УТВЕРЖДАЮ
Директор МАОУ СОШ № 31
_____Е.В. Иванова
«22» сентября 2023г.

ДСП
Экз.№ 1

Инструкция
о порядке доступа работников в помещения, в которых ведется обработка персональных данных, в том числе с использованием средств криптографической защиты информации (СКЗИ)

Оглавление

1. Общие положения

1.1. Настоящая инструкция разработана в целях обеспечения безопасности персональных данных, средств вычислительной техники информационных систем персональных данных, материальных носителей персональных данных.

Объектами охраны муниципального автономного общеобразовательного учреждения города Калининграда средней общеобразовательной школы № 31 (далее - МАОУ СОШ № 31) являются:

- помещения, в которых происходит обработка персональных данных, как с использованием средств автоматизации, так и без таковых;
- помещения, в которых установлено коммутационное оборудование, участвующее в обработке персональных данных;
- помещения, в которых хранятся материальные носители персональных данных;
- помещения, в которых хранятся резервные копии персональных данных.

1.2. Бесконтрольный доступ посторонних лиц в указанные помещения должен быть исключён.

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

1.4. Ответственность за соблюдение положений настоящей инструкции несут работники МАОУ СОШ № 31, обрабатывающих персональные данные.

1.5. Контроль за соблюдением требований настоящей инструкции обеспечивают ответственные за обеспечение безопасности персональных данных в МАОУ СОШ № 31.

1.6. Все помещения МАОУ СОШ № 31 должны быть оборудованы охранной сигнализацией.

1.7. Ограждающие конструкции объектов охраны предполагают существенные трудности для нарушителя по их преодолению. Пример: круглосуточная охрана, система СКУД.

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

2.1. Доступ посторонних лиц в помещения, в которых ведётся обработка персональных данных, осуществляется только ввиду служебной необходимости. Самостоятельный доступ в помещение не сотрудников МАОУ СОШ № 31 запрещен.

2.2. На момент присутствия посторонних лиц в помещении (в виду выполнения трудовых обязанностей, договорных отношений, информирования субъектов персональных данных и т.д.) применяются меры по недопущению ознакомления посторонних лиц с персональными данными. Пример: мониторы повёрнуты в сторону от посетителей (либо включен режим просмотра отображаемой на экране монитора АРМ информации), документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

2.3. Допуск сотрудников в помещения, в которых ведётся обработка персональных данных, оформляется после подписания сотрудником обязательства о неразглашении и инструктажа ответственного за организацию обработки персональных данных, либо администратора информационной безопасности.

2.4. В нерабочее время, помещения, в которых ведётся обработка персональных данных, ставятся под 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 лиц в помещение, где ведется обработка персональных данных с использованием средств криптографической защиты информации

3.1. Помещение выделяют с учётом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещение имеют прочные входные двери с замками, гарантирующими надёжное закрытие помещений в нерабочее время.

3.2. Размещение, специальное оборудование, охрана и организация режима охраны в помещении исключают возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

3.3. Для предотвращения просмотра извне помещения, их окна надежно защищены.

3.4. Помещение, оснащено охранной сигнализацией, связанной с дежурным охраны здания. Исправность сигнализации, периодически проверяется ответственным за организацию обработки персональных данных.

3.5. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей, предусмотрено металлическое хранилище, оборудованное внутренними замками с двумя экземплярами ключей и приспособлениями для опечатывания замочных скважин. Один экземпляр ключа от хранилища находиться у ответственного за организацию обработки персональных данных.

3.6. По окончании рабочего дня помещение и установленные в нем хранилище закрываются, хранилища опечатываются.

3.7. Ключи от помещения, а также ключ от хранилища, сдаются под расписку в соответствующем журнале. Печати, предназначенные для опечатывания хранилищ, должны находиться у пользователей криптосредств, ответственных за хранилище.

3.8. При утрате ключа от хранилища или от входной двери в помещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный за организацию обработки персональных данных.

3.9. В обычных условиях помещение, находящиеся в них опечатанные хранилища могут быть вскрыты только пользователями криптосредств или ответственным за организацию обработки персональных данных.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в это помещение или хранилище посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за организацию обработки персональных данных. 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.

3.10. Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в помещении должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам.

3.11. На время отсутствия пользователей криптосредств указанное оборудование, при наличии технической возможности, должно быть выключено, отключено от линии связи и убрано в опечатываемое хранилище. В противном случае по согласованию с ответственным за организацию обработки персональных данных необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.