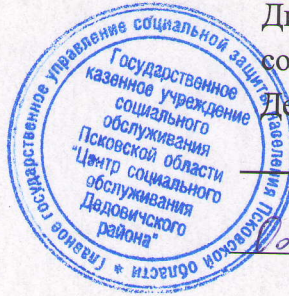


УТВЕРЖДАЮ

Директор ГКУСО «Центр
социального обслуживания
Дедовичского района»

И.Р.Воронина



22-12-2014

ПОРЯДОК ДОСТУПА СОТРУДНИКОВ

1. Общее положение

- 1.1. Настоящий порядок доступа сотрудников в помещения, в которых ведется обработка персональных данных в информационных системах персональных данных, устанавливает единые требования к доступу сотрудников в служебные помещения в целях предотвращения нарушения прав субъектов ПДн, обработка ПДн которых необходима для оказания государственных услуг и обеспечения кадровой и бухгалтерской деятельности, а также в целях обеспечения соблюдения требований законодательства РФ в области ПДн
- 1.2. Настоящий порядок разработан в соответствии с частью 1 «Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ними нормативными правовыми актами, операторами, являющимися государственными органами, утвержденными постановлением Правительства РФ от 21.03.2012 № 211, и на основании «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом ФСТЭК России от 11.02.2013 г. № 17, и «Типовых требований по организации и обеспечению функционирования шифровальных средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах, утвержденных ФСБ России 21.02.2008 г. № 149/6/6-622.
- 1.3. Контролируемая зона, в котором расположены средства автоматизации и защиты ИСПДн, в том числе автоматизированные рабочие места, на которых ведется обработка ПДн
- 1.4. Перечень помещений, в которых ведется обработка ПДн, и их границы устанавливаются приказом «Об определении границ контролируемой зоны и требований к ее безопасности»
- 1.5. Настоящий порядок обязателен для применения и использования всеми сотрудниками.
- 1.6. Ответственность за соблюдение положений настоящего Порядка несут сотрудники структурных подразделений, обрабатывающие ПДн, а также руководители данных структурных подразделений.
- 1.7. Контроль соблюдения требований настоящего порядка обеспечивает ответственный за организацию обработки ПДн.

2. Требования к помещениям контролируемой зоны

- 2.1. Бесконтрольный доступ сторонних лиц в помещения контролируемой зоны должен быть исключен.
- 2.2. Все помещения контролируемой зоны должны быть оборудованы охранной сигнализацией, либо предусматривать круглосуточное дежурство.
- 2.3. Ограждающие конструкции помещений контролируемой зоны должны предполагать существенные трудности для нарушителя по их преодолению.
- 2.4. К помещениям контролируемой зоны, в которых установлены криптографические средства защиты ПДн или хранятся ключевые документы к ним, предъявляются ужесточенные требования по безопасности, указанные в разделе 5 настоящих Правил.

3. Доступ в помещении контролируемой зоны

- 3.1. Доступ посторонних лиц в помещения контролируемой зоны, должен осуществляться только ввиду служебной необходимости.
- 3.2. На момент присутствия посторонних лиц в помещении контролируемой зоны, должны быть приняты меры по недопущению ознакомления посторонних лиц с ПДн.
- 3.3. Допуск сотрудников в помещение контролируемой зоны оформляется после подписания сотрудником Обязательства о неразглашении информации, содержащие персональные данные, и инструктажа ответственным за организацию обработки ПДн, либо ответственным за обеспечение безопасности персональных данных информационных систем персональных данных.
- 3.4. В нерабочее время помещения контролируемой зоны должны ставиться на охрану. При этом все окна и двери в смежные помещения должны быть надежно закрыты, материальные носители ПДн должны быть убраны в запираемые шкафы, АРМ выключены или заблокированы.

4. Доступ в серверные помещения контролируемой зоны

- 4.1. Доступ в серверные помещения контролируемой зоны разрешен только администратору ИСПДн, ответственному за обеспечение безопасности персональных данных информационных систем персональных данных и ответственному за организацию обработки персональных данных.
- 4.2. Уборка серверных помещений происходит только при строгом контроле лиц, указанных в пункте 4.1 настоящих Правил.
- 4.3. Серверные помещения контролируемой зоны в обязательном порядке оснащаются охранной сигнализацией, системой видеонаблюдения и системой автономного питания средств охраны.
- 4.4. Доступ в серверные помещения контролируемой зоны посторонних лиц допускается строго по согласованию с ответственным лицом за организацию обработки ПДн.

5. Требования к режимным помещениям

- 5.1. Режимные помещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам.

Помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможна проникновение в режимные помещения

посторонних лиц необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

- 5.2. Размещение, специальное оборудование, охрана и организация режима в режимных помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ
- 5.3. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены
- 5.4. Режимные помещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственному за организацию обработки ПДн в совместно с представителем службы охраны по организации с отметкой в соответствующих журналах
- 5.5. Для хранения ключевых документов, эксплуатационной и технической документации, устанавливающих криптосредства носителей должно быть предусмотрено необходимое число надежных металлических хранилищ, оборудованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища должен находиться у ответственного за организацию обработки ПДн.
- 5.6. По окончании рабочего дня режимное помещение и установленное в нем хранилища должны быть закрыты, хранилища опечатаны.
- 5.7. Ключи от режимных помещений, а также ключ от хранилища, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих режимных помещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.
- 5.8. При утрате ключа от хранилища или от входной двери в режимное помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный за организацию обработки ПДн
- 5.9. В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств или ответственным за организацию обработки ПДн. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному лицу за организацию обработки ПДн. Прибывший ответственный за организацию обработки ПДн должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять, при необходимости, меры к локализации последствий компрометации персональных данных и к замене скомпрометированных криптоключей
- 5.10. Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами
- 5.11. На время отсутствия пользователей криптосредств указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемые хранилища. В противном случае по согласованию с ответственными за организацию обработки ПДн необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.