УТВЕРЖДЕНО
приказом № 323 от 04.06.2024
Директор ГАПОУ СО «ТМК»
И.А.Мочалов

П 364-2024

ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ В ГОСУДАРСТВЕННОМ АВТОНОМНОМ ПРОФЕССИОНАЛЬНОМ ОБРАЗОВАТЕЛЬНОМ УЧРЕЖДЕНИИ САМАРСКОЙ ОБЛАСТИ «ТОЛЬЯТТИНСКИЙ МАШИНОСТРОИТЕЛЬНЫЙ КОЛЛЕДЖ»

Тольятти, 2024 г.

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение об организации обработки персональных данных с использованием средств автоматизации (далее - Положение) определяет цели, содержание и порядок автоматизированной обработки персональных данных, меры, направленные на защиту персональных данных (далее – ПДн), обрабатываемые в государственном автономном профессиональном образовательном учреждении Самарской области «Тольяттинский машиностроительный колледж» (далее – Учреждение, Оператор).

1.2. Положение разработано 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 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации», Политикой ГАПОУ СО «ТМК» в отношении обработки и защиты персональных данных (далее - Политика), а также иными нормативно-правовыми актами в сфере защиты персональных данных, действующими на территории Российской Федерации.

2 ПОРЯДОК ИСПОЛЬЗОВАНИЯ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Обработка ПДн, осуществляемая с использованием средств автоматизации Учреждением, основана на следующих принципах:

– законности и справедливой основы;

– ограничения обработки персональных данных достижением конкретных, заранее определенных и законных целей;

– недопущения обработки персональных данных, несовместимой с целями сбора персональных данных;

– недопущения объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой;

– обработки только тех персональных данных, которые отвечают целям их обработки;

– соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки;

– недопущения обработки персональных данных, избыточных по отношению к заявленным целям их обработки;

– обеспечения точности, достаточности и актуальности персональных данных по отношению к целям обработки персональных данных;

– хранение персональных данных должно осуществляться в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

– уничтожения либо обезличивания персональных данных по достижении целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения Учреждением допущенных нарушений персональных данных, если иное не предусмотрено федеральным законом.

2.2. Обработка персональных данных в ГАПОУ СО «ТМК» может осуществляться исключительно в тех целях, которые указаны в Политике.

2.3. При определении объема и содержания обрабатываемых персональных данных работники ГАПОУ СО «ТМК» должны

руководствоваться Политикой с учетом действующего законодательства Российской Федерации, а также настоящим Положением.

2.3. Обработка ПДн с использованием средств автоматизации (автоматизированным способом) может осуществляться исключительно на автоматизированных рабочих местах.

2.4. Перечень нормативно-правовых актов, определяющих основания обработки персональных данных в ГАПОУ СО «ТМК» определяется Политикой.

3 ПОРЯДОК ХРАНЕНИЯ И ПЕРЕДАЧИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Персональные данные субъектов ПДн у Оператора содержатся в том числе и в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в том числе и базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

3.2. Конкретные обязанности по работе с информационными системами персональных данных и материальными носителями информации, в том числе с документами, содержащими персональные данные субъектов ПДн, возлагаются на сотрудников Оператора и закрепляются в должностных инструкциях.

3.3. Работа в информационных системах персональных данных, материальными носителями, в том числе с документацией, содержащими персональные данные Клиентов, осуществляется в специально отведённых для этого помещениях.

3.4. Перечень лиц, имеющих право доступа к персональным данным субъектов ПДн и обработке их ПДн, определяется приказом директора Оператора.

3.5. С лицами, допущенными к обработке персональных данных Клиентов, заключается Соглашение о неразглашении и вносятся соответствующие изменения в трудовой договор с ними.

3.6. Оператор при создании и эксплуатации информационных систем персональных данных (далее - ИСПДн) субъектов ПДн с использованием средств автоматизации обеспечивает проведение определения уровня защищенности ПДн в ИСПДн в установленном порядке.

