

УТВЕРЖДАЮ

Директор ГБУ СО ЯО

Дом социального
обслуживания «Забота»



М.В.Филиппова

2026 г.

ИНСТРУКЦИЯ

**по работе с инцидентами информационной безопасности
в государственном учреждении социального обслуживания Ярославской
области Дом социального обслуживания «Забота»**

1. Ответственность за выявления инцидентов информационной безопасности и реагирование на них в государственном учреждении социального обслуживания Ярославской области Дом социального обслуживания «Забота» (далее – Учреждение) возлагается на ответственного за обеспечение безопасности персональных данных в информационных системах персональных данных (далее – ИСПДн).

2. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных имеет полномочия инициировать проведение служебных проверок по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации.

3. Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных обязан вести журнал учета инцидентов информационной безопасности (событий, действий, повлекших за собой риски безопасности защищаемой информации и создающих предпосылки к нарушению критериев безопасности информации). К ним относятся нарушения пользователями положений организационно-распорядительных документов, установленных порядков и технологии работы в информационных системах, разглашение защищаемой информации и любые действия, направленные на это, не антропогенные инциденты (сбои программного обеспечения, стихийные бедствия).

4. В журнале в свободной форме описывается инцидент с указанием следующих данных:

- дату и времени;
- причины и описание инцидента и задействованных лиц;

- информацию о последствиях;
- информацию о возможных последствиях.

5. Журнал с данным отчетом об инциденте предоставляется на ознакомление ответственному за организацию обработки персональных данных для принятия мер по предотвращению рецидива (возникновения повторного инцидента).

6. В случае возникновения рецидива со стороны пользователя информационных систем персональных данных по ходатайству ответственного за организацию обработки персональных данных руководителем учреждения накладывается дисциплинарное взыскание.

7. Соккрытие нарушений и инцидентов информационной безопасности, вызванных любыми должностными лицами учреждения, является грубым нарушением трудовой дисциплины.

8. Любой сотрудник должен согласовывать следующие действия с администратором информационной безопасности: замена прикладного оборудования, установка дополнительного программного обеспечения, изменение сетевых настроек рабочего места, замена (изменение) любой аппаратной части рабочего места.