

**ОБ ОСУЩЕСТВЛЕНИИ ВНУТРЕННЕГО
КОНТРОЛЯ СООТВЕТСТВИЯ
ОБРАБОТКИ ПЕРСОНАЛЬНЫХ
ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ
ПЕРСОНАЛЬНЫХ ДАННЫХ И О
ВНУТРЕННИХ ПРОВЕРКАХ РЕЖИМА
ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ
В ГКУСО «ЦЕНТР СОЦИАЛЬНОГО
ОБСЛУЖИВАНИЯ СЕБЕЖСКОГО
РАЙОНА»**

Главное государственное
управление социальной защиты населения
Псковской области

Государственное казенное учреждение
социального обслуживания
Псковской области
**«Центр социального обслуживания
Себежского района»**

ПРИКАЗ

17.07.2019 № 180-од

г. Себеж

Об осуществлении
внутреннего контроля
по защите персональных данных

В целях повышения эффективности защиты персональных данных в ГКУСО «Центр социального обслуживания Себежского района», руководствуясь ст. 16 Федерального закона от 06.10.2003 N 131-ФЗ "Об общих принципах организации местного самоуправления в Российской Федерации", Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 21.03.2012 N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными актами, операторами, являющимися государственными или муниципальными органами", ст.ст. 37, 38, 42 Устава учреждения,

ПРИКАЗЫВАЮ:

1. Утвердить Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в учреждении. (Приложение №1)
2. Разработать План внутренних проверок режима защиты персональных данных в учреждении (Приложение №2).
3. Контроль за исполнением настоящего распоряжения возложить на Назарову В.Ф., заместителя директора, и Дашкову И.В., заместителя директора.

Директор учреждения



А.П.Михайлова

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ К ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГКУСО «ЦЕНТР СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ СЕБЕЖСКОГО РАЙОНА»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных в учреждении (далее - Правила) определяют порядок осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных, установленным действующим законодательством, в том числе Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", принятыми в соответствии с ним нормативными правовыми актами.

1.2. Правила разработаны с учетом требований Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", постановления Правительства Российской Федерации от 21.03.2011 N 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", иных нормативных правовых актов.

2. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ВНУТРЕННЕГО КОНТРОЛЯ СООТВЕТСТВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ ТРЕБОВАНИЯМ ЗАКОНОДАТЕЛЬСТВА

2.1. Цель проведения внутреннего контроля состоит в проверке и оценке соответствия обеспечения безопасности персональных данных (далее - ПДн) требованиям действующего законодательства, в том числе Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", политики в отношении обработки ПДн, правовых актов учреждения, регулирующих

работу с ПДн в структурных подразделениях.

2.2. При проведении контроля используются процедуры документальной проверки, опрос и интервью с руководителями и специалистами учреждения. При необходимости уточнения результатов документальной проверки, опросов и интервью в рамках внутреннего контроля в качестве дополнительного способа может применяться "проверка на месте", которая проводится для обеспечения уверенности в том, что конкретные защитные меры реализуются, правильно используются и проверяются с помощью тестирования.

2.3. При проведении внутреннего контроля должно быть обеспечено документальное и, если это необходимо, техническое подтверждение того, что:

- политика в отношении обработки ПДн соответствует требованиям законодательства Российской Федерации;
- организационная структура обеспечения безопасности ПДн создана;
- процессы выполнения требований безопасности ПДн исполняются и удовлетворяют поставленным целям;
- защитные меры (межсетевые экраны, средства защиты информации от несанкционированного доступа и т.п.) настроены и используются правильно;
- остаточные риски безопасности ПДн оценены и остаются приемлемыми;
- рекомендации предшествующих проверок реализованы.

2.4. При проведении внутреннего контроля могут использоваться журналы средств защиты информации для выявления попыток несанкционированного доступа к защищаемым ресурсам, а также журнал учета нештатных ситуаций информационных систем персональных данных (далее - ИСПДн), ведущийся администратором безопасности.

ПЛАН ВНУТРЕННИХ ПРОВЕРОК РЕЖИМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГКУСО «ЦЕНТР СОЦИАЛЬНОГО ОБСЛУЖИВАНИЯ СЕБЕЖСКОГО РАЙОНА»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. План внутренних проверок режима защиты персональных данных в учреждении (далее - План) содержит перечень мероприятий (внутренних проверок) по проверке режима защиты персональных данных в ГКУСО «Центр социального обслуживания Себежского района».

1.2. План содержит следующую информацию:

- название проводимого мероприятия;
- периодичность проведения;
- исполнитель мероприятия.

1.3. План распространяется на все структурные подразделения учреждения, в которых осуществляется обработка персональных данных либо имеется доступ к персональным данным.

Руководители структурных подразделений учреждения доводят до сведения работников, назначенных ответственными за организацию обработки персональных данных в соответствующем структурном подразделении учреждения, настоящий План под роспись.

2. МЕРОПРИЯТИЯ ПО ПРОВЕРКЕ РЕЖИМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Мероприятия по проверке режима защиты персональных данных имеют следующую периодичность:

- ежедневные мероприятия - мероприятия, предусматривающие постоянный контроль за выполнением требований действующего законодательства

ответственным за организацию обработки персональных данных в соответствующем структурном подразделении учреждения (далее - ответственный исполнитель) и незамедлительное реагирование на инциденты информационной безопасности;

- еженедельные и ежемесячные мероприятия - мероприятия, предусматривающие проведение мероприятий ответственными исполнителями в один и тот же день недели или месяца. Факт проведения мероприятия должен быть зафиксирован в журнале, указанном в разделе 3 настоящего Плана;

- ежегодные или проводимые раз в несколько лет - мероприятия, предусматривающие проведение мероприятий в четко определенные ответственными исполнителями периоды времени. В ходе мероприятий должны быть учтены результаты проводимых ранее мероприятий по проверке режима защиты персональных данных в данном периоде.

3. ЖУРНАЛ УЧЕТА МЕРОПРИЯТИЙ ПО КОНТРОЛЮ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Информация о периодически проводимых мероприятиях и их результатах фиксируется в журнале учета мероприятий по контролю за соблюдением режима защиты персональных данных (далее - Журнал). Форма Журнала представлена в Приложении N 1 к настоящему Плану.

В Журнале отмечаются мероприятия в соответствии с Планом, носящие периодический характер.

В Журнал заносится следующая информация:

- название проведенного мероприятия;
- дата проведенного мероприятия;
- исполнитель мероприятия;
- результат (отчет, действия) мероприятия (при необходимости).