

УТВЕРЖДАЮ

**Директор ГОБПОУ «Липецкий
машиностроительный колледж»**

А.М. Гончаров

Приказ № 691 от «10» ноября 2017г.



ПРАВИЛА

обработки конфиденциальной информации, в том числе персональных данных

1. Общие положения

1.1. Настоящие правила обработки конфиденциальной информации, в том числе персональных данных (далее – КИ), устанавливают единый порядок обработки КИ в ГОБПОУ «Липецкий машиностроительный колледж».

1.2. Настоящие правила разработаны на основании и в соответствии с требованиями следующих законодательных и нормативных правовых актов Российской Федерации:

- Трудовой кодекс Российской Федерации (ст. 65, ст.85-90);
- Гражданский кодекс Российской Федерации, Часть 1 (ст. ст. 150, 152, 152.1) от 30.11.1994 №51-ФЗ;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ);
- Постановление Правительства Российской Федерации от 21 марта 2012 года № 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;
- Постановление Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Постановление Правительства Российской Федерации от 01 ноября 2012 года

№ 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

- Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- Приказ ФСБ России от 10 июля 2014 г. N 378 «Об утверждении Состав 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».

1.3. Настоящие правила устанавливают и определяют:

1) процедуры, направленные на выявление и предотвращение нарушений законодательства Российской Федерации в сфере обработки и защиты КИ;

2) цели обработки КИ;

3) содержание обрабатываемой КИ для каждой цели обработки КИ;

4) категории субъектов, персональные данные (далее – ПДн) которых обрабатываются;

5) сроки обработки и хранения обрабатываемой КИ;

6) порядок уничтожения обработанной КИ при достижении целей обработки или при наступлении иных законных оснований.

1.4. Основные понятия и термины, используемые в настоящих Правилах, применяются в значениях, определенных Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» и Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

1.5. ГОБПОУ «Липецкий машиностроительный колледж» (далее – Организация или Оператор) является оператором персональных данных, осуществляющим обработку ПДн сотрудников, студентов и их родителей или законных представителей.

1.6. Доступ к Правилам неограничен, так как Правила являются документом, определяющим политику Оператора в отношении обработки конфиденциальной

информации, в том числе ПДн.

1.7. Правила являются обязательными для исполнения всеми сотрудниками Организации, имеющими доступ к КИ.

1.8. Правила вступает в силу с момента их утверждения и действуют до замены их новыми Правилами.

2. Процедуры, направленные на выявление и предотвращение нарушений, предусмотренных законодательством Российской Федерации в сфере конфиденциальной информации, в том числе персональных данных

2.1. Оператор при обработке КИ должен руководствоваться принципами и условиями определенными нормами главы 2 Федерального закона №152-ФЗ.

2.2. Права субъектов ПДн определены в главе 3 Федерального закона №152-ФЗ.

2.3. При определении обязанностей Оператора при сборе КИ и при обращении к нему субъектов ПДн Оператор должен руководствоваться главой 4 Федерального закона №152-ФЗ.

2.4. Оператор должен принимать меры направленные на обеспечение выполнения обязанностей предусмотренных Федеральным законом №152-ФЗ, в частности:

- назначить ответственного за организацию обработки КИ в Организации;

- издать:

- документы, определяющие политику Оператора в отношении обработки КИ;
- локальные акты по вопросам обработки КИ;
- локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- применять правовые, организационные и технические меры по обеспечению безопасности КИ, в соответствии со статьей 19 Федерального закона №152-ФЗ «О персональных данных» и Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

- осуществлять внутренний контроль и (или) аудит соответствия обработки ПДн Федеральному закону №152-ФЗ «О персональных данных» и принятым в

соответствии с ним нормативным правовым актам, требованиям к защите КИ, политике оператора в отношении обработки КИ, локальным актам оператора;

- оценивать вред, который может быть причинён субъектам ПДн в случае нарушения законодательства Российской Федерации и настоящих Правил;

- ознакомить работников, непосредственно осуществляющих обработку КИ, с положениями законодательства Российской Федерации о ПДн, требованиями к защите КИ и настоящими Правилами;

- запрещать обработку КИ лицами, не допущенными к их обработке.

