МУНИЦИПАЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ
«СТАНЦИЯ ЮНЫХ ТЕХНИКОВ БУДЕННОВСКОГО РАЙОНА»
356800 г.Будённовск Ставропольского края, ул.Кирова, 261
тел. 8(86559) 7-35-23; 7-40-24
E-mail:budennovsk.syt@gmail.com
ОКПО 51995190 ОГРН 1022603229252
ИНН/КПП 2624023490/262401001

ПРИКАЗ

От 10.01.2020г. № 10 ОД

Об утверждении документов, определяющих порядок доступа в помещения, в которых обрабатывается конфиденциальная информация, в том числе персональные данные, и где размещены или хранятся средства криптографической защиты информации

В целях принятия мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных», в том числе выполнения требований к защите персональных данных, установленных постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Приказом ФСБ России от 10 июля 2014 г. N 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» и постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

ПРИКАЗЫВАЮ:

1. Утвердить Порядок доступа служащих в МУ ДО СЮТ в помещения, в которых ведется обработка КИ и где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (Приложение № 2 к настоящему приказу).

двери, оборудованные механическими замками, а при необходимости, замками с контролем доступа;

- в нерабочее время помещения должны закрываться, а ключи сдаваться охране;

- выдачу ключей от помещения осуществляет по списку, утвержденному руководителем образовательного учреждения;

- в случае ухода в рабочее время из помещения сотрудников, необходимо это помещение закрыть на ключ;

- уборка помещения должна производиться в присутствии лица, ответственного за это помещения.

- пребывание в помещениях посторонних лиц, не имеющих права доступа в эти помещения, разрешено только после согласования с руководителем образовательного учреждения или его заместителем по направлению деятельности и в сопровождении лица, работающего в этом помещении.

- контроль за пребыванием в помещении посторонних лиц, не имеющих права доступа в эти помещения, осуществляет ответственный за это помещение.

4. Защита информационной системы и машинных носителей КИ от несанкционированного доступа, повреждения или хищения

4.1. В период эксплуатации информационных систем должны быть предусмотрены меры по исключению случаев несанкционированного доступа при проведении ремонтных, профилактических и других видов работ.

4.2. В случае необходимости проведения ремонтных работ средств вычислительной техники, входящих в состав информационной системы, с привлечением специализированных ремонтных организаций обеспечивается обязательное гарантированное уничтожение (стирание) КИ, записанной на

материальном носителе под контролем лица, ответственного за организацию обработки КИ с составлением соответствующего акта.

4.3. Хранение съемных машинных носители КИ должно исключать возможность несанкционированного доступа к ним.

5. Служащие образовательной организации, должны ознакомиться с настоящими Правилами под роспись.

Директор МУ ДО СЮТ М.М.Заикина

Лицо, ответственное за организацию обработки конфиденциальной информации в том числе персональных данных

Приложение № 2

К приказу от 10.01.2020г № 10 ОД

Правила организации режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения

1. Настоящие правила устанавливают требования к организации режима обеспечения безопасности помещений МУ ДО СЮТ (далее – образовательное учреждение), в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

2. Пропускной режим предусматривает:

- защиту от проникновения посторонних лиц в помещения образовательного учреждения, которое обеспечивает само режим доступа.

- запрет на внос и вынос за пределы помещения материальных носителей конфиденциальной информации, в том числе персональных данных (далее – КИ);

- определение перечня должностных лиц, имеющих право доступа в помещения.

3. Внутриобъектовый режим предусматривает:

- назначение ответственного за помещение;

- помещения, в которых обрабатывается КИ с использованием средств автоматизации и без использования таких средств, должны иметь прочные

- в присутствии лица, ответственного за организацию обработки КИ и непосредственного руководителя, вскрыть Помещение и осмотреть его;

- составить акт о выявленных нарушениях и передать его руководителю для организации служебного расследования.

11. Ответственность за соблюдение порядка доступа в Помещения возлагается на лиц, обрабатывающих КИ.

12. Служащие образовательного учреждения, должны ознакомиться с настоящим порядком доступа в помещения, в которых ведется обработка КИ, под роспись.

Директор МУ ДО СЮТ М.М.Заикина

Лицо, ответственное за организацию обработки конфиденциальной информации, в том числе персональных данных

4. Иные лица допускаются в Помещения по согласованию с руководителем образовательного учреждения или его заместителем по направлению деятельности и в сопровождении лица, работающего в этом Помещении.

5. Помещения по окончании рабочего дня должны закрываться на ключ.

6. Вскрытие и закрытие Помещения производится лицами, имеющими право доступа.

7. Уборка Помещения должна производиться в присутствии лица, осуществляющего обработку КИ.

8. Перед закрытием Помещения по окончании рабочего дня, лица, имеющие право доступа в помещения, обязаны:

- убрать материальные носители КИ в шкафы, закрыть и опечатать шкафы;

- отключить технические средства (кроме постоянно действующей техники) и электроприборы от сети, выключить освещение;

- закрыть окна.

9. Перед открытием Помещения лица, имеющие право доступа в помещения, обязаны:

- провести внешний осмотр с целью установления целостности двери;

- открыть дверь и осмотреть Помещение, проверить наличие и целостность печатей на шкафах, где хранятся материальные носители.

10. При обнаружении неисправности двери и запирающих устройств необходимо:

- не вскрывая Помещение, доложить непосредственному руководителю;

Приложение № 2

К приказу от 10.01.2020г №10 ОД

Порядок

доступа служащих МУ ДО СЮТ в помещения, в которых ведется обработка конфиденциальной информации, в том числе персональных данных, и где размещены средства криптографической защиты информации

1. Доступ служащих МУ ДО СЮТ (далее – образовательное учреждение) в помещения, в которых ведется обработка конфиденциальной информации, в том числе персональных данных (далее – КИ), и где размещены используемые средства криптографической защиты информации (далее – СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, осуществляется с учетом обеспечения безопасности КИ.

2. Для помещений, в которых обрабатывается КИ и где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее – Помещения), должен обеспечиваться режим безопасности, при котором исключается возможность неконтролируемого проникновения и пребывания в этих помещениях посторонних лиц.

3. Право самостоятельного входа в помещения имеют сотрудники, непосредственно работающие в этих помещениях, лицо, ответственное за организацию обработки КИ, лицо, ответственное за обеспечение безопасности обработки КИ, и лица, ответственные за организацию работ по криптографической защите информации.

2. Утвердить Правила организации режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения (Приложение № 3 к настоящему приказу).

3. Ознакомить с настоящим приказом сотрудников организации в части их касающейся.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Директор МУ ДО СЮТ М.М.Заикина

МУ ДО СЮТ

ОЗНАКОМЛЕНЫ: