УТВЕРЖДЕНО
приказом № 324 от « 04 » 06 2024
Директор ГАПОУ СО «ТМК»

И.А.Мочалов

П 365-2024

ПОЛОЖЕНИЕ
ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ГОСУДАРСТВЕННОМ АВТОНОМНОМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ САМАРСКОЙ ОБЛАСТИ «ТОЛЬЯТТИНСКИЙ МАШИНОСТРОИТЕЛЬНЫЙ КОЛЛЕДЖ»

Тольятти, 2024 г.

ОГЛАВЛЕНИЕ

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Положение об обеспечении безопасности персональных данных (далее – Положение) в информационных системах персональных данных (далее – ИСПДн) предназначено для организации и проведения мероприятий по обеспечению защиты персональных данных (далее – ПДн) в государственном автономном профессиональном образовательном учреждении Самарской области «Тольяттинский машиностроительный колледж» (далее – ГАПОУ СО «ТМК», Учреждение) в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», постановлением Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», 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», 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».

1.2. Настоящее Положение определяет порядок организации работ, требования, правила и рекомендации по обеспечению безопасности персональных данных (далее – ПДн) в ГАПОУ СО «ТМК».

1.3. Настоящее Положение является внутренним локальным актом ГАПОУ СО «ТМК» по вопросам обеспечения безопасности персональных данных, обрабатываемых в ГАПОУ СО «ТМК». Требования Положения обязательны для выполнения всеми работниками Учреждения, которые допущены к обработке персональных данных и реализуют мероприятия по защите персональных данных.

1.4. К другим основным внутренним локальным актам ГАПОУ СО «ТМК» по вопросам обеспечения безопасности персональных данных, обрабатываемых в ГАПОУ СО «ТМК», относятся:

1) Концепция информационной безопасности в ГАПОУ СО «ТМК»;

2) Политика ГАПОУ СО «ТМК»в отношении обработки и защиты персональных данных;

3) Положение об организации обработки персональных данных без использования средств автоматизации в ГАПОУ СО «ТМК»;

4) Положение об организации обработки персональных данных с использованием средств автоматизации в ГАПОУ СО «ТМК»;

5) Регламент присвоения прав доступа к ИСПДн ГАПОУ СО «ТМК»;

6) Инструкция ответственного за организацию обработки персональных данных;

7) Инструкция ответственному за обеспечение безопасности информации (Администратора безопасности);

8) Инструкция администратора ИСПДн ГАПОУ СО «ТМК»;

9) Инструкция пользователя ИСПДн ГАПОУ СО «ТМК»;

10) Инструкция по организации парольной защиты в ИСПДн;

11) Инструкция по проведению антивирусного контроля на объектах информатизации;

12) Инструкция по модификации программного обеспечения и технических средств информационных систем персональных данных;

13) Инструкция по организации резервного копирования;

14) Инструкция пользователю по действиям в случае возникновения нештатных ситуаций (инцидентов) на объектах информатизации;

15) Инструкция по применению и обращению с шифровальными (криптографическими) средствами защиты информации на объектах информатизации;

16) Инструкция по учету носителей персональных данных в ГАПОУ СО «ТМК».

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. Основные понятия, используемые в настоящем Положении:

– персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

– оператор персональных данных - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

– обработка персональных данных - любое действие (операция) или совокупность действий (операций) с персональными данными, совершаемых с использованием средств автоматизации или без их использования. Обработка персональных данных включает в себя в том числе сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

– автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники;

– распространение персональных данных - действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

– предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

– блокирование персональных данных - временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

– уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

– обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

– информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

- трансграничная передача персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Целью защиты ПДн является предотвращение возможной утечки информации и (или) несанкционированного и непреднамеренного изменения или разрушения ПДн.

3.2. Защита ПДн достигается выполнением комплекса организационных мероприятий и применением средств защиты информации от несанкционированного доступа, программно-математических воздействий с целью нарушения целостности (модификации, уничтожения) и доступности информации в процессе ее обработки, передачи и хранения, а также работоспособности технических средств.

3.3. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

3.4. Методы и способы защиты ПДн в информационных системах Учреждения устанавливаются Федеральной службой по техническому и экспортному контролю России и Федеральной службой безопасности России в пределах их полномочий.

3.5. Выбор методов, способов и средств защиты информации осуществляется в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю Российской Федерации, на основе определяемых угроз безопасности ПДн (модели угроз) и уровней защищенности персональных данных при их обработке в ИС.

3.6. Модель угроз разрабатывается на основе методических документов, принятых Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю Российской Федерации.

3.7. Выбранные и реализованные, в соответствии с настоящим Положением, методы и способы защиты информации в ИС должны обеспечивать нейтрализацию предполагаемых угроз безопасности ПДн при их обработке в ИС в составе создаваемой СЗИ.

3.8. Достаточность принятых мер по обеспечению безопасности ПДн при их обработке в ИС оценивается при проведении государственного контроля и надзора.

3.9. Все сотрудники ГАПОУ СО «ТМК», обрабатывающие ПДн и обеспечивающие защиту ПДн, должны быть ознакомлены с настоящим Положением под подпись.

4.ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ПОДЛЕЖАЩИЕ ЗАЩИТЕ

4.1. Персональные данные, подлежащие защите, утверждаются приказом директора ГАПОУ СО «ТМК» в виде «Перечня обрабатываемых персональных данных в ГАПОУ СО «ТМК».

4.2. Персональные данные, подлежащие защите в ГАПОУ СО «ТМК», обрабатываются без использования средств автоматизации, а также с использованием средств автоматизации, в ИСПДн.

4.3. Проверка соответствия состава обрабатываемых персональных данных осуществляется ежегодно в рамках проведения уполномоченными сотрудниками ГАПОУ СО «ТМК» мероприятий по контролю состояния защиты персональных данных в ГАПОУ СО «ТМК». Изменения, дополнения Перечня обрабатываемых персональных данных в ГАПОУ СО «ТМК», осуществляются ежегодно на основании информации, предоставляемой руководителями подразделений, в которых осуществляется обработка

персональных данных.

5.ОРГАНИЗАЦИОННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. В состав организационной системы обеспечения безопасности ПДн ГАПОУ СО «ТМК» входят:

– Директор ГАПОУ СО «ТМК»;

– Ответственный за организацию обработки персональных данных, назначенный приказом директора ГАПОУ СО «ТМК»;

– Администратор безопасности ИСПДн (далее - Администратор ИБ), на которого возложены функции ответственного за защиту информации, за проведение работ по технической защите информации и ответственного за обеспечение безопасности персональных данных при их обработке в ИСПДн «АРМ оператора ФИС ГИА и Приема», назначенный приказом директора ГАПОУ СО «ТМК»;

– Ответственный за обеспечение функционирования и безопасности криптосредств в объектах информатизации ГАПОУ СО «ТМК», назначенный приказом директора ГАПОУ СО «ТМК»;

– Администратор ИСПДн, назначенный назначаемый приказом директора ГАПОУ СО «ТМК»;

– Сотрудники ГАПОУ СО «ТМК», которые осуществляют обработку ПДн.

5.2. Общее руководство организацией работ по защите ПДн осуществляет директор ГАПОУ СО «ТМК».

5.3. Ответственный за организацию обработки персональных данных в ГАПОУ СО «ТМК» получает указания непосредственно от директора ГАПОУ СО «ТМК» и подотчетно ему. Обязанности ответственного за организацию обработки персональных данных в ГАПОУ СО «ТМК» определены в «Инструкции ответственного за организацию обработки персональных

данных».

5.4. Ответственный за организацию обработки персональных данных в ГАПОУ СО «ТМК», в рамках обеспечения безопасности ПДн выполняет следующие функции:

– организует процессы разработки, утверждения и корректировки локальных правовых актов ГАПОУ СО «ТМК» по обеспечению безопасности ПДн;

– доводит до сведения сотрудников ГАПОУ СО «ТМК» положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

– организует внутренний контроль за соблюдением сотрудниками ГАПОУ СО «ТМК» законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных.

5.5. Ответственный за организацию обработки персональных данных в ГАПОУ СО «ТМК» также осуществляет организацию работ по созданию системы защиты ПДн (далее – СЗПДн) и разработке организационно-распорядительных документов (далее – ОРД), регламентирующих вопросы обеспечения безопасности ПДн.

5.6. Администратор ИБ выполняет следующие функции:

– согласовывает изменения списка пользователей ИСПДн;

– осуществляет контроль настроек средств защиты информации в соответствии с изменениями в списке пользователей ИСПДн;

– осуществляет взаимодействие со структурными подразделениями ГАПОУ СО «ТМК», в том числе обеспечивает и обобщает предложения от подразделений по совершенствованию и реализации мероприятий по обеспечению безопасности ПДн в ИСПДн ГАПОУ СО «ТМК»;

– контролирует деятельность структурных подразделений ГАПОУ СО «ТМК» по выполнению ими установленных требований обеспечения безопасности ПДн в ИСПДн ГАПОУ СО «ТМК»;

– организует расследования по фактам разглашения или утечки персональных данных в ГАПОУ СО «ТМК».

5.7. Права и обязанности Администратора ИБ определены в «Инструкции администратора безопасности ИСПДн».

5.8. Администратор ИСПДн выполняет следующие функции:

– вносит изменения списка пользователей ИСПДн;

– осуществляет системное администрирование серверов, сетевого оборудования, администрирование прикладных систем ИСПДн, рабочих станций ИСПДн;

– осуществляет резервное копирование защищаемых информационных ресурсов;

– контролирует деятельность структурных подразделений ГАПОУ СО «ТМК» по выполнению ими установленных правил работы в ИСПДн ГАПОУ СО «ТМК»;

5.9. Права и обязанности Администратора ИСПДн определены в «Инструкции Администратора ИСПДн».

5.10. Ответственный за обеспечение функционирования и безопасности криптосредств в объектах информатизации ГАПОУ СО «ТМК» выполняет следующие функции:

– ведение Журнала поэкземплярного учета СКЗИ, эксплуатационной и технической документации к ним, ключевых документов;

– принятие СКЗИ, эксплуатационной и технической документации к ним, ключевых документов от пользователя при его увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ;

– осуществление периодической проверки журнала учета СКЗИ, перечня

пользователей СКЗИ и иных документов.

5.11. Руководители подразделений ГАПОУ СО «ТМК», сотрудникам которых предоставлен доступ к ПДн:

– формируют заявки на допуск пользователей к обработке ПДн в ИСПДн;

– обеспечивают выполнение мероприятий по защите ПДн в подразделениях ГАПОУ СО «ТМК»;

– готовят предложения в перечень персональных данных, в список сотрудников, допущенных в помещения, где ведется обработка ПДн и в список сотрудников, допущенных к работе в ИСПДн, предназначенных для выполнения функций подразделения.

5.12. Сотрудники ГАПОУ СО «ТМК», которым предоставлен доступ к обработке ПДн без использования средств автоматизации, реализуют организационные меры по обеспечению сохранности носителей ПДн и выполнению процедур по соблюдению требований законодательства.

5.13. Пользователи ИСПДн ГАПОУ СО «ТМК» реализуют требования безопасности информации, принятые для ИСПДн, исполняют установленные режимы защиты ПДн, обеспечивают строгое исполнение предписанных правил работы в ИСПДн. Права и обязанности пользователей ИСПДн определены в «Инструкции пользователя ИСПДн».

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБРАБОТКЕ БЕЗ ИСПОЛЬЗОВАНИЯ СРЕДСТВ АВТОМАТИЗАЦИИ

6.1. Требования к обеспечению безопасности персональных данных при их обработке без использования средств автоматизации установлены Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

6.2. Порядок обработки ПДн без использования средств автоматизации устанавливается в Положении об организации обработки персональных данных без использования средств автоматизации в ГАПОУ СО «ТМК».

6.3. Защита ПДн, обрабатываемых без использования средств автоматизации в ГАПОУ СО «ТМК», обеспечивается выполнением следующих мероприятий:

– определением мест хранения персональных данных (материальных носителей) и перечня лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ;

– обеспечением раздельного хранения персональных данных (материальных носителей), обработка которых осуществляется в различных целях в соответствии с Положением об организации обработки персональных данных в ГАПОУ СО «ТМК»;

– соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

6.4. Бумажные носители ПДн подлежат уничтожению по достижении целей обработки и/или в случае истечения их сроков хранения. Уничтожение носителей осуществляется по Акту, в соответствии с Инструкцией по уничтожению персональных данных в ГАПОУ СО «ТМК».

6.5. Бумажные носители ПДн постоянного срока хранения (свыше 5 лет) передаются в архив ГАПОУ СО «ТМК».

7. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

1) Определение требуемого уровня защищенности ИСПДн ГАПОУ СО «ТМК»;

2) Определение угроз безопасности персональных данных при их обработке в ИСПДн, формирование на их основе модели угроз;

3) Разработку модели нарушителя;

4) Разработку на основе модели угроз и модели нарушителя системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего уровня защищенности информационных систем;

5) Применение прошедших в установленном порядку процедуру оценки соответствия средств защиты информации;

6) Описание системы защиты персональных данных;

7) Установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

8) Обучение лиц, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;

9) Оценку эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

10) Установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

11) Учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, машинных носителей персональных данных;

12) Учет лиц, допущенных к работе с персональными данными в информационной системе;

13) Контроль за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных, включая контроль над соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

14) Разбирательство и составление заключений по фактам несоблюдения условий хранения машинных носителей персональных данных, некорректного использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;

15) Принятие мер в случае обнаружения фактов несанкционированного доступа к персональным данным;

16) Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

7.2. Определение уровня защищенности ИСПДн и моделирование угроз безопасности ПДн.

