Приложение 3

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 23

Подписано цифровой подписью: МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 23
Дата: 2023.02.27 14:50:14 +04'00'

УТВЕРЖДЕНА
приказом МБОУ СОШ № 23
от 03 октября 2022 № 384-ОД

И Н С Т Р У К Ц И Я
по обеспечению порядка доступа в помещения, в которых ведется обработка персональных данных в информационной системе МБОУ СОШ № 23

1. Общие положения

1.1. Настоящая инструкция по обеспечению доступа в помещения МБОУ СОШ № 23 (далее – Школа), в которых ведется обработка персональных данных (далее – Инструкция), разработана в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), 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», утвержденного постановлением Правительства РФ от 21 марта 2012 г. № 211, постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом ФАПСИ от 13.06.2001 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», а также приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

1.2. Целью настоящей Инструкции является обеспечение безопасности персональных данных при их обработке (в том числе хранении) путем создания условий, затрудняющих несанкционированный доступ к техническим средствам и средствам защиты, участвующим в обработке персональных данных, и машинным носителям персональных данных.

1.3. Ознакомлению с настоящей Инструкцией подлежат все лица, имеющие право доступа и самостоятельного пребывания в помещениях Школы, в которых размещены используемые средства защиты информации, в том числе средства криптографической защиты информации (далее – СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ или хранятся машинные носители персональных данных (далее – Помещения).

1.4. Настоящая Инструкция вступает в силу с момента её утверждения и действует до её отмены либо замены новой Инструкцией.

2. Требования к помещениям

Для помещений, в которых хранятся и обрабатываются персональные данные, организуется режим обеспечения безопасности, при котором обеспечивается сохранность носителей информации, содержащей персональные данные, а также исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц. Данный режим достигается:

– оснащением помещения входными дверьми с замками;

– отдельным хранением дубликатов ключей;

– закрытием металлических шкафов (сейфов), где хранятся носители информации, содержащие персональные данные;

– утверждением перечня лиц, имеющих право доступа в помещение.

Сейфы (металлические шкафы) для хранения съемных машинных носителей персональных данных должны быть оборудованы внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов).

2.1. Для помещений, в которых размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, организуется режим обеспечения безопасности, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

Данный режим достигается:

– оснащением помещения входными дверьми с замками;

– обеспечением постоянного закрытия дверей Помещения на замок и их открытия только для санкционированного прохода;

– опечатыванием помещения по окончании рабочего дня или оборудованием помещения соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещения;

– отдельным хранением дубликатов ключей;

– закрытием металлических шкафов и сейфов, где хранятся носители ключевой, аутентифицирующей и парольной информации СКЗИ;

– утверждением перечня лиц, имеющих право доступа в Помещения (приложение 1).

3. Организация доступа в Помещения

3.1. В Помещения допускаются сотрудники Школы, указанные в «Перечне лиц, имеющих право самостоятельного доступа в помещения, в которых располагаются СКЗИ (далее – Перечень), утвержденном приказом директора школы.

3.2. Помимо лиц, указанных в Перечне (далее – лица, имеющие право доступа в Помещения), право самостоятельного пребывания в Помещениях, для которых введен режим безопасности, имеет директор школы, его заместители.

3.3. Лица, не внесенные в Перечень (далее – лица, не имеющие право доступа в Помещения), являются сторонними лицами и могут находиться в Помещениях только в присутствии лиц, имеющих права доступа в Помещения.

3.4. Посторонние лица имеют право пребывать в Помещениях только в присутствии лиц, имеющих право доступа в Помещения, и в течение ограниченного количества времени, необходимого для решения вопросов, связанных с исполнением государственных (муниципальных) функций и (или) осуществлением полномочий в рамках договоров, заключенных с Организацией, обслуживанием компьютерной техники и оргтехники.

3.5. Доступ в Помещения разрешается только в рабочее время.

3.6. В течение рабочего времени лица, имеющие право доступа в Помещения:

– закрывают дверь Помещения на ключ при оставлении последним Помещения (при этом запрещается оставлять ключ в замке Помещения);

– не покидают Помещение, если в нем находятся лица, не имеющие право доступа в Помещения;

– при обнаружении фактов нарушения режима безопасности Помещения ставят в известность ответственного за обеспечение безопасности персональных данных в информационной системе Школы (далее – Ответственный за обеспечение безопасности ПДн);

– при посещении Помещения посторонними лицами с целями проведения контрольных, проверочных мероприятий, а также работ по обслуживанию Помещения и его инженерно-технических средств ставят в известность Ответственного за обеспечение безопасности ПДн, директора школы и /или его заместителей.

3.7. Доступ в Помещения в нерабочее время возможен только по письменной заявке работника, согласованной с директором школы и имеющей разрешающую резолюцию. Данные заявки хранятся у Ответственного за обеспечение безопасности ПДн.

3.8. Доступ в Помещения при возникновении нештатной ситуации в нерабочее время осуществляется в присутствии Ответственного за обеспечение безопасности ПДн с составлением акта на вскрытие (далее – Акт). В Акте необходимо указать:

– фамилии, имена, отчества должностных лиц, принимавших участие во вскрытии Помещения;

– дату и время вскрытия Помещения;

– причины вскрытия Помещения;

– кто был допущен (должность и фамилия) в Помещение для ликвидации последствий нештатной ситуации;

– как осуществлялась охрана вскрытого Помещения в этот период;

– какое имущество, в каком количестве, куда эвакуировано из вскрытого Помещения и как осуществлялась его охрана;

– кто из должностных лиц и когда был информирован по указанному факту происшествия;

– другие сведения.

Акт подписывается должностными лицами, вскрывшими Помещение. Вскрытие сейфов с машинными носителями, содержащими персональные данные, осуществляется работниками, отвечающими за их сохранность.

3.9. При обслуживании Помещений (уборка или ремонт Помещений, инженерно-технического оборудования):

– обслуживающий персонал находится в Помещении только в присутствии лиц, имеющих право доступа в Помещение;

– ключи от замков дверей Помещения обслуживающему персоналу и другим лицам, не имеющим права доступа в Помещение, без согласования с Ответственным за обеспечение безопасности ПДн не выдаются;

– сотрудники, обеспечивающие контроль действий обслуживающего персонала в Помещении, обязаны не допускать несанкционированных действий в отношении компонентов информационной системы и машинных носителей персональных данных;

– капитальный или иной ремонт может проводиться без присутствия лиц, имеющих право доступа в Помещение, только в том случае, если компоненты информационной системы и машинные носители персональных данных были предварительно вынесены из ремонтируемого Помещения в другое контролируемое Помещение, а по окончании ремонта заменены замки.

Организует и контролирует исполнение Ответственный за обеспечение безопасности ПДн.

3.10. Лица, имеющие право доступа в Помещения, несут ответственность за нерегламентированное пребывание в Помещениях работников школы и иных сторонних лиц, не имеющих права доступа в Помещения.

4. Контроль соблюдения порядка доступа в Помещения

4.1. Контроль выполнения требований настоящей Инструкции осуществляется Ответственным за обеспечение безопасности ПДн.

4.2. Ответственный за обеспечение безопасности ПДн в случае установления факта нарушения лицом, имеющим право доступа в Помещения, настоящей Инструкции проводит с ним разъяснительную работу, а в случае неоднократного нарушения уведомляет директора школы.

Приложение 1
к Инструкции по обеспечению
порядка доступа в помещения, в которых
ведется обработка персональных данных
в информационной системе МБОУ СОШ № 23

Список лиц, допущенных к вскрытию и закрытию служебных помещений
МБОУ СОШ № 23, где установлены средства криптографической защиты информации или хранятся ключевые документы к ним

№ п/п	Фамилия, имя, отчество	Должность	Помещение	Подпись