МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ЦЕНТР ТВОРЧЕСТВА

УТВЕРЖДАЮ
директор МБОУ ДО ЦТ
_____Е.С.Миндрина
Приказ №25 от "04" марта 2024 г

ПОРЯДОК
доступа служащих государственного или муниципального органа в помещения, в которых ведётся обработка персональных данных

1. Общие положения

Настоящий порядок разработан в целях обеспечения безопасности персональных данных, средств вычислительной техники информационных систем персональных данных, материальных носителей персональных данных, а также обеспечения внутриобъектового режима.

Объектами охраны муниципального бюджетного образовательного учреждения дополнительного образования Центра творчества (далее – МБОУ ДО ЦТ) являются:

1) помещения, в которых происходит обработка персональных данных как с использованием средств автоматизации, так и без таковых;

2) помещения, аттестованные по требованиям безопасности речевой информации (далее – защищаемые помещения);

3) помещения, в которых установлены компьютеры, сервера и коммутационное оборудование, участвующее в обработке персональных данных;

4) помещения, в которых хранятся материальные носители персональных данных;

5) помещения, в которых хранятся резервные копии персональных данных.

Бесконтрольный доступ посторонних лиц в указанные помещения должен быть исключён.

К помещениям, в которых установлены криптографические средства, предназначенные для шифрования персональных данных (в том числе носители ключевой информации) (далее – спецпомещения), предъявляются ужесточённые требования по безопасности.

Ответственность за соблюдение положений настоящего порядка несут работники структурных подразделений, допущенные в защищаемые помещения и спецпомещения, а также руководители их структурных подразделений.

Контроль соблюдения требований настоящего порядка обеспечивает работник, назначенный ответственным за организацию

обработки персональных данных в МБОУ ДО ЦТ. Контроль соблюдения требований настоящего порядка к спецпомещениям обеспечивает работник, назначенный ответственным пользователем криптосредств.

Некоторые положения настоящего порядка могут не применяться в зависимости от специфики обработки персональных данных структурными подразделениями МБОУ ДО ЦТ по согласованию с ответственным за организацию обработки персональных данных.

Все объекты охраны МБОУ ДО ЦТ должны быть оборудованы охранной сигнализацией, либо предусматривать круглосуточное дежурство.

Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению.

Например: металлические решётки на окнах, металлическая дверь, система контроля и управления доступа и так далее.

2. Допуск в помещения, в которых ведётся обработка персональных данных

Доступ посторонних лиц в помещения, в которых ведётся обработка персональных данных, должен осуществляется только ввиду служебной необходимости.

При этом на момент присутствия посторонних лиц в помещении(ях) должны быть приняты меры по недопущению ознакомления посторонних лиц с персональными данными.

Например: мониторы повёрнуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

Допуск работников (служащих) в помещения, в которых ведётся обработка персональных данных, оформляется после подписания работником (служащим) обязательства о неразглашении и инструктажа, проводимого работником, назначенным ответственным за организацию обработки персональных данных в МБОУ ДО ЦТ, либо работника, назначенного ответственным за обеспечение безопасности информационных систем персональных данных.

В нерабочее время помещения, в которых осуществляется обработка персональных данных, должны ставиться на охрану. При этом все окна и двери в смежные помещения должны быть надёжно закрыты, материальные носители персональных данных должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

3. Допуск в серверные помещения

Доступ в серверные помещения осуществляется в соответствии со списком, утверждённым в МБОУ ДО ЦТ и согласованным с работником, назначенным ответственным за организацию обработки персональных данных и администратором информационной безопасности МБОУ ДО ЦТ. Уборка серверных помещений происходит только при строгом контроле лиц, указанных в утверждённом списке.

Серверное помещение в обязательном порядке оснащается охранной сигнализацией, системой видеонаблюдения и системой автономного питания средств охраны.

Доступ в серверные помещения посторонних лиц допускается строго по согласованию с ответственным за организацию обработки персональных данных.

Нахождение в серверных помещениях посторонних лиц без сопровождающего не допустимо.

4. Допуск лиц в спецпомещения

Спецпомещения 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 спецпомещения посторонних лиц, необходимо оборудовать металлическими решётками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

Расположение спецпомещения, специальное оборудование, охрана и организация режима в спецпомещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

Для предотвращения просмотра извне спецпомещений их окна должны быть защищены.

Спецпомещения должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственному пользователю криптосредств совместно с представителем службы охраны или дежурным по организации с отметкой в соответствующих журналах.

Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей должно быть предусмотрено необходимое количество надёжных металлических хранилищ, оборудованных внутренними

замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Второй экземпляр ключа от хранилища должен находиться у ответственного пользователя криптосредств.

По окончании рабочего дня спецпомещение и установленные в нём хранилища должны быть закрыты, хранилища опечатаны.

Ключи от спецпомещений, а также ключ от хранилища, в котором находятся ключи от всех других хранилищ спецпомещения, в опечатанном виде должны быть сданы под расписку в соответствующем журнале службы охраны или дежурному по организации одновременно с передачей под охрану самих спецпомещений. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за эти хранилища.

При утрате ключа от хранилища или от входной двери в спецпомещение, 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 ответственного пользователя криптосредств.

В обычных условиях спецпомещения, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств или ответственного пользователя криптосредств.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственного пользователя криптосредств. Прибывший ответственный за организацию обработки персональных данных 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.

Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в спецпомещениях 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.

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 пользователем криптосредств необходимо предусмотреть

организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также других ситуаций, которые могут создавать угрозу жизни и здоровью граждан, доступ в спецпомещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с работником, назначенным ответственным за организацию обработки персональных данных в МБОУ ДО ЦТ.

В случае, если нештатная ситуация не создает угрозу жизни и здоровью граждан, доступ в спецпомещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с работником, назначенным ответственным за организацию обработки персональных данных в МБОУ ДО ЦТ, но под контролем лиц, имеющих право допуска в спецпомещения.

Директор Е.С.Миндрина