1) Определение уровня защищенности ИСПДн проводится в соответствии с «Требованиями к защите персональных данных при их обработке в информационных системах персональных данных», утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119).

2) Определение уровня защищенности ИСПДн проводит специальная Комиссия, состав которой утверждается приказом директора ГАПОУ СО «ТМК».

3) Результаты работы Комиссии утверждаются Актом определения уровня защищенности ИСПДн.

4) Уровень защищенности ИСПДн может быть пересмотрен:

– по решению Комиссии по определению уровня защищенности информационных систем персональных данных при изменении характеристик ИСПДн;

– по решению Комиссии по определению уровня защищенности информационных систем персональных данных, исходя из результатов проведенных мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

5) Уточнение и пересмотр уровня защищенности ИСПДн осуществляется в случае изменения:

– состава обрабатываемых ПДн в ИСПДн (изменении категории ПДн);

– количества обрабатываемых ПДн;

– типа актуальных угроз безопасности ПДн (угрозы наличия и использования недекларированных возможностей в системном или прикладном ПО).

6) Все имеющиеся и вводимые в эксплуатацию ИСПДн вносятся в перечень ИСПДн ГАПОУ СО «ТМК».

7) Модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных разрабатывается с использованием методических документов ФСТЭК России и (или) ФСБ России. Результаты определения и оценки актуальных угроз безопасности ПДн при их обработке в ИСПДн ГАПОУ СО «ТМК» утверждаются приказом директора ГАПОУ СО «ТМК».

8) Выявление угроз безопасности ПДн, реализуемых с применением программных и программно-аппаратных средств, осуществляется на основе метода экспертных оценок, в том числе путем опроса специалистов по информационным технологиям, персонала ИСПДн, при этом могут использоваться специальные инструментальные средства (сетевые сканеры) для

подтверждения наличия и выявления уязвимостей программного и аппаратного обеспечения ИСПДн. Для проведения опроса могут составляться специальные опросные листы.

9) Анализ актуальности моделей угроз безопасности ПДн должен проводиться в соответствии с Инструкцией по проведению контроля за состоянием обеспечения безопасности информации на объектах информатизации Учреждения.

10) Уточнение и пересмотр угроз безопасности ПДн при их обработке в ИСПДн осуществляется вне зависимости от проведения плановых проверок состояния защиты ПДн в случаях:

- изменения технологических процессов обработки ПДн;
- изменения состава средств защиты информации в ИСПДн;
- изменения характеристик ИСПДн, влияющих на уровень защищенности (наличие подключений к сетям общего пользования, тип ИСПДн и т.д.).

11) При необходимости применения (в случае передачи ПДн по незащищенным каналам связи) средств криптографической защиты информации для ИСПДн разрабатывается Модель нарушителя безопасности персональных данных на основе «Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных» ФСБ России. На основе такой модели нарушителя для ИСПДн определяется уровень криптографической защиты ПДн, которому должны соответствовать применяемые средства криптографической защиты.

7.3. Требования к обеспечению безопасности ПДн при их обработке в ИСПДн.

1) Безопасность ПДн при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных (СЗПДн),

включающей организационные меры и средства защиты информации, а также используемые в информационной системе информационные технологии.

2) Требования к СЗПДн разрабатываются на основе модели угроз и модели нарушителя и должны обеспечивать нейтрализацию предполагаемых актуальных угроз, выявленных по результатам моделирования. Требования формируются на основании методов и способов защиты информации для соответствующего класса информационных систем, задаваемых требованиями нормативных документов по защите ПДн ФСТЭК России и ФСБ России.

