Приложение № 6
к приказу директора
от 01.06.25 № 1160

ПОЛОЖЕНИЕ
ОБ ОРГАНИЗАЦИИ РЕЖИМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПОМЕЩЕНИЙ, ГДЕ ОСУЩЕСТВЛЯЕТСЯ РАБОТА С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящее Положение определяет порядок доступа и правила охраны (обеспечения безопасности) помещений, в которых обрабатываются персональные данные (ПДн) без использования средств автоматизации и в информационных системах персональных данных (ИСПДн) областного бюджетного учреждения «Центр социальной защиты населения Липецкой области» (далее - Учреждение).

2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПОМЕЩЕНИЙ ОБРАБОТКИ ПДН

2.1. Целью Учреждения при организации режима обеспечения безопасности в помещениях обработки ПДн является обеспечение конфиденциальности ПДн, сохранности носителей ПДн и средств защиты информации (СЗИ), обеспечивающих техническую защиту ПДн. Правила обеспечения безопасности помещений также должны исключать возможность неконтролируемого проникновения или пребывания в помещениях обработки ПДн посторонних лиц.

2.2. Запрещается нахождение в помещениях, где ведется обработка ПДн, посторонних лиц, не имеющих полномочий по доступу в данное помещение, при отсутствии в данном помещении лиц, состоящих в списке лиц, допущенных в помещение.

2.3. В рабочее время, в случае ухода всех сотрудников, или в нерабочее время помещения, где производится обработка ПДн, должны закрываться на ключ.

2.4. В ночное время коридоры Учреждения, где расположены подразделения, участвующие в процессах обработки персональных данных, должны закрываться специальными металлическими решетками. Ключи от специальных металлических решеток сдаются под охрану сторожу.

2.5. Должны выполняться все предписания на эксплуатацию средств защиты информации, связи, вычислительной техники, оргтехники, бытовых приборов и др. оборудования, установленного в помещении, где происходит обработка ПДн.

2.6. Уборка помещений должна производиться под контролем сотрудника, имеющего доступ в помещение и постоянно в нем работающего.

2.7. Выносить технические средства обработки ПДн (непосредственно содержащие базы персональных данных) за пределы контролируемой зоны Учреждения с целью их ремонта, замены и т. п. без согласования с руководителем подразделения запрещено. При принятии решения о выносе компьютеров, жесткие магнитные диски должны быть демонтированы и сданы на хранение ответственному за учет служебных документов ограниченного распространения структурного подразделения. В случае действия гарантийных обязательств фирмы-поставщика вскрытие корпуса и демонтаж носителей должны быть предварительно согласованы с ней.

2.8. Мониторы технических средств обработки ПДн должны быть размещены таким образом, чтобы исключалась возможность случайного или преднамеренного визуального просмотра отображаемой на них информации посторонними лицами.

3. ОТВЕТСТВЕННОСТЬ ЗА РЕЖИМ БЕЗОПАСНОСТИ

3.1. Ответственность за режим безопасности в помещениях обработки ПДн отдела (подразделения) и правильность использования установленных в нем технических средств, в том числе средств защиты информации, несет руководитель данного подразделения.

3.2. Установка нового оборудования, мебели и т.п. или замена их, а также ремонт помещения должны проводиться только по согласованию с ответственным за обработку и обеспечение безопасности персональных данных в Учреждении.