

ПРИЛОЖЕНИЕ №17

УТВЕРЖДЕНО

Приказом «О вводе в действие комплекта
организационно-распорядительной
документации по организации обработки и
защиты персональных данных» МБОУ
Сокольская СШ
от «30» августа 20 24 г.
№ 595

(М.П.)

Порядок

доступа в помещения, в которых размещены
информационные системы персональных данных

Оглавление

1. Общие положения.....	3
2. Порядок организации режима обеспечения безопасности Помещений	4
3. Правила доступа в контролируемую зону в рабочее, нерабочее время, в нештатных ситуациях	5
4. Ответственность	5

1. Общие положения

1.1. Муниципальное бюджетное общеобразовательное учреждение Сокольская средняя школа (далее – Организация) руководствуется настоящим Порядком доступа в помещения (далее - Порядок), обеспечения режима безопасности помещений, в которых размещены информационные системы персональных данных «Управление сферой образования в Нижегородской области», «Сведения ГИА», «Сведения о документах об образовании» (далее – информационные системы), который определяет правила доступа в помещения, в которых размещены информационные системы, в рабочее, нерабочее время и в нештатных ситуациях.

1.2. Сокращения, термины и определения:

В настоящем Порядке используются сокращения, термины и определения, приведенные в таблицах 1 и 2 соответственно.

Таблица 1 – Перечень сокращений

Сокращение	Расшифровка сокращения
ФСТЭК России	Федеральная служба по техническому и экспортному контролю
ПДн	Персональные данные
Помещения	Помещения, в которых размещены информационные системы (технические средства информационных систем, включая средства защиты информации)

Таблица 2 – Перечень терминов и определений

Термин	Определение	Источник
Администратор безопасности информационной системы персональных данных (администратор безопасности)	Работник, ответственный за обеспечение безопасности персональных данных в информационной системе персональных данных	
Информационная система	Совокупность, содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств	ГОСТ Р 51583-2014
Контролируемая зона	Пространство, в пределах которого осуществляется контроль над пребыванием и действиями лиц и/или	ГОСТ Р 56115-2014

Термин	Определение	Источник
	транспортных средств	
Персональные данные	Любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)	Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

1.3. Перечень нормативных правовых актов, на основании которых разработан Порядок:

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»,

Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.4. Пользователи информационных систем должны быть ознакомлены с настоящей инструкцией Порядком до начала работы в информационных системах под роспись. Обязанность по организации ознакомления пользователей с Порядком возлагается на ответственного за организацию обработки ПДн.

2. Порядок организации режима обеспечения безопасности Помещений

2.1. Для Помещений организуется режим обеспечения безопасности, при котором обеспечивается сохранность технических средств обработки персональных данных, средств защиты информации и носителей персональных данных, а также исключается возможность неконтролируемого проникновения и пребывания в этих Помещениях посторонних лиц.

2.2. Перечень Помещений утверждается приказом Организации.

2.3. Помещения оснащаются входными дверями с замками, оборудованными механическими замками.

2.4. Вскрытие и закрытие Помещений производится работниками Организации, имеющие права доступа в данные Помещения.

2.5. Ключи от Помещений хранятся у работников Организации либо в ином порядке, устанавливаемом Инструкцией по обеспечению внутриобъектового и пропускного режима в Организации, утверждаемой приказом Организации.

2.6. Обеспечение режима безопасности Помещений, где размещены и хранятся используемые криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств, осуществляется в соответствии с «Порядком доступа в помещения, где размещены используемые

криптосредства, хранятся криптосредства и (или) носители ключевой, аутентифицирующей и парольной информации криптосредств».

2.7. Внутренний контроль за соблюдением порядка доступа в Помещения осуществляется ответственным за организацию обработки ПДн.

3. Правила доступа в контролируемую зону в рабочее, нерабочее время, в нештатных ситуациях

3.1. На период обработки защищаемых ПДн в помещениях, где размещено оборудование информационных систем и средств защиты информации, могут находиться только работники, допущенные к обработке персональных данных в соответствии с утвержденным приказом Организации Перечнями лиц, имеющих право доступа в помещения, в которых размещены информационные системы.

3.2. В нерабочее время пребывание вышеуказанных работников разрешается на основании служебных записок (или иных видов разрешающих документов), подписанных руководителем Организации.

3.3. Нахождение в помещениях контролируемых зон информационных систем других лиц (например, для проведения необходимых профилактических или ремонтных работ, посетителей) возможно только в присутствии работника, допущенного к обработке персональных данных в настоящем помещении.

3.4. Запрещается бесконтрольное нахождение в помещениях контролируемой зоны посторонних лиц в рабочее и нерабочее время.

3.5. Руководитель и лица, его замещающие, могут находиться в помещениях контролируемой зоны в любое время, в том числе в нерабочие и праздничные дни.

3.6. В случае возникновения нештатной ситуации необходимо незамедлительно сообщать непосредственному руководителю структурного подразделения Организации.

3.7. Сотрудники территориальных подразделений Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий и аварийных служб, врачи «скорой медицинской помощи» допускаются в помещения контролируемой зоны информационных систем для ликвидации нештатной ситуации, иных чрезвычайных ситуаций или оказания медицинской помощи в сопровождении руководителя структурного подразделения Организации.

4. Ответственность

4.1. Работники Организации несут ответственность за ненадлежащее исполнение или неисполнение своих обязанностей, предусмотренных настоящим Порядком, в соответствии с действующим законодательством Российской Федерации.