3) Методы и способы защиты персональных данных включают в себя:

– реализацию разрешительной системы допуска пользователей к информационным ресурсам, информационной системе и связанным с ее использованием работам, документам;

– разграничение доступа пользователей к информационным ресурсам, программным средствам обработки (передачи) и защиты информации;

– регистрацию действий пользователей, контроль несанкционированного доступа и действий пользователей, посторонних лиц;

– учет и хранение съемных носителей информации, их обращение, исключающее хищение, подмену и уничтожение;

– резервирование технических средств, дублирование массивов и носителей информации;

– использование сертифицированных средств защиты информации;

– использование защищенных каналов связи;

– размещение технических средств, позволяющих осуществлять обработку персональных данных, только в пределах охраняемой территории (рабочие станции, серверы, коммутационное оборудование, сетевые принтеры);

– организацию физической защиты помещений и технических средств, позволяющих осуществлять обработку персональных данных;

– предотвращение внедрения в информационные системы вредоносных программ (программ-вирусов) с использованием средств антивирусной защиты.

7.4. Разрешительная система допуска пользователей к информационным ресурсам.

1) Разграничение доступа к информационным ресурсам, содержащим ПДн, должно осуществляться в соответствии с «Положением о разрешительной системе доступа в ИСПДн», на основании должностных обязанностей сотрудников, допущенных к работе с персональными данными в ГАПОУ СО «ТМК». Список сотрудников ГАПОУ СО «ТМК», доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных, необходим для выполнения служебных обязанностей, утверждается приказом руководителя ГАПОУ СО «ТМК».

2) Допуск сотрудника к информационным ресурсам ИСПДн должен оформляться в виде заявки на регистрацию и/или предоставление доступа к сетевым ресурсам от руководителей структурных подразделений ГАПОУ СО «ТМК», согласованной с начальником подразделения ИТ и Администратором безопасности ИСПДн ГАПОУ СО «ТМК».

3) Согласованная заявка на допуск сотрудника к информационным ресурсам ИСПДн передается на исполнение в подразделение ИТ ГАПОУ СО «ТМК». Заявка должна храниться в подразделении ИТ ГАПОУ СО «ТМК» в течение всего срока эксплуатации ИСПДн.

4) Проверка соответствия пользователей ИСПДн, определенных в матрице доступа к ИСПДн, с имеющимися заявками на предоставление доступа сотрудников ГАПОУ СО «ТМК» к ИСПДн, осуществляется на периодической основе в соответствии с Инструкцией по проведению контроля за состоянием обеспечения безопасности информации на объектах информатизации Учреждения.

7.5. Регистрация действий пользователей.

1) Регистрация действий пользователей должна осуществляться средствами системного программного обеспечения и СЗИ ИСПДн.

2) Подлежат обязательной регистрации следующие операции, осуществляемые в ИСПДн:

– регистрация входа (выхода) пользователей в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова.

– регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;

– регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

– регистрация попыток доступа программных средств к дополнительным защищаемым объектам доступа.

7.6. Обеспечение безопасности при хранении носителей информации ПДн.

1) Подлежат учету следующие защищаемые носители ПДн:

– накопители на жестких магнитных дисках, установленные в серверы ИСПДн;

– накопители на жестких магнитных дисках, установленные в АРМ, на которых предусмотрено хранение ПДн;

– накопители для хранения резервных копий;

– внешние носители ПД (дискеты, компакт-диски, flash-накопители), на которых технологией обработки ПДн разрешается хранение или передача ПДн.

2) Учет защищаемых носителей информации должен осуществляться в Журналах учета носителей ПДн в соответствии с «Инструкцией по учету носителей персональных данных».

3) Обязанность по ведению учета внешних носителей ПДн (дискет, компакт-дисков, flash-дисков, на которые осуществляется кратковременное

хранение ПДн и/или передача их во внешние организации) возлагается на Администратора безопасности ИСПДн ГАПОУ СО «ТМК».

4) В случае смены владельца или назначения, списания и выведения из эксплуатации защищаемых носителей информации необходимо обеспечить уничтожение ПДн с носителей. Уничтожение информации с носителей информации должно осуществляться путем многократной записи информации на носители и/или путем физического уничтожения носителя.

7.7. Уничтожение же самих ПДн на носителях ПДн осуществляется в следующих случаях:

– при выявлении неправомерных действий с ПДн и в случае невозможности устранения допущенных нарушений, соответствующие ПДн уничтожаются в срок, не превышающий трех рабочих дней с даты такого выявления. Об устранении допущенных нарушений или об уничтожении ПДн руководитель соответствующего структурного подразделения Учреждения обязан в срок, не превышающий пяти рабочих дней с даты устранения допущенных нарушений или уничтожения ПДн, уведомить субъекта ПДн или его законного представителя, а в случае если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн - также указанный орган;