3.7. Оператор при создании и эксплуатации системы защиты персональных данных ИСПДн с использованием средств автоматизации и без использования средств автоматизации принимает все необходимые организационные и технические меры, обеспечивающих выполнение установленных действующим законодательством требований к обработке персональных данных.

3.8. Оператор по достижении целей обработки персональных данных обязан прекратить обработку этих персональных данных и обеспечить их уничтожение в установленном порядке.

3.9. В целях соблюдения законодательства Российской Федерации для достижения целей обработки, а также в интересах и с согласия субъектов персональных данных, ГАПОУ СО «ТМК» в ходе своей деятельности может предоставлять ПДн организациям, перечисленным в Политике.

4 ОБЕЗЛИЧИВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ. УСЛОВИЯ И СПОСОБЫ ОБЕЗЛИЧИВАНИЯ

4.1. Обезличивание персональных данных может быть проведено с целью ведения статистических данных, снижения ущерба от разглашения защищаемых персональных данных, снижения класса используемых информационных систем персональных данных и по достижению сроков обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законодательством Российской Федерации.

4.2. К способам обезличивания персональных данных при условии дальнейшей обработки персональных данных относятся:

1) уменьшение перечня обрабатываемых сведений;

2) замена части сведений идентификаторами;

3) обобщение (понижение) точности некоторых сведений;

4) деление сведений на части и обработка их в разных информационных системах;

5) другие способы.

4.3. К способам обезличивания персональных данных в случае достижения целей обработки или в случае утраты необходимости в достижении этих целей является сокращение перечня персональных данных.

4.4. Правила работы с обезличенными данными:

– Обезличенные персональные данные не подлежат разглашению и нарушению конфиденциальности.

– Обезличенные персональные данные могут обрабатываться с использования и без использования средств автоматизации.

– При обработке обезличенных персональных данных с использованием средств автоматизации необходимо:

1) использование паролей;

2) использование антивирусных программ;

3) соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных.

– При обработке обезличенных персональных данных без использования средств автоматизации необходимо соблюдение:

1) хранения бумажных носителей в условиях, исключающих доступ к ним посторонних лиц;

2) соблюдение правил доступа в помещение, в котором ведётся обработка персональных данных.

5 ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ, ОСУЩЕСТВЛЯЕМОЙ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ АВТОМАТИЗАЦИИ

5.1. Защита персональных данных должна вестись по трём взаимодополняющим направлениям:

5.1.1. Проведение организационных мероприятий:

– разработка и внедрение внутренних организационно-распорядительных документов, регламентирующих обработку и защиту персональных данных субъектов, в том числе порядок доступа в помещения и к персональным данных;

– ознакомление работников с законодательством РФ и внутренними нормативными документами, получение обязательств, касающихся обработки персональных данных;

– организация учета носителей персональных данных;

– разработка модели угроз безопасности персональных данных;

– проведение инструктажа работников по вопросам защиты персональных данных;

– проведение аттестации по требованиям информационной безопасности или проведение оценки эффективности принятых мер по обеспечению безопасности ПДн в ИСПДн.

5.1.2. Программная и программно-аппаратная защита:

– внедрение программных и программно-аппаратных средств защиты информации в соответствии с нормативными документами ФСТЭК России и ФСБ России.

5.1.3. Инженерно-техническая защита:

– установка сейфов или запирающихся шкафов для хранения носителей персональных данных;

– выделение отдельных помещений с возможной системой контроля доступа, в которых находятся элементы объектов ИСПДн, с установленной сигнализацией, с возможной установкой видеонаблюдения;

– организация режима охраны здания.

6 ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДН

6.1. Состав ИСПДн ГАПОУ СО «ТМК» определяется соответствующим Перечнем ИСПДн ГАПОУ СО «ТМК», утвержденного приказом.