2.5. Обработка КИ должна осуществляться после получения согласия субъекта ПДн (за исключением случаев, предусмотренных частью 2 статьи 6 Федерального закона №152-ФЗ «О персональных данных»), при условии выполнения требований к защите КИ.

2.6. Безопасность КИ, при её обработке в информационных системах (далее – ИС), обеспечивает Оператор.

2.7. При обработке КИ необходимо соблюдать следующие требования:

- к работе с КИ допускаются только лица, назначенные соответствующим распоряжением руководителя Организации.

- в целях обеспечения сохранности документов, содержащих КИ, все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться сотрудниками Организации, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных регламентах (инструкциях);

- на период обработки защищаемой информации в помещении могут находиться только лица, допущенные в установленном порядке к обрабатываемой информации.

2.8. Особенности обработки КИ с использованием средств автоматизации

2.8.1. Обработка КИ с использованием средств автоматизации осуществляется в ИС, состав которых должен быть определен в Перечне информационных систем.

2.8.2. Машинные носители КИ должны подлежать обязательной регистрации и учету, в соответствии с Приказом Организации, регламентирующим порядок учета и хранения носителей.

2.8.3. Обработка КИ должна осуществляться при условии выполнения требований к защите ПДн, утвержденных постановлением Правительства от

01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказом ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2.8.4. Оператор при обработке КИ обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты КИ от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения КИ, а также от иных неправомерных действий в отношении КИ. Состав и содержание таких мер утвержден приказом ФСТЭК России от 11.02.2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2.9. Особенности обработки ПДн без использования средств автоматизации

2.9.1. Особенности обработки ПДн, осуществляемой без использования средств автоматизации, изложены в постановлении Правительства Российской Федерации от 15.09.2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» (Приложение № 1).

2.9.2. Особенности организации обработки ПДн, осуществляемой без использования средств автоматизации:

- ПДн при их обработке должны обособляться от иной информации, в частности, путем фиксации их на отдельных носителях;

- при фиксации ПДн на материальных носителях не допускается фиксация на одном материальном носителе ПДн, цели обработки которых заведомо несовместимы;

- для обработки различных категорий ПДн для каждой категории ПДн должен использоваться отдельный материальный носитель;

- лица, осуществляющие обработку ПДн, должны быть проинформированы о факте обработки ими ПДн, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых ПДн, а также об особенностях и правилах осуществления такой обработки, установленных

нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации;

- требования к типовым формам документов, характер информации в которых предполагает или допускает включение в них ПДн, изложены в п. 7 «Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденного постановлением Правительства от 15.09.2008 года № 687;

- уточнение ПДн производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными ПДн.

2.9.3. Меры по обеспечению безопасности ПДн при их обработке, осуществляемой без использования средств автоматизации:

- обработка ПДн должна осуществляться таким образом, чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн (материальных носителей) и установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ;

- необходимо обеспечивать раздельное хранение ПДн (материальных носителей), обработка которых осуществляется в различных целях;

- при хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный к ним доступ.

3. Цели обработки конфиденциальной информации, в том числе персональных данных

3.1. Цель обработки КИ определяется целями создания и видами деятельности образовательного учреждения, а именно:

- обеспечение соблюдения законов и иных нормативных правовых актов в связи с осуществлением деятельности в соответствии с Уставом Оператора, оказанием государственных и муниципальных услуг в сфере образования;

- заполнение и использование баз данных автоматизированных

информационных систем бухгалтерского учета, персонифицированного учета, кадрового учёта, налогового учета в целях повышения эффективности, быстрого поиска, формирования отчётов;

- организация учебного процесса, учёт контингента обучающихся;
- формирование и ведение государственных информационных систем в сфере образования.

3.2. Субъектами, персональные данные которых обрабатываются для указанных целей, являются сотрудники, студенты и их родители или законные представители.

4. Содержание обрабатываемой конфиденциальной информации, в том числе персональных данных

4.1. Содержание обрабатываемой КИ должно определяться целью обработки КИ и утверждаться локальным актом Оператора (Перечень конфиденциальной информации, в том числе персональных данных, обрабатываемой в организации в связи с реализацией трудовых отношений, а также в связи с оказанием услуг).

4.2. Содержание обрабатываемых персональных данных определяется для каждой цели обработки персональных данных.