– в случае достижения цели обработки ПДн либо утраты необходимости в такой цели соответствующие ПДн уничтожаются в срок, не превышающий тридцати дней с даты достижения цели обработки ПДн, если иное не предусмотрено федеральными законами. Руководитель соответствующего структурного подразделения Учреждения обязан в срок, не превышающий пяти рабочих дней с даты уничтожения ПДн, уведомить об уничтожении ПДн субъекта ПДн или его законного представителя, а в случае если обращение или запрос были направлены уполномоченным органом по защите прав субъектов ПДн - также указанный орган;

– в случае отзыва субъектом ПДн согласия на обработку своих ПДн соответствующие ПДн уничтожаются в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между Учреждением и субъектом ПДн. Об уничтожении ПДн руководитель соответствующего структурного подразделения Учреждения обязан уведомить субъекта персональных данных в срок, не превышающий пяти рабочих дней с даты уничтожения ПДн.

5) По факту уничтожения носителя ПДн должен составляться соответствующий Акт, в порядке, предусмотренном в документе «Порядок обращения со съемными машинными носителями персональных данных».

7.8. Резервирование технических средств, дублирование массивов и носителей информации.

1) Обеспечение целостности и доступности ПДн, программных и аппаратных средств ИСПДн, а также средств защиты, при их случайной или намеренной модификации, должно осуществляться с помощью резервного копирования (дублирования массивов и носителей информации) обрабатываемых данных, резервирования элементов ИСПДн.

2) Для обеспечения целостности ИСПДн должны выполняться следующие мероприятия по резервированию:

– резервные копии информационных ресурсов, содержащих ПДн, должны храниться в специально выделенном месте, территориально отдаленном от места обработки самой информации;

– для обеспечения сохранности резервных копий должен быть применён комплекс организационных и физических мер защиты от НСД;

– носители, на которые осуществляется резервное копирование, должны регулярно проверяться на отсутствие механических повреждений, сбоев логической структуры, файловой системы;

– должны проводиться регулярные проверки процедур восстановления данных.

7.9. Использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия.

1) При защите ПДн используются СЗИ, сертифицированные в системах сертификации Федеральной службы по техническому и экспортному контролю и Федеральной службы безопасности Российской Федерации в пределах их полномочий.

2) При использовании средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия (сертификацию), должны выполняться следующие мероприятия:

– установка и ввод в эксплуатацию средств защиты информации осуществляется в соответствии с эксплуатационной и технической документацией сотрудниками сектора информационных технологий и организационно-документационного обеспечения ГАПОУ СО «ТМК»;

– проведение обучения работников ГАПОУ СО «ТМК», использующих средства защиты, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним. Форма журнала учета средств защиты информации, эксплуатационной и технической документации к ним утверждена соответствующим Приказом. Форма журнала учета средств криптографической защиты информации, эксплуатационной и технической документации к ним утверждена Приказом о защите СКЗИ;

– контроль Администратором ИБ соблюдения условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

– проведение Администратором ИБ периодического тестирования средств защиты в соответствии с эксплуатационной документацией на СЗИ.

Форма журнала проведения периодического тестирования СЗИ приведена в Приложении 1;

– проведение Администратором ИБ разбирательств и составление заключений по фактам несоблюдения условий использования средств защиты информации, которые могут привести к нарушению целостности, конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

7.10. Использование защищенных каналов связи.

1) При взаимодействии информационных систем с информационно-телекоммуникационными сетями международного информационного обмена (сетями связи общего пользования) основными методами и способами защиты информации от несанкционированного доступа являются:

– межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для скрытия структуры информационной системы;

– обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных;

– анализ защищенности информационных систем, предполагающий применение специализированных программных средств (сканеров безопасности);

– защита информации при ее передаче по каналам связи;

– использование средств антивирусной защиты;

– централизованное управление системой защиты персональных данных информационной системы.

2) Для обеспечения безопасности персональных данных при удаленном доступе к информационной системе через информационно-телекоммуникационную сеть международного информационного обмена

дополнительно должны применяться следующие основные методы и способы защиты информации от несанкционированного доступа:

– проверка подлинности отправителя (удаленного пользователя) и целостности передаваемых по информационно-телекоммуникационной сети международного информационного обмена данных;

– управление доступом к защищаемым персональным данным информационной сети.

3) Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных информационных систем через информационно-телекоммуникационную сеть международного информационного обмена должны применяться следующие основные методы и способы защиты информации от несанкционированного доступа:

– создание канала связи, обеспечивающего защиту передаваемой информации;

– осуществление аутентификации взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных.