6.2. Безопасности ПДн достигается путем исключения несанкционированного, в том числе и случайного, доступа к ПДн, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий.

6.3. Средства защиты информации, применяемые в ИСПДн, в обязательном порядке проходят процедуру оценки соответствия в установленном законодательством Российской Федерации порядке.

6.4. Обмен ПДн при их обработке в ИСПДн осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер, а также применения технических и (или) программных средств.

6.5. Организация режима обеспечения безопасности помещений, в которых размещены элементы ИСПДн, должна исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

6.6. Безопасность ПДн при их обработке в ИСПДн обеспечивает специалист, ответственный за обеспечение безопасности ПДн в информационных системах.

6.7. При обработке ПДн в информационной системе должно быть обеспечено:

– проведение мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;

– своевременное обнаружение фактов несанкционированного доступа к ПДн;

– недопущения воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;

– возможность незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

– постоянный контроль надо обеспечением уровня защищенности персональных данных при их обработке в ИСПДн.

6.8. Мероприятия по обеспечению безопасности ПДн при их обработке в информационных системах включают:

– определение угроз безопасности ПДн при их обработке в ИСПДн, формирование на их основе модели угроз;

– разработку на основе модели угроз системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса информационных систем;

– проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

– установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

– использование защищенных каналов связи;

– предотвращение внедрения в ИСПДн вредоносных программ и закладок;

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

– использование средств антивирусной защиты;

– обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

– учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;

– учет лиц, допущенных к работе с персональными данными в информационной системе;

– контроль по соблюдению условий использования средств защиты информации, предусмотренных эксплуатационной и технической документации;

– разбирательство и составление заключений по фактам несоблюдения условий хранения носителей ПДн, использования средств защиты информации, которые могут привести к нарушению конфиденциальности ПДн или другим нарушениям, приводящим к снижению уровня защищенности ПДн, разработку и принятие мер и предотвращению возможных опасных последствий подобных нарушений;

– описание системы защиты персональных данных.

6.9. Иные требования по обеспечению безопасности информации и средств защиты информации в ГАПОУ СО «ТМК» выполняются в соответствии с требованиями федеральных органов исполнительной власти и органов исполнительной власти субъекта Российской Федерации, в котором находится Оператор.

7 ПОРЯДОК УНИЧТОЖЕНИЯ ОБРАБОТАННЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. Под уничтожением обработанных персональных данных понимаются действия, в результате которых невозможно восстановить содержание

персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

7.2. В случае достижения цели обработки персональных данных оператор обязан прекратить обработку персональных данных или обеспечить ее прекращение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

7.3. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных оператор обязан прекратить их обработку или обеспечить прекращение такой обработки (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные или обеспечить их уничтожение (если обработка персональных данных осуществляется другим лицом, действующим по поручению оператора) в срок, не превышающий тридцати дней с даты поступления указанного отзыва, если иное не предусмотрено договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных, иным соглашением между оператором и субъектом персональных данных либо если оператор не вправе осуществлять обработку персональных данных без согласия

субъекта персональных данных на основаниях, предусмотренных настоящим Федеральным законом или другими федеральными законами.

7.4. Уничтожение обработанных персональных данных производится комиссионно и если используются какие-либо средства автоматизации (компьютеры, ноутбуки, планшеты, мобильные средства и т.д.) или смешанная обработки, то документами, подтверждающими уничтожение персональных данных субъектов, являются (в соответствии с приказом Роскомнадзора «Об утверждении Требований к подтверждению уничтожения персональных данных» от 28 октября 2022 г. №179):

- Акт об уничтожении персональных данных;

- Выгрузка из журнала регистрации событий в информационной системе персональных данных.

7.5. Если в выгрузке из журнала невозможно указать какие-то сведения, их можно отразить в акте. В таком случае подтверждением будут оба способа, независимо от способа обработки ПДн.

7.6. Если средства автоматизации не используются, то подтверждением будет только акт об уничтожении ПДн.