5. Категории субъектов, персональные данные которых обрабатываются:

- 1) сотрудники Оператора, состоящие с ним в трудовых отношениях.
- 2) не сотрудники Оператора, обратившиеся в Организацию по вопросам, касающимся установленной сферы ее деятельности.

6. Сроки обработки и хранения обрабатываемых персональных данных

6.1. Хранение КИ должно осуществляться в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки КИ, если срок хранения КИ не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн.

6.2. Обрабатываемые КИ подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено федеральным законом.

6.3. Основания для прекращения обработки КИ и сроки их уничтожения определены в частях 3, 4, 5 статьи 21 Федерального закона №152-ФЗ.

6.4.Основанием (условием) прекращения обработки КИ также является ликвидация Организации.

6.5.В случае отсутствия возможности уничтожения КИ в течение срока, указанного в частях 3, 4, 5 статьи 21 Федерального закона №152-ФЗ, Оператор осуществляет блокирование таких КИ или обеспечивает их блокирование (если обработка КИ осуществляется другим лицом, действующим по поручению Оператора) и обеспечивает уничтожение КИ в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7.Порядок уничтожения обработанных конфиденциальной информации, в том числе персональных данных, при достижении целей обработки или при наступлении иных законных оснований

7.1. При уничтожении материальных носителей содержащих КИ должно быть исключено ознакомление с ними посторонних лиц, неполное или случайное их уничтожение.

7.2. При необходимости уничтожения части КИ уничтожается материальный носитель с предварительным копированием сведений, не подлежащих уничтожению, способом, исключающим одновременное копирование КИ, подлежащих уничтожению или блокированию.

7.3.Уничтожение части КИ, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этой КИ с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

7.4.Для уничтожения КИ Оператор создает комиссию. В состав комиссии включается ответственный за организацию обработки КИ. Уничтожение КИ производится в присутствии всех членов комиссии.

7.5.После уничтожения материальных носителей членами комиссии подписывается Акт об уничтожении КИ и в Журнале учета материальных носителей, а также в номенклатурах и описях дел проставляется отметка «Уничтожено, Акт №__ «__» _____ 201__ г.».

8.Ответственность за нарушение требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»

8.1. Лица, виновные в нарушении требований Федерального закона №152-ФЗ, несут предусмотренную законодательством Российской Федерации ответственность.

8.2. Моральный вред, причиненный субъекту ПДн вследствие нарушения его прав, нарушения правил обработки КИ, установленных Федеральным законом №152-ФЗ, а также требований к защите КИ, установленных в соответствии с Федеральным законом №152-ФЗ, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом ПДн убытков.

9. Заключительные положения

9.1. Сотрудники, определенные приказом по Организации, как пользователи, участвующие в обработке КИ, должны ознакомиться с настоящими правилами обработки КИ.

9.2. Обязанность доводить до сведения работников Оператора положения законодательства Российской Федерации о КИ, локальных актов по вопросам обработки КИ, требований к защите КИ лежит на лице, ответственном за организацию обработки КИ (п. 2, часть 4, статья 22.1 Федерального закона №152-ФЗ).

Начальник отдела кадров _____ Дегтярева Н.Н.

Лицо, ответственное за организацию
обработки конфиденциальной информации,
в том числе персональных данных _____ Гостеева Н.Н.

к Правилам обработки конфиденциальной информации, в том числе
персональных данных от « ___ » _____ 2017 г. № _____

**Постановление Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении
Положения об особенностях обработки персональных данных, осуществляемой
без использования средств автоматизации"**

В целях реализации Федерального закона "О персональных данных" Правительство Российской Федерации постановляет:

1. Утвердить прилагаемое Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации.
2. Федеральным органам исполнительной власти в месячный срок привести свои акты по вопросам обработки персональных данных, осуществляемой без использования средств автоматизации, в соответствие с настоящим постановлением.
3. Настоящее постановление вступает в силу по истечении одного месяца со дня его официального опубликования.

Председатель Правительства Российской Федерации

В. Путин

**Положение об особенностях обработки персональных данных, осуществляемой
без использования средств автоматизации (утв. постановлением Правительства
РФ от 15 сентября 2008 г. N 687)**

I. Общие положения

1. Обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы (далее - персональные данные), считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

2. Обработка персональных данных не может быть признана осуществляемой с использованием средств автоматизации только на том основании, что персональные данные содержатся в информационной системе персональных данных, либо были извлечены из нее.

