УТВЕРЖДЕНО
приказом № 329 от «04» 06 2024
Директор ГАПОУ СО «ТМК»
И.А.Мочалов

П 370-2024

ПОЛОЖЕНИЕ
ОБ ОРГАНИЗАЦИИ РАБОТ СО СРЕДСТВАМИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННОМ АВТОНОМНОМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ САМАРСКОЙ ОБЛАСТИ «ТОЛЬЯТТИНСКИЙ МАШИНОСТРОИТЕЛЬНЫЙ КОЛЛЕДЖ»

Тольятти, 2024 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об организации работ со средствами криптографической защиты информации в государственном автономном профессиональном образовательном учреждении Самарской области «Тольяттинский машиностроительный колледж» разработано 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», федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», Приказом ФСБ России от 10.07.2014 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 определяет основные положения об организации работ со средствами криптографической защиты информации в государственном автономном профессиональном образовательном учреждении Самарской области «Тольяттинский машиностроительный колледж» (далее - ГАПОУ СО «ТМК», Учреждение).

2. ОСНОВНЫЕ ПОЛОЖЕНИЯ

2.1 В ГАПОУ СО «ТМК» должно быть назначено приказом лицо, ответственное за обеспечение безопасности эксплуатации средств криптографической защиты информации.

2.2 В Учреждении должны быть разработан документ, устанавливающий «Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведению

атак» и Модель угроз, в соответствии с которой должен быть определен необходимый класс СКЗИ для информационных систем персональных данных.

2.3 В зависимости от установленного класса СКЗИ, масштаба и структуры информационных систем должны использоваться СКЗИ сертифицированные по требованиям ФСБ России.

2.4 Охрана и организация режима в помещениях, в которых происходит обработка ПДн с помощью СКЗИ, должна исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

2.5 Должна быть разработана и утверждена необходимая документация, касающаяся использования СКЗИ:

– приказ о защите СКЗИ на объектах Учреждения;

– инструкция по применению и обращению с шифровальными (криптографическими) средствами защиты информации;

– правила доступа в помещения, в которых ведется эксплуатация и (или) хранение средств криптографической защиты информации, эксплуатационной и технической документации к ним;

– перечень помещений ГАПОУ СО «ТМК», в которых эксплуатируются СКЗИ;

– перечень лиц, имеющих право доступа в помещения ГАПОУ СО «ТМК», в которых эксплуатируются СКЗИ;

– состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием СКЗИ;

– перечень пользователей СКЗИ в ГАПОУ СО «ТМК»;

– программа подготовки пользователей 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 заключения о возможности эксплуатации СКЗИ;

– форма журнала учета обучения пользователей СКЗИ

– форма журнала поэкземплярного учета СКЗИ;

– форма журнала учета хранилищ (сейфов), металлических шкафов, спецхранилищ и ключей к ним;

– форма журнала учета лиц, допущенных к работе с СКЗИ;

– форма технического (аппаратного) журнала;

– форма акта уничтожения СКЗИ;

– форма лицевого счета пользователя СКЗИ;

– форма журнала учета ключей от помещений, в которых размещены СКЗИ.

2.6 Все пользователи ГАПОУ СО «ТМК», допущенные к работе с СКЗИ, должны ознакомиться с настоящей Инструкцией по работе с СКЗИ и Правилами доступа в помещения с СКЗИ и под роспись и строго выполнять требования документов. В случае компрометации ключевых носителей информации пользователь должен немедленно прекратить обработку персональных данных и обратиться к ответственному пользователю СКЗИ для дальнейших мероприятий.

2.7 Ответственный пользователь СКЗИ должен своевременно заполнять соответствующие журналы и акты, касаемо СКЗИ, а также проводить:

– регистрацию и учет СКЗИ, ключевых документов и эксплуатационной и технической документации к ним;

– выдачу СКЗИ, ключевых документов, эксплуатационной и технической документации к ним;

– при необходимости инсталляцию СКЗИ;

– контроль за эксплуатацией СКЗИ пользователями;

– служебную проверку по фактам нарушения правил эксплуатации СКЗИ;

– при необходимости деинсталляцию и уничтожение СКЗИ.

РАЗРАБОТАНО:

Ведущий специалист по кадрам _____ Т.О.Медяшкина

СОГЛАСОВАНО:

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

Юрисконсульт _____ Э.Н. Зайкова

ЛИСТ ОЗНАКОМЛЕНИЯ

с Положением об организации работ со СКЗИ в ГАПОУ СО «ТМК»

Ф.И.О.	Должность	Подпись, дата