Ниже приводится перечень работ, производимых обслуживающим персоналом с ресурсами ИСПДн.

4.1. Обеспечение работоспособности ИСПДн

В соответствии с утвержденным графиком, а также по требованию АБ обслуживающий персонал проводит проверку работоспособности технических средств, используемых на ОВТ. В случае обнаружения неисправностей необходимо произвести следующие действия:

- для устранения неисправности технических средств, требующего нарушения целостности защитной наклейки, необходимо поставить в известность АБ, а в случае его отсутствия – ответственного за обеспечение безопасности персональных данных;
- при устранении неисправности съемного жесткого диска, все работы производятся в присутствии АБ;

4.2. Обеспечение работоспособности ВТСС и прочие работы

В соответствии с утвержденным графиком, а также по требованию АБ обслуживающий персонал проводит проверку работоспособности ВТСС (датчики сигнализации, соответствующие кабели и др.) и прочие работы в помещении (ремонт системы электропитания, освещения и пр.). При этом необходимо выполнять следующие требования:

- график проведения работ согласовывается с ответственным за обеспечение безопасности персональных данных;
- вне графика производится обязательная проверка в случае обнаружения неисправностей в работе ВТСС;
- при установлении неисправности ВТСС необходимо поставить в известность АБ или ответственного за обеспечение безопасности персональных данных;
- при демонтаже неисправных ВТСС присутствие АБ является обязательным;
- если для устранения неисправности демонтаж ВТСС не требуется, присутствие АБ или ответственного за обеспечение безопасности персональных данных при проведении работ также является обязательным;
- аналогично производятся прочие работы в помещениях.

5. Ответственность

Обслуживающий персонал несет персональную ответственность за:

- неразглашение сведений, ставших им известными при выполнении своих обязанностей;
- сохранность ресурсов ИСПДн, изъятых для ремонта;
- качество выполняемых работ;
- соблюдение требований данной Инструкции и правомерное использование ресурсов ИСПДн.

Приложение
к приказу о защите персональных данных

от 25.11.2022 № 255-ОД

План
мероприятий по защите персональных данных

№ п/п	Мероприятие	Срок исполнения	Исполнитель
1	Определение круга лиц, участвующих в обработке персональных данных		
2	Определение ответственности лиц, участвующих в обработке		
3	Определение прав разграничения доступа пользователей ИСПДн, необходимых для выполнения трудовых обязанностей		
4	Определение уровня защищенности персональных данных при их обработке во всех выявленных ИСПДн		
5	Анализ актуальности угроз безопасности персональных данных		
6	Выбор помещений для установки аппаратных средств ИСПДн с целью исключения несанкционированного доступа лиц, не допущенных к обработке персональных данных		
7	Разработка организационно-распорядительных документов по защите персональных данных		
8	Контроль за сбором согласий на обработку персональных данных		
9	Организация информирования и обучения работников о порядке обработки персональных данных		
10	Организация информирования и обучения работников о введенном режиме защиты персональных данных		

11	Закупка средств защиты информации		
12	Установка и настройка средств защиты информации		
13	Подтверждение выполнения предъявленных к ИСПДн требований по защите информации		

а10

Приложение

к Положению об организации проведения внутреннего контроля состояния защиты персональных данных
от 25.11.22 № 255-ОД

План
проведения внутренних проверок состояния защиты персональных данных

№ п/п	Наименование мероприятия	Периодичность	Ответственный исполнитель	Отметка об исполнении
1	2	3	4	5
1.	Проверка системы допуска и учета лиц, допущенных к работе со средствами криптографической защиты информации	Ежеквартально		
2.	Проверка ведения резервного копирования	Ежеквартально		
3.	Контроль за проведением антивирусной защиты	Ежеквартально		
4.	Проверка соблюдения прав доступа пользователей к информационным системам персональных данных	Ежеквартально		
5.	Проверка ведения средств защиты информации, в том числе криптографических, а также хранения и уничтожения материальных носителей конфиденциальной информации	Ежеквартально		
6.	Проверка отсутствия на автоматизированных рабочих местах	Ежеквартально		