3. Правила обработки персональных данных, осуществляемой без использования средств автоматизации, установленные нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами организации, должны применяться с учетом требований настоящего Положения.

II. Особенности организации обработки персональных данных, осуществляемой без использования средств автоматизации

4. Персональные данные при их обработке, осуществляемой без использования средств автоматизации, должны обособляться от иной информации, в частности путем фиксации их на отдельных материальных носителях персональных данных (далее - материальные носители), в специальных разделах или на полях форм (бланков).

5. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

6. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в том числе сотрудники организации-оператора или лица, осуществляющие такую обработку по договору с оператором), должны быть проинформированы о факте обработки ими персональных данных, обработка которых осуществляется оператором без использования средств автоматизации, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, а также локальными правовыми актами

организации (при их наличии).

7. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

а) типовая форма или связанные с ней документы (инструкция по ее заполнению, карточки, реестры и журналы) должны содержать сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, имя (наименование) и адрес оператора, фамилию, имя, отчество и адрес субъекта персональных данных, источник получения персональных данных, сроки обработки персональных данных, перечень действий с персональными данными, которые будут совершаться в процессе их обработки, общее описание используемых оператором способов обработки персональных данных;

б) типовая форма должна предусматривать поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации, - при необходимости получения письменного согласия на обработку персональных данных;

в) типовая форма должна быть составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных;

г) типовая форма должна исключать объединение полей, предназначенных для внесения персональных данных, цели обработки которых заведомо не совместимы.

8. При ведении журналов (реестров, книг), содержащих персональные данные, необходимые для однократного пропуска субъекта персональных данных на территорию, на которой находится оператор, или в иных аналогичных целях, должны соблюдаться следующие условия:

а) необходимость ведения такого журнала (реестра, книги) должна быть предусмотрена актом оператора, содержащим сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способы фиксации и состав информации, запрашиваемой у субъектов персональных

данных, перечень лиц (поименно или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журнала (реестра, книги), сроки обработки персональных данных, а также сведения о порядке пропуска субъекта персональных данных на территорию, на которой находится оператор, без подтверждения подлинности персональных данных, сообщенных субъектом персональных данных;

б) копирование содержащейся в таких журналах (реестрах, книгах) информации не допускается;

в) персональные данные каждого субъекта персональных данных могут заноситься в такой журнал (книгу, реестр) не более одного раза в каждом случае пропуска субъекта персональных данных на территорию, на которой находится оператор.

9. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, должны быть приняты меры по обеспечению отдельной обработки персональных данных, в частности:

а) при необходимости использования или распространения определенных персональных данных отдельно от находящихся на том же материальном носителе других персональных данных осуществляется копирование персональных данных, подлежащих распространению или использованию, способом, исключающим одновременное копирование персональных данных, не подлежащих распространению и использованию, и используется (распространяется) копия персональных данных;

б) при необходимости уничтожения или блокирования части персональных данных уничтожается или блокируется материальный носитель с предварительным копированием сведений, не подлежащих уничтожению или блокированию, способом, исключающим одновременное копирование персональных данных, подлежащих уничтожению или блокированию.

10. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, может производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе

(удаление, вымарывание).

11. Правила, предусмотренные пунктами 9 и 10 настоящего Положения, применяются также в случае, если необходимо обеспечить отдельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными.

12. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

III. Меры по обеспечению безопасности персональных данных при их обработке, осуществляемой без использования средств автоматизации

13. Обработка персональных данных, осуществляемая без использования средств автоматизации, должна осуществляться таким образом, чтобы в отношении каждой категории персональных данных можно было определить места хранения персональных данных (материальных носителей) и установить перечень лиц, осуществляющих обработку персональных данных либо имеющих к ним доступ.

14. Необходимо обеспечивать отдельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

15. При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключаящие несанкционированный к ним доступ. Перечень мер, необходимых для обеспечения таких условий, порядок их принятия, а также перечень лиц, ответственных за реализацию указанных мер, устанавливаются оператором.

