|  |
| --- |
| УТВЕРЖДАЮ  Пр. № 39от «18» \_\_\_мая\_\_\_ 2017 г.  заведующий МБДОУ детского сада  № 26 «Аленький цветочек»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С. В. Шаталова |

ПОРЯДОК

доступа сотрудников МБДОУ детского сада № 26 «Аленький цветочек»

1.​ Общие положения

2.1.​ Настоящие порядок доступа (далее – Порядок) сотрудников Муниципального бюджетного дошкольного образовательного учреждения детского сада № 26 «Аленький цветочек» (далее – Учреждение) в помещения, в которых ведется обработка персональных данных (далее – ПДн) в информационных системах персональных данных (далее – ИСПДн), устанавливает единые требования к доступу сотрудников Учреждения 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 Учреждении, а также в целях обеспечения соблюдения требований законодательства РФ в области ПДн.

2.2.​ 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.

2.3.​ 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.

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

2.5.​ Настоящий Порядок обязателен для применения и исполнения всеми сотрудниками Учреждения.

2.6.​ Ответственность за соблюдение положений настоящего Порядка несут сотрудники структурных подразделений , обрабатывающие ПДн, а также руководители данных структурных подразделений.

2.7.​ Контроль соблюдения требований настоящего Порядка обеспечивает ответственный за организацию обработки ПДн в Учреждении.

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.

3.​ Доступ в помещения контролируемой зоны.

2.1.​ Доступ посторонних лиц в помещения контролируемой зоны, должен осуществляется только ввиду служебной необходимости.

2.2.​ 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).

2.3.​ 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 Учреждении, либо ответственным за обеспечение безопасности персональных данных информационных систем персональных данных Учреждения.

2.4.​ 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.

3.​ Требования к режимным помещениям.

3.1.​ 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, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

3.2.​ 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.

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

3.4.​ По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны.

3.5.​ Ключи от режимных помещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ режимного помещения, 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.

3.6.​ 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.

3.7.​ 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 Учреждении необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.