

УТВЕРЖДАЮ

Директор ГБУ СО ЯО

Дом социального
обслуживания «Забота»



М.В.Филиппова

2026 г.

ПРАВИЛА

работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей в государственном учреждении социального обслуживания Ярославской области Дом социального обслуживания «Забота»

1. Правила работы лиц, доступ которых к персональным данным, в том числе обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей в государственном учреждении социального обслуживания Ярославской области Дом социального обслуживания «Забота» (далее – Правила) определяют порядок работы лиц, доступ которых к персональным данным, в том числе, обрабатываемым в информационных системах персональных данных, необходим для выполнения ими служебных (трудовых) обязанностей в государственном учреждении социального обслуживания Ярославской области Дом социального обслуживания «Забота» (далее – Учреждение).

2. Настоящие Правила разработаны в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), Федеральным законом от 02.05.2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Постановлением Правительства Российской Федерации от 21.03.2012 г. № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ними нормативными правовыми актами в сфере защиты персональных данных.

3. Допуск для работы на автоматизированных рабочих местах (далее – АРМ), состоящих в составе информационной системы персональных данных (далее – ИСПДн) осуществляется на основании утвержденного перечня лиц, доступ которых к персональным данным (далее – ПДн), в том

числе обрабатываемых в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей (далее – Пользователи ИСПДн).

4. Пользователь ИСПДн имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения и записи информации, содержащей ПДн, разрешается использовать только машинные носители, учтенные в журнале учета машинных носителей информации, использующихся в ИСПДн для обработки, хранения и транспортировки информации.

5. Пользователь несет ответственность за правильность включения и выключения АРМ, входа и выхода в систему и за все свои действия при работе с ИСПДн.

6. Вход пользователя в систему осуществляется по выданному ему электронному идентификатору и по персональному паролю.

7. При работе со съемными машинными носителями информации пользователь каждый раз перед началом работы обязан проверить их на отсутствие вирусов и иных вредоносных программ с использованием штатных антивирусных средств, установленных на АРМ. В случае обнаружения вирусов либо вредоносных программ пользователь ИСПДн обязан немедленно прекратить их использование и действовать в соответствии с требованиями инструкции по организации антивирусной защиты.

8. Каждый работник, участвующий в рамках своих служебных обязанностей в процессе обработки персональных данных в ИСПДн и имеющий доступ к АРМ, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- Строго соблюдать установленные соответствующими инструкциями правила обеспечения безопасности информации в ИСПДн;
- Знать и строго выполнять правила работы со средствами защиты информации, установленными на АРМ;
- Хранить в тайне свой пароль (пароли). Выполнять требования инструкции по организации парольной защиты в полном объеме;
- Хранить индивидуальное устройство идентификации (ключ) и другие реквизиты в сейфе (металлическом шкафу);
- Выполнять требования инструкции по организации антивирусной защиты в полном объеме;
- Немедленно известить ответственного за обеспечение безопасности персональных данных в случае утери электронного идентификатора или при подозрении компрометации личных ключей и паролей, а также при обнаружении:
 - несанкционированных изменений в конфигурации АРМ;
 - отклонений в нормальной работе системных и прикладных

программных средств, затрудняющих эксплуатацию АРМ, выхода их строя или неустойчивого функционирования компонентов АРМ, а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на АРМ технических средств защиты;

- непредусмотренных отводов кабелей и подключенных устройств.

9. Пользователю АРМ категорически запрещается:

- Использовать компоненты программного и аппаратного обеспечения АРМ в личных целях;

- Самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные или аппаратные средства, не предусмотренные архивом дистрибутивов установленного программного обеспечения АРМ;

- Записывать и хранить конфиденциальную информацию на неучтённых машинных носителях информации;

- Оставлять включенным без присмотра АРМ, не активизировав средства защиты от НСД;

- Оставлять без личного присмотра на рабочем месте или в ином месте свой электронный идентификатор, машинные носители и распечатки, содержащие персональные данные;

- Умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты.