ПРИНЯТО
Общим собранием
работников МКДОУ
«Детский сад № 19»
Протокол № 1 от 27.01.2017

УТВЕРЖДАЮ
Заведующий МКДОУ
«Детский сад № 19»
Т.Н. Крезова
№ 12/03-05 от 27.01.2017

ПОРЯДОК

доступа сотрудников
муниципального казенного дошкольного образовательного учреждения
«Детский сад № 19»

1. Общие положения

1.1. Настоящие порядок доступа (далее - Порядок) сотрудников муниципального казенного образовательного учреждения «Детский сад № 19» (далее - ОО) в помещения, в которых ведется обработка персональных данных (далее - ПДн) в информационных системах персональных данных (далее - ИСПДн), устанавливает единые требования к доступу сотрудников ОО в служебные помещения в целях предотвращения нарушения прав субъектов ПДн, обработка ПДн которых необходима для оказания государственных и муниципальных услуг и обеспечения кадровой и бухгалтерской деятельности в ОО, 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 ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», утвержденных постановлением Правительства РФ от 21 марта 2012 г. № 211, и на основании «Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденных приказом ФСТЭК России от 11 февраля 2013г. № 17, и «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) 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 персональных данных», утвержденных ФСБ России 21 февраля 2008 г. № 149/6/6-622.

1.3. Контролируемая зона (далее - контролируемая зона) - пространство (территория, здание, часть здания, помещение), в котором расположены средства автоматизации и защиты ИСПДн, в том числе автоматизированные рабочие места (далее - АРМ), на которых ведется обработка ПДн.

1.4. Перечень помещений, в которых ведется обработка ПДн, и их границы устанавливаются приказом заведующего ОО «Об определении границ контролируемой зоны и требований к ее безопасности».

1.5. Настоящий Порядок обязателен для применения и исполнения всеми сотрудниками ОО.

1.6. Ответственность за соблюдение положений настоящего Порядка несут

1.1. несут сотрудники структурных подразделений ОО, обрабатывающие ПДн, а также руководители данных структурных подразделений.

1.2. Контроль соблюдения требований настоящего Порядка обеспечивает ответственный за организацию обработки ПДн в ОО.

2. Требования к помещениям контролируемой зоны

2.1. Бесконтрольный доступ сторонних лиц в помещения контролируемой зоны должен быть исключён.

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 (далее - криптосредства) или хранятся ключевые документы к ним, (далее - режимные помещения), предъявляются ужесточённые требования по безопасности, указанные в разделе 5 настоящих Правил.

3. Доступ в помещения контролируемой зоны

3.1. Доступ посторонних лиц в помещения контролируемой зоны, должен осуществляется 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 (например: мониторы повёрнуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке или накрыты чистыми листами бумаги).

3.3. Допуск сотрудников в помещения контролируемой зоны оформляется после подписания сотрудником Обязательства о неразглашении информации, содержащей персональные данные, и инструктажа ответственным за организацию обработки ПДн в ОО, либо ответственным за обеспечение безопасности персональных данных информационных систем персональных данных ОО.

3.4. В нерабочее время помещения контролируемой зоны должны ставиться на охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, материальные носители ПДн должны быть убраны в запираемые шкафы (сейфы), АРМ выключены или заблокированы.

4. Требования к режимным помещениям

4.1. Режимные помещения выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надёжное 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 возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решётками, препятствующими неконтролируемому проникновению в режимные помещения.

4.2. 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.

4.3. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.

4.4. Режимные помещения охраняются дежурным по организации и ночным сторожем.

4.5. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено надёжное металлическое хранилище - сейф. Один экземпляр ключа от хранилища должен находиться у ответственного за организацию обработки ПДн в ОО.

4.6. По окончании рабочего дня режимное помещение и установленное в нем хранилище должно быть закрыто.

4.7. 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 необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный за организацию обработки ПДн в ОО.

4.8. В обычных условиях режимное помещение, находящиеся в них хранилище могут быть вскрыты только пользователями криптосредств или ответственным за организацию обработки ПДн в ОО. При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за организацию обработки ПДн в ОО. Прибывший ответственный за организацию обработки ПДн в ОО 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.

4.9. 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.

4.10. 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 ответственным за организацию обработки ПДн в ОО необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.