УТВЕРЖДЕН

приказом № 318 от 04.06. 2024

Директор ГАПОУ СО «ТМК»

И.А.Мочалов _____

П 369-2024

СОСТАВ И СОДЕРЖАНИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННОМ АВТОНОМНОМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ САМАРСКОЙ ОБЛАСТИ «ТОЛЬЯТТИНСКИЙ МАШИНОСТРОИТЕЛЬНЫЙ КОЛЛЕДЖ»

Тольятти, 2024 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Данный документ разработан в соответствии с приказом ФАПСИ от 13.06.2001 № 152 «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», Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи», 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" и определяет состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации в государственном автономном профессиональном образовательном учреждении Самарской области «Тольяттинский машиностроительный колледж» (далее - ГАПОУ СО «ТМК», Учреждение).

2. СОСТАВ И СОДЕРЖАНИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

2.1. Имеющиеся в Учреждении ИСПДн имеют 3 и 4 уровень защищенности персональных данных, в соответствии с Актом определения уровня защищенности, для которых в ГАПОУ СО «ТМК» реализованы следующие меры касаемо использования СКЗИ:

а) организован режим обеспечения безопасности помещений, в которых размещены элементы ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения:

– входные двери в помещения ИСПДн оснащены замками;

– утвержден перечень помещений ИСПДн, в которых эксплуатируются СКЗИ;

– утвержден порядок доступа в помещения с СКЗИ;

– утвержден перечень пользователей СКЗИ и перечень лиц, имеющих доступ в помещения с ИСПДн и СКЗИ.

б) обеспечена сохранность носителей персональных данных и носителей, содержащих ключевую информацию:

- осуществлено хранение съемных машинных носителей в сейфах, в соответствии с Приказами об определении мест хранения материальных носителей ПДн с использованием и без использования средств автоматизации;

- осуществляется периодический контроль за целостностью печатей и замков и/или оттисков печатей при вскрытии сейфов с инсталлирующими СКЗИ носителями;

- осуществлен поэкземплярный учет машинных носителей путем ведения соответствующего журнала.

в) утвержден Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей, который поддерживается в актуальном состоянии администратором безопасности;

г) используется криптошлюз «С-Терра VPN» версия 4.3, исполнение 3-5 – С-Терра шлюз ST КС3, имеющий сертификаты ФСБ России: СКЗИ КС1, КС2, КС3 и ФСТЭК России: МЭ А4, Б4 и уровень доверия Минкомсвязь России (не принадлежит Учреждению).

2.2 По имеющимся ИСПДн в Учреждении разработаны и утверждены Модели угроз, в которых приведена Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведению атак.

2.3 Также приказом назначено должностное лицо, ответственное за обеспечение безопасности персональных данных в информационных системах и назначено ответственный пользователь СКЗИ, обладающие достаточными навыками в области информационной безопасности.

2.4 Помимо этого, разработан ряд документов, который направлен на обеспечение безопасности ПДн с использованием СКЗИ:

- приказ о защите СКЗИ в Учреждении;
- программа подготовки к самостоятельной работе с криптосредствами;
- проект теста по СКЗИ (по итогу самостоятельной подготовки по работке со СКЗИ);
- форма заключения о допуске к самостоятельной работке с СКЗИ;
- форма о возможности эксплуатации СКЗИ;
- форму журнала учета обучения пользователей СКЗИ;
- форма журнала учета хранилищ (сейфов) и ключей к ним;
- форма журнала поэкземплярного учета СКЗИ;
- форма технического (аппаратного) журнала;

- форма акта уничтожения СКЗИ;

- форма лицевого счета пользователя СКЗИ.

2.5 Пользователи СКЗИ ознакомлены с тем, что за нарушение порядка обращения с СКЗИ и/или несанкционированные действия в отношении СКЗИ виновные в этом лица несут ответственность (дисциплинарную, административную, материальную, уголовную) в зависимости от характера нарушения и тяжести наступивших отрицательных последствий.

РАЗРАБОТАНО:

Ведущий специалист по кадрам _____ Т.О.Медяшкина

СОГЛАСОВАНО:

Заместитель директора по учебно – производственной работе _____ С.А. Крюков

Юрисконсульт _____ Э.Н. Зайкова