

УТВЕРЖДАЮ

Директор
МБОУ СОШ № 12 им. И.Х.
Тхагушева с. Георгиевское

З.И. Такахо

«05» апреля 2021 года



ИНСТРУКЦИЯ

по допуску лиц в помещения Муниципального бюджетного общеобразовательного учреждения средняя общеобразовательная школа № 12 имени Героя Советского Союза Исмаила Халаловича Тхагушева с. Георгиевское Муниципального образования Туапсинский район, в которых ведется обработка персональных данных

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, а также обеспечения внутри объектового режима.

Документ устанавливает правила доступа в помещения в рабочее и нерабочее время, а также в нестандартных ситуациях.

Объектами охраны Муниципального бюджетного общеобразовательного учреждения средняя общеобразовательная школа № 12 имени Героя Советского Союза Исмаила Халаловича Тхагушева с. Георгиевское Муниципального образования Туапсинский район (далее – Учреждение) являются:

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

2) помещения, в которых хранятся материальные носители персональных данных и резервные копии персональных данных;

3) помещения, в которых установлены криптографические средства, предназначенные для шифрования персональных данных, в том числе носители ключевой информации (далее – спецпомещения).

1.2. Бесконтрольный доступ посторонних лиц в указанные помещения исключён.

Посторонними лицами считаются сотрудники Учреждения, не допущенные к обработке персональных данных и лица, не являющиеся

сотрудниками Учреждения.

1.3. К спецпомещениям, предъявляются дополнительные требования по безопасности, указанные в разделе 4.

1.4. Ответственность за соблюдение положений настоящей инструкции несут сотрудники структурных подразделений, допущенные в помещения, являющиеся объектами охраны, а также их руководители.

1.5. Контроль соблюдения требований настоящей инструкции обеспечивает сотрудник, назначенный ответственным за организацию обработки персональных данных в Учреждении.

1.6. Ограждающие конструкции объектов охраны должны предполагать существенные трудности для нарушителя по их преодолению. Пример: металлические решетки на окнах, металлическая дверь, СКУД и т.д.

2. Правила доступа в помещения, в которых ведется обработка персональных данных

2.1. Доступ посторонних лиц в помещения, в которых ведется обработка персональных данных, а также хранятся материальные носители персональных данных и резервные копии персональных данных, должен осуществляться только ввиду служебной необходимости и под контролем сопровождающего лица, из числа сотрудников, допущенных к обработке персональных данных.

2.2. При этом должны быть приняты меры, исключающие ознакомление посторонних лиц с персональными данными. Пример: мониторы повернуты в сторону от посетителей, документы убраны в стол, либо находятся в непрозрачной папке (накрыты чистыми листами бумаги).

2.3. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в помещения, в которых ведется обработка персональных данных лиц из числа сотрудников Учреждения, не допущенных к обработке персональных данных.

2.4. В нерабочее время все окна и двери в помещениях (в том числе в смежные помещения), в которых ведется обработка персональных данных, должны быть надежно закрыты, материальные носители персональных данных должны быть убраны в запираемые шкафы (сейфы), компьютеры выключены либо заблокированы.

2.5. Доступ сотрудников в помещения, в которых ведется обработка персональных данных в нерабочее время, допускается по распоряжению руководства Учреждения.

3. Правила доступа в серверные помещения

3.1. Доступ в серверные помещения, в которых ведётся обработка персональных данных осуществляется в соответствии со списком,

утверждённым в Учреждения.

Уборка серверных помещений происходит только под контролем лица, из указанных в утверждённом списке.

3.2. Доступ в серверные помещения посторонних лиц допускается по согласованию с ответственным за обеспечение безопасности информационных систем персональных.

3.3. Нахождение в серверных помещениях посторонних лиц без сопровождающего запрещено.

3.4. 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 серверные помещения, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться без согласования с ответственным за обеспечение безопасности информационных систем персональных.

3.5. Доступ сотрудников в серверные помещения в нерабочее время допускается по распоряжению руководства Учреждения.

4. Правила доступа в спецпомещения

4.1. Спецпомещения выделяют с учетом размеров контролируемых зон, регламентированных эксплуатационной и технической документацией к криптосредствам. Помещения должны иметь прочные входные двери с замками, гарантирующими надежное 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 решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в спецпомещения.

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

4.3. Для предотвращения просмотра извне спецпомещений их окна должны быть защищены.

4.4. Спецпомещения должны быть оснащены входными дверьми с замками. Должно быть обеспечено постоянное закрытие дверей спецпомещений на замок и открытие только для санкционированного прохода, а также опечатывание спецпомещений по окончании рабочего дня или оборудование спецпомещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии спецпомещений.

4.5. Доступ в спецпомещения осуществляется в соответствии с перечнем лиц, имеющих право доступа в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и

парольной информации СКЗИ, утверждённым приказом Директора Учреждения.

Доступ иных лиц в спец помещения может осуществляться под контролем лиц, имеющих право допуска в спецпомещения.

4.6. При возникновении чрезвычайных ситуаций природного и техногенного характера, аварий, катастроф, стихийных бедствий, а также ситуаций, которые могут создавать угрозу жизни и здоровью граждан, в целях оказания помощи гражданам, предотвращения, ликвидации предпосылок и последствий нештатной ситуации, может осуществляться доступ в спецпомещения иных лиц из числа сотрудников Учреждения.

Сотрудники органов МЧС и аварийных служб, врачи «скорой помощи» допускаются в спецпомещения для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения Учреждения.

4.7. При утрате ключа от входной двери в спецпомещение замок необходимо заменить или переделать его секрет с изготовлением к нему новых ключей с документальным оформлением.

4.8. Доступ сотрудников в спецпомещения в нерабочее время допускается на основании служебных записок (или иных видов разрешающих документов), подписанных Директором Учреждения.

Нахождение в спецпомещениях посторонних лиц в нерабочее время запрещается.

Заместитель директора по УВР

А.А. Рымаренко