

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных
в областном государственном бюджетном учреждении
«Центр социальной адаптации г. Томска»

1. В областном государственном бюджетном учреждении «Центр социальной адаптации г. Томска» (далее – ОГБУ «ЦСА г. Томска») назначается лицо, ответственное за организацию обработки персональных данных (далее - ПДн).

2. Деятельность ответственного лица за организацию обработки ПДн в ОГБУ «ЦСА г. Томска» регламентируется федеральными законами и иными нормативными правовыми актами в области защиты ПДн, актами Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности, нормативными правовыми актами по эксплуатации средств защиты информации, а также правовыми актами Департамента социальной защиты населения Томской области.

3. Ответственное лицо обязано:

3.1. Знать и выполнять требования действующих нормативных правовых актов в области защиты ПДн, а также внутренних инструкций, распоряжений, регламентирующих порядок действий при обработке ПДн и их защите.

3.2. Организовывать работу руководителей структурных подразделений ОГБУ «ЦСА г. Томска» по выполнению подчиненными работниками установленных требований к обработке ПДн и их защите.

3.3. На лицо, ответственное за организацию обработки персональных данных возлагается обязанность организации решения следующих вопросов:

- установка и настройка средств защиты, контрольные и тестовые испытания и проверки элементов информационных систем персональных данных (далее - ИСПДн), ведение их учета;

- приемка новых программных средств;

- обеспечение доступа к защищаемым ПДн пользователям ИСПДн согласно их правам, в соответствии с матрицей доступа;

- уточнение в установленном порядке обязанностей пользователей ИСПДн при обработке объектов защиты;

- ведение контроля над процессом осуществления резервного копирования объектов защиты;

- анализ состояния защиты ИСПДн и их отдельных подсистем;

- контроль неизменности состояния средств защиты, их параметров и режимов защиты;

- контроль физической сохранности средств и оборудования ИСПДн;

- контроль исполнения пользователями ИСПДн введенного режима безопасности, а также правильности работы с элементами ИСПДн и средствами защиты;

- осуществлять внутренний контроль за соблюдением учреждением и его работниками законодательства РФ о ПДн, в т.ч. требований к защите ПДн;

- доведение до сведения работников учреждения положений законодательства РФ о ПДн, требований к защите ПДн;

- организация приема и обработки обращений и запросов субъектов ПДн или их представителей и (или) осуществление контроля за приемом и обработкой таких обращений и запросов;

- контроль исполнения пользователями парольной политики;

- контроль работы пользователей в сетях общего пользования и (или) международного обмена;

- своевременный анализ журнала учета событий, регистрируемых средствами защиты, с целью выявления возможных нарушений;

- недопущение установки, использования, хранения и размножения в ИСПДн программных средств, не связанных с выполнением функциональных задач;

- недопущение к работе на элементах ИСПДн посторонних лиц;

- осуществление периодических контрольных проверок рабочих станций и тестирование правильности функционирования средств защиты ИСПДн;

- оказание помощи пользователям ИСПДн в части применения средств защиты и консультирование по вопросам введенного режима защиты;

- в случае отказа работоспособности технических средств и программного обеспечения ИСПДн, в том числе средств защиты, прием необходимых мер по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности;

- прием необходимых мер по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций с целью ликвидации их последствий.

3.4. В установленные сроки и по запросу вышестоящих организаций, ответственный за организацию обработки персональных данных, предоставляет отчет о состоянии защиты ИСПДн, о внештатных ситуациях на объектах ИСПДн и допущенных пользователями нарушениях установленных требований по защите информации для выработки необходимых решений;

4. Ответственное лицо имеет право:

4.1. На прохождение обучения в учебных центрах и курсах повышения квалификации по вопросам обработки ПДн и их защиты.

4.2. Ставить вопросы о наказании отдельных работников, имеющих санкционированный доступ к ПДн, допустивших серьезные нарушения в обеспечении безопасности ПДн.