	пользователей нештатного программного обеспечения			
7.	Проверка актуальности нормативно-организационных документов	Ежеквартально		
8.	Контроль за выполнением парольной защиты	Ежеквартально		
9.	Контроль над соблюдением режима обработки персональных данных	Ежеквартально		
10.	Контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах информационных систем персональных данных	Ежеквартально		
11.	Контроль за соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена	Ежеквартально		
12.	Организация анализа и пересмотра моделей угроз безопасности информационных систем персональных данных	Ежегодно		
13.	Контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты	Ежеквартально		

	информации и принятие мер, направленных на устранение выявленных недостатков			

Приложение
к приказу МКУ СО «СРЦ для несовершеннолетних»
Ленинского района
от 25.11.22 № 255-ОД

Порядок
доступа работников в помещения, в которых ведется обработка персональных данных

1. Порядок доступа работников МКУ СО «СРЦ для несовершеннолетних» Ленинского района в помещения, в которых ведется обработка персональных данных и организацию безопасности этих помещений (далее - Порядок), разработан в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», постановлениями Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации».

2. Ответственность за режим безопасности в помещении, в котором ведется обработка персональных данных и правильность использования установленных в нем технических средств несет должностное лицо, которое постоянно в нем работает, или лицо, специально на то уполномоченное.

3. В нерабочее время помещение должно закрываться на ключ и опечатываться ответственным лицом.

4. В рабочее время, в случае ухода ответственного лица, помещение должно закрываться на ключ или оставляться под ответственность уполномоченного лица.

6. В помещения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только работники МКУ СО «СРЦ для несовершеннолетних» Ленинского района, уполномоченные на обработку персональных данных.

7. Нахождение лиц, не являющихся уполномоченными лицами на обработку персональных данных, в помещениях, возможно только в сопровождении ответственного или уполномоченного лица на время, ограниченное необходимостью решения вопросов, связанных с исполнением должностных обязанностей и (или) осуществлением полномочий в рамках договоров, заключенных с МКУ СО «СРЦ для несовершеннолетних» Ленинского района.

8. При обработке персональных данных и хранении материальных носителей персональных данных должны соблюдаться условия, при которых обеспечивается сохранность носителей персональных данных и средств защиты информации и исключающие несанкционированный доступ к ним, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

9. Повседневный контроль за выполнением требований по защите помещения осуществляют лица, ответственные за помещение.

10. Периодический контроль эффективности мер защиты помещения осуществляется ответственным за организацию обработки персональных данных.

Приложение
к приказу
от 25.11.2022 № 255-ОД

п 6

Список
Помещений, где обрабатываются персональные данные и лиц, допущенных в данные помещения

Наименование помещения	ФИО работников, имеющих право доступа	ФИО работника, ответственного за помещение	Назначение помещения
Каб. ОПСС	Кузнецова К.Е. Некрасова О.В. Говорухина К.А. Теньковская А.Ф.	Когосова А.В.	Обработка данных ИСПДн «VipNet»
Каб. ОСПП	Калисов А.А.	Шабаров Е.В	Обработка данных ИСПДн «VipNet»
Каб. Бухгалтерия	Хабибулина Д.Г.	Студеникина Е.В.	Обработка данных ИСПДн «Сбербанк»

Приложение к приказу
от 25.11.22 № 255-ОД

Инструкция
пользователя информационных систем персональных данных

1. Общие положения

1. Настоящая инструкция определяет порядок деятельности работников МКУ СО «СРЦ для несовершеннолетних» Ленинского района, участвующих в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющих доступ к аппаратным средствам, программному обеспечению и данным информационных систем персональных данных «МКУ СО «СРЦ для несовершеннолетних» Ленинского района.

2. Изменения и дополнения к данной Инструкции утверждаются в установленном порядке.

