

УТВЕРЖДАЮ

Директор – ОГБОУ «Елатомская
школа-интернат для
детей-сирот»

Н.В.Тимохина

«31» 03 2017 г.



ПОРЯДОК
доступа работников в помещения,
в которых ведется обработка персональных данных
ОГБОУ «Елатомская школа-интернат для детей-сирот»

Настоящий Порядок доступа в помещения, в которых ведется обработка персональных данных с использованием информационной системы персональных данных, предназначенной для реализации государственной услуги «Прием заявлений, постановка на учет и зачисление детей в образовательные учреждения, реализующие основную общеобразовательную программу основного общего образования» (далее - Порядок), устанавливает единые требования к доступу в служебные помещения в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в ОГБОУ «Елатомская школа-интернат для детей-сирот» (далее школа - интернат) и обеспечения соблюдения требований законодательства о персональных данных.

Настоящий Порядок обязателен для применения и исполнения всеми работниками школы - интерната, участвующими в обработке персональных данных с использованием информационной системы персональных данных предназначенной для реализации государственной услуги «Прием заявлений, постановка на учет и зачисление детей в образовательные учреждения, реализующие основную общеобразовательную программу основного общего образования».

Помещения, в которых ведется обработка персональных данных, с использованием информационной системы персональных данных предназначенной для реализации государственной услуги «Прием заявлений, постановка на учет и зачисление детей в образовательные учреждения, реализующие основную общеобразовательную программу основного общего образования» (Далее - Помещения) должны обеспечивать сохранность информации и технических средств, исключать возможность бесконтрольного проникновения в помещение и их визуального просмотра посторонними лицами и оснащены охранной сигнализацией.

Персональные данные на бумажных носителях должны находиться в недоступном для посторонних лиц месте.

Бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) хранятся в хранилищах, оборудованных печатающими устройствами.

Помещения, запираются на ключ, а в нерабочее время подключаются к охранной сигнализации.

Вскрытие и закрытие (опечатывание) помещений, производится работниками, имеющими право доступа в данные помещения.

Перед закрытием помещений, по окончании рабочего времени работники, имеющие право доступа в помещения, обязаны: убрать бумажные носители персональных данных и электронные носители персональных данных (диски, флеш-карты) в шкафы, закрыть и опечатать шкафы; отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение; закрыть окна; подключить охранную сигнализацию.

Перед открытием помещений, работники, имеющие право доступа в помещения, обязаны: провести внешний осмотр с целью установления целостности двери и замка; открыть дверь и осмотреть помещение, проверить наличие и целостность печатей на шкафах.

При обнаружении неисправности двери и запирающих устройств работники обязаны: не вскрывая помещение, доложить непосредственному руководителю; в присутствии не менее двух иных работников, включая непосредственного руководителя, вскрыть помещение и осмотреть его; составить акт о выявленных нарушениях и передать его руководителю для организации служебного расследования.

Право самостоятельного входа в помещения, имеют только работники, непосредственно работающие в данном помещении. Иные работники имеют право пребывать в помещении, только в присутствии работников, непосредственно работающих в данном помещении.

При работе с информацией, содержащей персональные данные, двери помещений должны быть всегда закрыты. Присутствие иных лиц, не имеющих права доступа к персональным данным, должно быть исключено.

Техническое обслуживание информационной системы персональных данных предназначенной для реализации муниципальной услуги «Прием заявлений, постановка на учет и зачисление детей в образовательные учреждения, реализующие основную образовательную программу основного общего образования», уборка помещения, в котором ведется обработка персональных данных, а также проведение других работ осуществляются в присутствии работника, работающего в данном помещении.

В случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещение, вскрывается комиссией в составе не менее двух человек.

Ответственность за соблюдение порядка доступа в помещения, возлагается на Руководителей обрабатывающих персональные данные.

УТВЕРЖДАЮ
Директор ОГБОУ «Елатомская школа-интернат
для детей-сирот»

_____ Н.В.Тимохина
« ___ » _____ г.

ПОРЯДОК

доступа сотрудников ОГБОУ «Елатомская школа-интернат для детей-сирот» в
помещения,
в которых ведется обработка персональных данных

1. Общие положения

1.1. Настоящий порядок доступа (далее - Порядок) сотрудников ОГБОУ «Касимовская школа - интернат» (далее - школа - интернат) в помещения, в которых ведется обработка персональных данных (далее - ПДн) в информационных системах персональных данных (далее - ИСПДн), устанавливает единые требования к доступу сотрудников школы - интерната 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 школе - интернате, 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 директора школы - интерната «Об определении границ контролируемой зоны и требований к ее безопасности».

1.5. Настоящий Порядок обязателен для применения и исполнения всеми сотрудниками школы - интерната.

1.6. Ответственность за соблюдение положений настоящего Порядка несут

сотрудники структурных подразделений школы - интерната, обрабатывающие ПДн, а также руководители данных структурных подразделений.

1.7. Контроль соблюдения требований настоящего Порядка обеспечивает ответственный за организацию обработки ПДн в школе - интернате.

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 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 (например: мониторы повернуты 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 школе - интернате, либо ответственным за обеспечение безопасности персональных данных информационных систем персональных данных школы - интерната.

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. Доступ в серверные помещения контролируемой зоны

4.1. Доступ в серверные помещения контролируемой зоны разрешён только администратору ИСПДн, ответственному за обеспечение безопасности персональных данных информационных систем персональных данных школы - интерната и ответственному за организацию обработки ПДн в школе - интернате.

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 за организацию обработки ПДн в школе - интернате.

4.5. Нахождение в серверных помещениях контролируемой зоны посторонних лиц без сопровождающего не допустимо.

5. Требования к режимным помещениям

5.1. 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.

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 или дежурным по организации с отметкой в соответствующих журналах.

5.5. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено необходимое число надёжных 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 в школе - интернате.

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

5.7. 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.

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 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 школе - интернате.

5.9. В обычных условиях режимные помещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств или ответственным за организацию обработки ПДн в школе - интернате. 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 школе - интернате. Прибывший ответственный за организацию обработки ПДн в школе - интернате 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 ответственным за организацию обработки ПДн в школе - интернате необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.