7.11. Физическая защита помещений и технических средств.

1) Размещение ИСПДн и охрана помещений, в которых ведется работа с персональными данными, должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

2) Выполнение требований по исключению возможности неконтролируемого проникновения или пребывания в помещениях ИСПДн посторонних лиц реализуется осуществлением организационных и технических мер по созданию контролируемой зоны (КЗ) ГАПОУ СО «ТМК».

3) Границами КЗ могут являться:

– периметр охраняемой территории ГАПОУ СО «ТМК»;

– ограждающие конструкции охраняемого здания;

– стены помещений ГАПОУ СО «ТМК».

4) В состав КЗ должны входить

– помещения, в которых размещены рабочие станции, серверы, сетевое оборудование, входящие в состав ИСПДн;

– помещения, в которых проходят кабельные линии связи ИСПДн;

– помещения, в которых хранятся бумажные носители ПДн (архивы, помещения сотрудников ГАПОУ СО «ТМК»).

5) Размещение технических средств, обрабатывающих ПДн, должно осуществляться с учетом требования минимизации доступа в рабочие помещения лиц, не связанных с обработкой ПДн и обслуживанием оборудования.

6) Доступ посторонних лиц (посетителей, работников обслуживающих организаций) в контролируемую зону в рабочее время осуществляется только в сопровождении работников ГАПОУ СО «ТМК».

7) Размещение устройств отображения и печати информации, используемых в составе ИСПДн, должно осуществляться с учетом максимального затруднения визуального просмотра информации посторонними лицами.

8) Серверы и коммуникационное оборудование ИСПДн должны располагаться в отдельном помещении или в металлических шкафах с прочной запираемой дверью. Ключи от дверей помещений и шкафов должны быть только у лиц, имеющих право доступа в них.

9) В нерабочее время доступ в контролируемую зону должен быть исключен следующими мерами:

– заключением договора с охранным предприятием, обязательными условиями которого являются следующие обязанности охранного предприятия:

- организация и обеспечение контроля доступа в здание Учреждения работников и посетителей в рабочее время;
- организация и обеспечение охраны помещений в нерабочее время, а также в выходные и праздничные дни (при необходимости использования помещений в указанное время, допуск в помещения осуществляется по письменной заявке ответственным лицом).

– в случае отсутствия возможности заключения договора с охранным предприятием для реализации мер по охране контролируемой зоны в нерабочее время необходимо выполнять следующие требования:

- на всех остекленных проемах первого и последнего этажа должны быть установлены металлические решетки или ставни с запорами;
- двери в помещения контролируемой зоны должны быть металлическими, с надежными замками;
- хранение ключей осуществляется назначенным приказом руководителя ГАПОУ СО «ТМК» ответственным лицом с выдачей под роспись сотрудникам ГАПОУ СО «ТМК» в случае необходимости.

7.12. Использование средств антивирусной защиты.

1) Средства антивирусной защиты предназначены для реализации следующих функций:

– антивирусное сканирование;

– блокирование вредоносных программ;

– автоматизированное обновление антивирусных баз;

– ограничение прав пользователя на изменение настроек антивирусного программного обеспечения;

– автоматический запуск сразу после загрузки операционной системы.

2) Подсистема антивирусной защиты реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

3) Обо всех случаях сбоев антивирусного программного обеспечения (появления сообщений об ошибках) пользователь должен немедленно уведомлять Администратора ИБ.

7.13. Порядок разработки, ввода в действие и эксплуатации СЗПДн.

1) Требования по защите ПДн для каждой ИСПДн должны формироваться в виде Технического задания на создание СЗПДн в ИСПДн на этапе разработки (модернизации) ИСПДн.

2) Требования должны формироваться на основании положений руководящих документов ФСТЭК России и ФСБ России.

3) Для вновь создаваемых ИСПДн, а также для функционирующих ИСПДн, не включающих в себя СЗПДн проводятся следующие мероприятия:

– обследование ИСПДн и разработка технического (частного технического) задания на создание СЗПДн;

– проектирование и реализация ИСПДн и СЗПДн в её составе;

– ввод в действие СЗПДн, включающее опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации.

4) Для функционирующих ИСПДн, включающих в себя СЗПДн, доработка (модернизация) СЗПДн должна проводиться в случае, если:

– изменился состав обрабатываемых ПДн;

– изменился состав или структура самой ИСПДн или технические особенности ее построения (изменился состав или структура программного обеспечения, технических средств обработки ПДн, топологии ЛВС ИСПДн) или технологический процесс обработки ПДн, вследствие которого произошли изменения в структуре ИСПДн;

– изменился состав угроз безопасности ПДн в ИСПДн;

– изменился уровень защищенности ИСПДн.