2. Термины и определения

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

4. База данных – это информация, упорядоченная в виде набора элементов, записей одинаковой структуры.

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

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

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

8. 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.

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

10. 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.

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

12. Персональные данные (далее – ПДн) – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

13. Пользователь ИСПДн – работник «Название организации», участвующий в рамках своих функциональных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн МКУ СО «СРЦ для несовершеннолетних» Ленинского района.

14. Программное обеспечение – все или часть программ, процедур, правил и соответствующей документации системы обработки информации.

15. Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц.

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

3. Права пользователей ИСПДн

17. Пользователи ИСПДн имеют следующие права:

1) пользоваться вверенными программными и аппаратными ресурсами для работы с персональными данными в ИСПДн с целью исполнения трудовых функций;

2) вносить предложения по изменению и дополнению данной Инструкции.

3) обращаться к ответственному за обеспечение безопасности персональных данных получения консультаций по вопросам информационной безопасности и исполнения требований данной Инструкции;

4. Обязанности пользователей ИСПДн

18. Каждый пользователь ИСПДн несет персональную ответственность за свои действия и обязан:

1) знать и соблюдать установленные требования к обработке ПДн, учету и хранению носителей информации, обеспечению безопасности ПДн, а также руководящих и организационно-распорядительных документов.

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

3) знать и строго выполнять правила работы со средствами защиты информации, установленными на его автоматизированном рабочем месте;

4) хранить в тайне свой пароль (пароли), соблюдать правила работы с паролями, установленные «Инструкции по организации парольной защиты»;

5) выполнять требования «Инструкции по организации антивирусной защиты персональных данных при их обработке в информационных системах персональных данных «Название организации» в части, касающейся действий пользователей АРМ ИСПДн;

6) самовольно вносить какие-либо изменения в конфигурацию АРМ или устанавливать в АРМ любые программные и аппаратные средства, кроме выданных или разрешённых к использованию ответственным за обеспечение безопасности персональных данных;

7) немедленно вызывать ответственного за обеспечение безопасности персональных данных и ставить в известность начальника своего структурного подразделения при обнаружении:

- нарушений, связанных с информационной безопасностью;
- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах АРМ или иных фактов совершения в его отсутствие попыток несанкционированного доступа (далее – НСД) к защищаемой АРМ;
- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств АРМ;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию АРМ, выхода из строя или неустойчивого функционирования узлов АРМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на АРМ технических средств защиты;
- непредусмотренных отводов кабелей и подключенных к АРМ дополнительных устройств;
- утери или подозрении на утечку пароля и персональных идентификаторов.

8) принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий в пределах возложенных на него функций;

9) заблокировать доступ к АРМ при отсутствии визуального контроля за рабочей станцией.

4. Ограничения и запреты

19. Пользователям ИСПДн запрещается:

1) разглашать защищаемую информацию посторонним лицам;

2) копировать защищаемую информацию на неучтенные внешние носители;

3) самостоятельно устанавливать, тиражировать или модифицировать программное и аппаратное обеспечение, изменять установленный порядок функционирования технических и программных средств, а также или устанавливать дополнительно любые программные и аппаратные средства

4) подключать к АРМ и корпоративной информационной сети личные внешние носители и мобильные устройства без согласования с ответственным за обеспечение безопасности персональных данных;

5) отключать (блокировать) средства защиты информации;

6) сообщать (или передавать) посторонним лицам параметры своей учетной записи (имя, персональный идентификатор (при его наличии) и пароль) в ИСПДн;

7) привлекать посторонних лиц для ремонта или настройки АРМ без согласования с ответственным за обеспечение безопасности персональных данных;

8) использовать компоненты программного и аппаратного обеспечения ИСПДн, а также сведения, содержащиеся в электронных документах и базах данных, в неслужебных целях;

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

10) записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных носителях информации;

11) оставлять включенной без присмотра свое АРМ, не активизировав средства защиты от НСД (временную блокировку экрана и клавиатуры);

12) умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках СЗИ, которые могут привести к возникновению кризисной ситуации. При обнаружении такого рода ошибок ставить в известность ответственного за обеспечение безопасности персональных данных и начальника структурного подразделения;

13) использовать для копирования информации непроверенные на наличие компьютерных вирусов и других вредоносных программ носители информации;

14) использовать при работе в АРМ вредоносные программы, ведущие к блокированию работы сети;

15) самовольно изменять сетевые адреса;

16) передавать АРМ из одного структурного подразделения в другое без согласования с ответственным за обеспечение безопасности;

5. Ответственность пользователей ИСПДн

20. Каждый пользователь ИСПДн несёт персональную ответственность за соблюдение требований настоящей Инструкции и за все действия, совершенные от имени его учётной записи в ИСПДн, если с его стороны не было предпринято необходимых действий для предотвращения несанкционированного использования его учётной записи.

21. За разглашение персональных данных и нарушение порядка работы со средствами ИСПДн, содержащими персональные данные, работники МКУ СО «СРЦ для несовершеннолетних» Ленинского района могут быть привлечены к гражданской, уголовной, административной, дисциплинарной и иной предусмотренной законодательством Российской Федерации ответственности.

Приложение 2 №11

к Положению об организации проведения внутреннего контроля состояния защиты персональных данных «МКУ СО «СРЦ для несовершеннолетних» Ленинского района
от 25.11.22 № 255-ОД

Форма
акта о результатах проведения внутренних проверок состояния защиты персональных данных

Акт от _____ № _____

О результатах проведения внутренних проверок состояния защиты персональных данных

Комиссия в составе:

Роль	ФИО	Должность
Председатель		
Члены комиссии		

произвела в «___» квартале 20___ года внутренние проверки состояния защиты персональных данных, обрабатываемых в информационных системах персональных данных «Название учреждения», результаты которых оформлены в таблице:

№ п/п	Наименование мероприятия	Описание нарушений	Отметка об устранении нарушений
1	2	3	4
1.	Проверка системы допуска и учета лиц, допущенных к работе со средствами криптографической защиты информации		
2.	Проверка ведения резервного копирования баз данных управления		
3.	Контроль за проведением антивирусной защиты		
4.	Проверка соблюдения прав доступа пользователей к информационным системам персональных данных		
5.	Проверка ведения средств защиты информации, а также хранения и уничтожения материальных носителей конфиденциальной информации		

6.	Проверка отсутствия на автоматизированных рабочих местах пользователей нештатного программного обеспечения		
7.	Проверка актуальности нормативно-организационных документов		
8.	Контроль за выполнением парольной защиты		
9.	Контроль за обновлениями программного обеспечения и единообразия применяемого программного обеспечения на всех элементах информационных систем персональных данных		
10.	Контроль за соблюдением режима защиты при подключении к сетям общего пользования и (или) международного обмена		

_____/_____/_____/
(должность, Ф.И.О. председателя комиссии) (подпись) (дата)

_____/_____/_____/
(должность, Ф.И.О. члена комиссии) (подпись) (дата)

_____/_____/_____/
(должность, Ф.И.О. члена комиссии) (подпись) (дата)

_____/_____/_____/
(должность, Ф.И.О. члена комиссии) (подпись) (дата)

Приложение к приказу
от 25.11.22 № 255-ОД

Перечень мест хранения материальных носителей персональных данных

Таблица 1

Список мест хранения материальных носителей персональных данных отдела _____

№ п/п	Носитель персональных данных	Место хранения	Примечание
1	2	3	4
1.			

Список мест хранения материальных носителей персональных данных отдела _____

№ п/п	Носитель персональных данных	Место хранения	Примечание
1	2	3	4
1.			

Таблица 2

Список мест хранения материальных носителей персональных данных отдела бухгалтерского учета

№ п/п	Носитель персональных данных	Место хранения	Примечание
1.			