

**Правила
осуществления внутреннего контроля соответствия обработки
персональных данных (ПДн) требованиям к защите ПДн
в ГБУ КЦСОН Дубровского района**

1. Общие положения

1.1. Настоящие правила осуществления внутреннего контроля режима обработки и защиты ПДн (далее - Правила) в ГБУ КЦСОН Дубровского района (далее - Учреждение) направлены на определение оснований и порядка проведения внутреннего контроля соответствия обработки и защиты ПДн в целях предотвращения и устранения нарушений законодательства Российской Федерации, локальных правовых актов в сфере ПДн (далее - ПДн) в Учреждении.

1.2. Пользователями информационных систем ПДн (далее - Пользователи) являются сотрудники Учреждения, участвующие в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки ПДн.

2. Организация внутреннего контроля (проверок)

2.1. Проверки соответствия обработки ПДн установленным требованиям в Учреждении разделяются на следующие виды: плановые и внеплановые.

2.2. Плановые проверки проводятся комиссией, создаваемой нормативным актом Учреждения, в соответствии с ежегодно утверждаемым Планом внутренних проверок режима обработки и защиты ПДн (далее - План) и направлены на:

проверку выполнения требований действующего законодательства Российской Федерации и организационно-распорядительной документации Учреждения в области обработки и защиты ПДн;

оценку уровня осведомленности и знаний работников Учреждения в области обработки и защиты ПДн;

оценку обоснованности и эффективности применяемых мер и средств защиты ПДн.

2.3. План разрабатывается ответственным за организацию обработки ПДн и утверждается локальным актом учреждения. В плане указываются виды проводимых проверок и сроки их проведения.

2.4. Внеплановые контрольные мероприятия проводятся на основании распоряжения ответственного за организацию обработки ПДн в Учреждении. Решение о проведении внепланового контрольного мероприятия может быть принято в следующих случаях:

2.4.1. По результатам расследования инцидента информационной безопасности.

2.4.2. По результатам внешних контрольных мероприятий, проводимых регулируемыми органами.

2.4.3. По решению директора Учреждения.

3. Порядок проведения контрольных мероприятий

3.1. Проведение плановых внутренних контрольных мероприятий (проверок) осуществляется Комиссией строго в соответствии с Планом.

3.2. Общий срок контрольных мероприятий не должен превышать пяти рабочих дней. При необходимости срок проведения контрольных мероприятий может быть продлен, но не более чем на десять рабочих дней.

3.3. Плановые и внеплановые контрольные мероприятия (проверки) проводятся Комиссией при обязательном участии лица, ответственного за обеспечение безопасности ПДн. Также, по его ходатайству к проведению контрольных мероприятий (проверок) могут привлекаться другие сотрудники, ответственные за отдельные вопросы обеспечения безопасности ПДн в ИСПДн Учреждения.

3.4. Лицо, ответственное за обеспечение безопасности ПДн, не позднее чем за три рабочих дня до начала проведения контрольных мероприятий уведомляет руководителей подразделений, в которых планируется проведение контрольных мероприятий о сроках проведения проверки.

3.5. При проведении внеплановых контрольных мероприятий уведомление не требуется.

3.6. По результатам проведения Комиссия разрабатывает и подписывает «Акт о результатах проведения внутренней проверки режима обработки и защиты ПДн» (далее - Акт).

3.7. В Акте указывается:

- основания для проведения проверки;
- сроки и место проведения;
- выполненные виды проверок;
- результаты проведения проверки (наличие или отсутствие нарушений, наличие недостатков в работе);
- в случае необходимости указывается перечень мероприятий и задач, которые необходимо выполнить для устранения выявленных нарушений, недостатков и сроки их выполнения.

3.8. Ответственный за организацию обработки ПДн в течение пяти рабочих дней после завершения проверки направляет директору Учреждения подписанный Акт для ознакомления.