7.7. Акт об уничтожении персональных данных должен содержать:

а) наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица) и адрес оператора;

б) наименование (юридического лица) или фамилию, имя, отчество (при наличии) (физического лица), адрес лица (лиц), осуществляющего (осуществляющих) обработку персональных данных субъекта (субъектов) персональных данных по поручению оператора (если обработка была поручена такому (таким) лицу (лицам);

в) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

г) фамилию, имя, отчество (при наличии), должность лиц (лица), уничтоживших персональные данные субъекта персональных данных, а также их (его) подпись;

д) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

е) наименование уничтоженного материального (материальных) носителя (носителей), содержащего (содержащих) персональные данные субъекта (субъектов) персональных данных, с указанием количества листов в отношении каждого материального носителя (в случае обработки персональных данных без использования средств автоматизации);

ж) наименование информационной (информационных) системы (систем) персональных данных, из которой (которых) были уничтожены персональные данные субъекта (субъектов) персональных данных (в случае обработки персональных данных с использованием средств автоматизации);

з) способ уничтожения персональных данных;

и) причину уничтожения персональных данных;

к) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

7.8. Акт об уничтожении персональных данных в электронной форме, подписанный в соответствии с законодательством РФ, признается электронным документом, равнозначным акту об уничтожении персональных данных на бумажном носителе, подписанному собственноручной подписью лиц, указанных в подпункте "г".

7.9. Акт об уничтожении персональных данных и выгрузка из журнала подлежат хранению в течение 3 лет с момента уничтожения персональных данных.

7.10. Выгрузка из журнала должна содержать:

а) фамилию, имя, отчество (при наличии) субъекта (субъектов) или иную информацию, относящуюся к определенному (определенным) физическому (физическим) лицу (лицам), чьи персональные данные были уничтожены;

б) перечень категорий уничтоженных персональных данных субъекта (субъектов) персональных данных;

в) наименование информационной системы персональных данных, из которой были уничтожены персональные данные субъекта (субъектов) персональных данных;

г) причину уничтожения персональных данных;

д) дату уничтожения персональных данных субъекта (субъектов) персональных данных.

8 ОТВЕТСТВЕННОСТЬ

8.1. Ответственность за соблюдение требований по защите информации ограниченного доступа и надлежащего порядка проводимых работ возлагается на пользователей ИСПДн, ответственного за обеспечение безопасности ПДн в информационных системах и ответственного за организацию обработки ПДн в ГАПОУ СО «ТМК».

8.2. Работники ГАПОУ СО «ТМК», виновные в нарушении норм, регулирующих получение, обработку и защиту ПДн субъекта, несут дисциплинарную, административную, гражданско-правовую и уголовную ответственность в соответствии с законодательством РФ.

8.3. Разглашение ПДн субъекта (передача их посторонним лицам, в том числе другим работникам, не имеющим к ним допуск), их публичное раскрытие, утрата документов и иных носителей, содержащих ПДн субъекта, а также иные нарушения обязанностей по их защите и обработке, установленных настоящим Положением, локальными нормативно-правовыми актами ГАПОУ СО «ТМК», влечет наложение на работника, имеющими доступ к ПДн, дисциплинарных взысканий в виде: замечания, выговора, увольнения. Работник ГАПОУ СО «ТМК», имеющий доступ к ПДн субъекта и совершивший указанный дисциплинарный проступок, несет полную материальную ответственность в случае причинения его действиями ущерба ГАПОУ СО

«ТМК» (в соответствии с п.7 ст. 243 Трудового кодекса Российской Федерации).

8.4. В отдельных случаях, при разглашении персональных данных, работник, совершивший указанный проступок, несет ответственность в соответствии со ст. 13.14 Кодекса об административных правонарушениях Российской Федерации.

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 обработки персональных данных

с использованием средств автоматизации ГАПОУ СО «ТМК»

Ф.И.О.	Должность	Подпись, дата