

Департамент социальной защиты населения администрации Владимирской области

**Государственное казенное учреждение социального обслуживания
Владимирской области
«Гусь-Хрустальный социально-реабилитационный центр для несовершеннолетних»**

П Р И К А З

27.10.2017

№ 123

*Об утверждении Порядка доступа
сотрудников ГКУСО ВО
«Гусь-Хрустальный социально-реабилитационный
центр для несовершеннолетних» в помещения,
в которых ведется обработка
персональных данных*

В соответствии с постановлением Правительства Российской Федерации от 21.03.2012 № 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», п р и к а з ы в а ю:

1. Утвердить с 27.10.2017 года:

- Порядок доступа сотрудников государственного казенного учреждения социального обслуживания Владимирской области «Гусь-Хрустальный социально-реабилитационный центр для несовершеннолетних» в помещения, в которых ведется обработка персональных данных (Приложение №1);

- журнал учета ключей от охраняемых помещений (Приложение № 2).

2. Администратору информационной безопасности:

- разместить настоящий приказ на официальном сайте учреждения не позднее 10 дней со дня его подписания;

- ознакомить сотрудников учреждения с настоящим Порядком доступа под роспись.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Директор



А.В. Ивашина

Порядок доступа сотрудников
государственного казенного учреждения социального обслуживания
«Гусь-Хрустальный социально-реабилитационный центр
для несовершеннолетних»
в помещения, в которых ведется обработка персональных данных.

1. Настоящий порядок доступа сотрудников государственного казенного учреждения социального обслуживания «Гусь-Хрустальный социально-реабилитационный центр для несовершеннолетних» в помещения, в которых ведется обработка персональных данных, разработан в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях персональных данных, осуществляемых без использования средств автоматизации», постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и другими нормативными правовыми актами.

2. Размещение информационных систем, в которых обрабатываются персональные данные, осуществляется только в охраняемых помещениях. Для помещений, в которых обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей персональных данных и средств защиты информации, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

3. При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

4. Доступ сотрудников учреждения и иных лиц в помещения, в которых ведется обработка персональных данных, осуществляется с учетом обеспечения безопасности информации и исключения доступа к персональным данным третьих лиц.

5. Доступ в помещения, в которых ведется обработка персональных данных, предоставляется:

- лицу, ответственному за организацию обработки персональных данных;
- сотрудникам, осуществляющим обработку персональных данных;
- иным лицам в случае необходимости по согласованию с руководителем.

6. Нахождение лиц в помещениях учреждения, в которых ведется обработка персональных данных, не являющихся уполномоченными лицами на обработку персональных данных, возможно только в сопровождении ответственных сотрудников учреждения* на время, ограниченное необходимостью решения вопросов, связанных с выполнением трудовых функций.

7. Во время пребывания лиц в помещениях учреждения, не являющихся уполномоченными лицами на обработку персональных данных, предотвратить либо прекратить вывод на экран мониторов информации с персональными данными, если данные лица находятся в непосредственной близости от монитора, либо от материальных носителей персональных данных.

8. В нерабочее время помещения учреждения, в которых ведется обработка персональных данных, хранятся документы, содержащие персональные данные, должны закрываться на ключ и должны быть опечатаны, ставиться на сигнализацию (при наличии).

9. Опечатывание помещений проводится должностными лицами, определяемыми приказом директора, при отсутствии должностного лица, опечатывание проводит лицо его замещающее.

10. Уборка помещений, в которых ведется обработка персональных данных, и хранятся документы, содержащие персональные данные, должна производиться в присутствии сотрудников, проводящих обработку персональных данных и ознакомленных с нормативными документами учреждения по информационной безопасности персональных данных.

11. Установка нового оборудования, его замена или ремонт в помещениях, в которых ведется обработка персональных данных, хранятся документы и носители информации, содержащие персональные данные, должны производиться по согласованию с администратором информационной безопасности и заведующего отделением и только в присутствии одного из указанных лиц.

12. В помещения учреждения, где размещены технические средства, позволяющие осуществлять обработку персональных данных, а также хранятся носители информации, допускаются только сотрудники учреждения, уполномоченные на обработку персональных данных.

13. Доступ в кабинет специалиста по кадрам разрешается только специалисту по кадрам. Доступ третьих лиц и сотрудников других отделов учреждения должен быть ограничен.

14. Документы, содержащие персональные данные сотрудников, получателей социальных услуг, хранятся на бумажных носителях в специально оборудованных и закрывающихся шкафах или сейфах, обеспечивающих защиту от несанкционированного доступа. Хранение персональных данных на АРМ осуществляется только на защищенных паролями доступа АРМ, информационная безопасность которых обеспечивается комплексом мер защиты информации, утвержденных требованиями к настройкам АРМ по минимизации угроз утечки, несанкционированного доступа, изменения, удаления, блокирования персональных данных, а также федеральным законодательством.

15. Ответственными за организацию доступа в помещения учреждения, в которых ведется обработка персональных данных, являются заведующие отделениями, главный бухгалтер, специалист по кадрам, заместитель директора.

16. Внутренний контроль за соблюдением порядка доступа в помещения учреждения, в которых ведется обработка персональных данных, проводится администратором информационной безопасности, заведующими отделениями.