**МБОУ «Средняя общеобразовательная школа №82
с углублённым изучением отдельных предметов им. Р.Г.Хасановой»
Приволжского района г.Казани**

ПРИНЯТО
Общее собрание работников школы
(протокол № 1 от 07.03.2015 г.)

СОГЛАСОВАНО
Заседание профсоюзного комитета
(протокол № 3 от 06.03.2015 г.)

УТВЕРЖДАЮ
Директор школы № 82
_____ Э. М. Скобелкина
Введено в действие
приказом по школе
от 11.03.2015 года № 40

Инструкция по допуску лиц в помещения, в которых ведётся обработка персональных данных

1. Общие положения

1.1.Настоящее Положение разработано в соответствии с Федеральным законом «Об образовании в Российской Федерации», Федеральным законом от 27 июля 2006 №152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», Постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», нормативно-правовых актов Российской Федерации в области трудовых отношений и образования, нормативных и распорядительных документов органов управления образования федерального, регионального, муниципального уровней, Уставом МБОУ «Средняя общеобразовательная школа № 82 с углублённым изучением отдельных предметов им. Р.Г.Хасановой» Приволжского района г. Казани (далее - Школа) с целью обеспечения защиты прав и свобод каждого работника и учащегося при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.2.Настоящим положением определяется порядок допуска работников Школы в помещения, в которых ведется обработка персональных данных работников и учащихся Школы.

1.3.Настоящая инструкция разработана в целях обеспечения безопасности персональных данных, средств вычислительной техники информационных систем персональных данных, материальных носителей персональных данных, а так же обеспечения внутриобъектового режима.

1.4.Настоящее Положение принято педагогическим советом Школы с учетом мнения профсоюзного комитета Школы.

2. Требования к объектам охраны

2.1. Объектами охраны являются:

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

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

– помещения, в которых хранятся материальные носители персональных данных;

– помещения, в которых хранятся резервные копии персональных данных.

.2. Бесконтрольный доступ посторонних лиц в указанные помещения должен быть исключён.
.3. Ответственность за соблюдение положений настоящей инструкции несут сотрудники Школы, обрабатывающие персональные данные, а так же члены администрации.

3. Организация допуска в помещения, в которых ведётся обработка персональных данных

.1. Доступ посторонних лиц в помещения, в которых ведётся обработка персональных данных, должен осуществляется только ввиду служебной необходимости.
.2. При этом на момент присутствия посторонних лиц в помещении должны быть приняты меры по недопущению ознакомления посторонних лиц с персональными данными. Пример: мониторы повёрнуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).
.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.
.4. В нерабочее время помещения, в которых ведётся обработка персональных данных, должны быть закрыты на ключ. 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.

4. Организация допуска в серверные помещения.

4.1. Доступ в серверные помещения разрешён только ответственному за техническое обслуживание ИСПДн, администратору информационной безопасности и ответственному за организацию обработки персональных данных. Уборка серверных помещений происходит только при строгом контроле указанных лиц.
4.2. Серверное помещение в обязательном порядке находится под видеонаблюдением и оснащается системой автономного питания средств охраны.
4.3. Доступ в серверные помещения посторонних лиц допускается строго по согласованию с ответственным за организацию обработки персональных данных.
4.4. Нахождение в серверных помещениях посторонних лиц без сопровождающего не допустимо.

5. Организация допуска лиц в спецпомещения.

5.1. 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.
5.2. Размещение, 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.
5.3. Для предотвращения просмотра извне спецпомещений их окна должны быть защищены.
5.4. Спецпомещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания или дежурным по организации. Исправность сигнализации периодически необходимо проверять ответственному за организацию обработки персональных данных 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

лючей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Один кземпляр ключа от хранилища должен находиться у ответственного за организацию обработки ерсональных данных.

.6. По окончании рабочего дня спецпомещение и установленные в нем хранилища должны быть акрыты, хранилища опечатаны.

.7. 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 оответствующем 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.

5.8. 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 ответственный за организацию обработки персональных данных.

5.9. В обычных условиях спецпомещения, 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 эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному за организацию обработки персональных данных. 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.

5.10. 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.

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 персональных данных необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

6. Заключительные положения.

6.1.Настоящее Положение действует до принятия нового с даты введения его в действие приказом директора Школы.

В данном документе пронумеровано,
прошнуровано, и скреплено печатью
3 (три) листа
Директор МБОУ «Школа№82»

Э. М. Скобелкина