7.14. Порядок оценки эффективности принимаемых мер по обеспечению безопасности ПДн в период эксплуатации ИСПДн выполняется в соответствии с «Инструкцией по проведению контроля за состоянием обеспечения безопасности информации на объектах информатизации ГАПОУ СО «ТМК», а также на основании доказательств, полученных с участием привлеченных организаций (внешний аудит), имеющих необходимые лицензии ФСТЭК РФ и ФСБ РФ.

8.ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. При вступлении в должность нового сотрудника непосредственный руководитель структурного подразделения ГАПОУ СО «ТМК», в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими порядок обработки и обеспечения защиты ПДн. Администратор ИБ обучает навыкам выполнения процедур, необходимых для работы в ИСПДн ГАПОУ СО «ТМК» и выполнения требований по защите ПДн в ИСПДн.

8.2. Сотрудники ГАПОУ СО «ТМК» должны соблюдать установленные организационно-распорядительными документами требования по режиму обработки персональных данных, учету, хранению, передаче носителей информации и обеспечению безопасности ПДн.

8.3. Сотрудники ГАПОУ СО «ТМК» должны быть проинформированы об ответственности за нарушение требований по обеспечению безопасности ПДн на момент заключения трудового договора с ГАПОУ СО «ТМК» специалистами подразделения по работе с персоналом (кадрами).

9.КОНТРОЛЬ ЗА ПРИНИМАЕМЫМИ МЕРАМИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Целью контроля состояния защиты является своевременное выявление и предотвращение утечки информации.

9.2. Контроль состояния защиты ПДн в ГАПОУ СО «ТМК» должен осуществляться ежегодно, в соответствии с утвержденным Планом внутренних проверок состояния защиты персональных данных.

9.3. Проведение контроля состояния защиты включает в себя мероприятия по оценке:

– соблюдения требований руководящих и нормативно-методических документов по защите ПДн;

– работоспособности применяемых средств защиты информации в соответствии с их эксплуатационной документацией;

– знания и выполнения персоналом своих функциональных обязанностей в части защиты ПДн.

9.4. Проверка проводится дополнительно при изменении состава технических средств и систем, условий обработки информации, содержащей ПДн.

10. ПРИНЯТИЕ МЕР В СЛУЧАЕ ОБНАРУЖЕНИЯ ФАКТОВ НАРУШЕНИЯ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ (НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ПДн), РАЗБИРАТЕЛЬСТВО И СОСТАВЛЕНИЕ ЗАКЛЮЧЕНИЙ ПО ФАКТАМ НАРУШЕНИЯ ТРЕБОВАНИЙ БЕЗОПАСНОСТИ

10.1. Лицо, обнаружившее факт нарушения требований, незамедлительно уведомляет Администратора ИБ о факте нарушения.

10.2. В случаях обнаружения нарушений при обработке ПДн в ИСПДн необходимо:

– немедленно прекратить обработку ПДн в ИСПДн, где обнаружены нарушения и принять меры к их устранению;

– организовать расследование причин и условий появления нарушений с целью недопущения их в дальнейшем;

– разработать план мероприятий по устранению нарушений.

10.3. Возобновление работ разрешается только после выполнения мероприятий по устранению нарушений и проверки достаточности и эффективности принятых мер.

11.ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ

11.1. Настоящее Положение пересматривается раз в пять лет и в случае изменения законодательства в области защиты ПДн.

11.2. Все изменения и дополнения в настоящее Положение вносятся приказом директора ГАПОУ СО «ТМК».

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 обеспечении безопасности персональных данных ГАПОУ СО «ТМК»

№ п/п	Фамилия, инициалы сотрудника	Должность	Подпись, дата

Приложение 1
к Положению об обеспечении
безопасности ПДн

Журнал периодического тестирования средств защиты информации

Журнал начат «____» _____
202__ г.

Должность, подразделение

_____ / ФИО должностного лица /

Журнал завершен «____» _____
202__ г.

Должность, подразделение

_____ / ФИО должностного лица /

№ п/п	Наименование СЗИ/СКЗИ	Регистрационные номера СЗИ/СКЗИ	Дата проведения тестирования	ФИО и подпись проводившего тестирование	Вид теста и используемые средства для его проведения	Результат тестирования (успешный/неуспешный), примечания	Дата проведения следующего тестирования