

Министерство общего и профессионального образования Ростовской области  
государственное бюджетное профессиональное  
образовательное учреждение Ростовской области  
«Таганрогский техникум строительной индустрии и технологий»

СОГЛАСОВАНО

с учетом мнения первичной  
профсоюзной организации  
ГБПОУ РО «ТТСИиТ»

Председатель профкома



Е.В. Бачинская

УТВЕРЖДЕНО

приказом директора по ГБПОУ РО  
«ТТСИиТ» от 29.08.2014г. № 301



Директор ГБПОУ РО «ТТСИиТ»  
Н.Н. Михалева

## ПОЛОЖЕНИЕ

об обеспечении безопасности персональных  
данных при их обработке в информационных  
системах персональных данных в ГБПОУ РО  
«Таганрогский техникум строительной индустрии  
и технологий»

Таганрог  
2014г.

## **I. Общие положения**

1.1. Настоящее Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в государственном бюджетном профессиональном образовательном учреждении Ростовской области «Таганрогский техникум строительной индустрии и технологий» (далее – Положение, техникум, работодатель) разработано в соответствии с Трудовым кодексом Российской Федерации, Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных», уставом техникума и определяет порядок обработки и защиты персональных данных работников и обучающихся техникума.

1.2. Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах техникума, а также к применению информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации.

1.3. Основными принципами обработки персональных данных в техникуме являются:

- принцип законности целей и способов обработки персональных данных;
- принцип соответствия объема и характера обрабатываемых персональных данных, способам их обработки и целям обработки персональных данных;
- принцип достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к заявленным при их сборе целям;
- принцип недопустимости объединения созданных для несовместимых между собой целей баз данных информационных систем персональных данных;
- принцип защиты персональных данных от неправомерного доступа и их использования или утраты.

## **2. Требования, предъявляемые к сбору, хранению и распространению персональных данных**

2.1. При обработке персональных данных работника должны соблюдаться следующие общие требования:

- обработка персональных данных работника может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества;
- при определении объема и содержания обрабатываемых персональных данных работника работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами;
- все персональные данные работника следует получать у него самого.

Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть

получено письменное согласие. Работодатель должен сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных и последствиях отказа работника дать письменное согласие на их получение;

- работодатель не имеет права получать и обрабатывать персональные данные работника о его политических, религиозных и иных убеждениях и частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия;
- работодатель не имеет права получать и обрабатывать персональные данные работника о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных Трудовым кодексом РФ или иными федеральными законами;
- при принятии решений, затрагивающих интересы работника, работодатель не имеет право основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного доступа;
- защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена работодателем за счет его средств в порядке, установленном Трудовым кодексом Российской Федерации или иными федеральными законами;
- работники и их представители должны быть ознакомлены под роспись с документами работодателя, устанавливающими порядок обработки персональных данных работником, а также об их правах и обязанностях в области обработки персональных данных;
- работники не должны отказываться от своих прав на сохранение и защиту тайны;
- работодатели, работники и их представители должны совместно вырабатывать меры защиты персональных данных работников.

### **3. Работа с документами, содержащими персональные данные**

3.1. Персональные данные работников содержатся в основном документе персонального учета работников - в личном деле работника, которое формируется специалистом по кадрам техникума после издания приказа о его приеме на работу и хранится в специально оборудованном шкафу.

3.2. Персональные данные обучающихся содержатся в основном документе персонального учета обучающихся - в личном деле, которое формируется секретарем учебной части техникума и мастером производственного обучения группы, в которую зачислен обучающийся, после издания приказа о его зачислении на учебу и хранится в специально оборудованном шкафу.

3.3. Для уничтожения персональных данных на бумажных носителях в подразделениях, работающих с персональными данными работников и обучающихся, предусматривается комиссионный порядок. Уничтожение документов, содержащих персональные данные работников и обучающихся осуществляется по акту в присутствии всех членов комиссии.

### **4. Хранение и использование персональных данных**

4.1. Персональные данные работников хранятся на бумажных носителях в помещении приемной директора техникума у специалиста по кадрам. Для этого используются специально оборудованные шкафы и сейф. Личные дела уволенных работников

хранятся в архиве сроком до 75 лет.

4.2. Персональные данные обучающихся хранятся на бумажных носителях в кабинете секретаря учебной части, архиве. Для этого используются специально оборудованные шкафы и сейфы. Личные дела отчисленных обучающихся хранятся в архиве сроком до 75 лет.

4.3. Сведения о начислении и выплате заработной платы работникам и стипендий обучающимся хранятся на бумажных носителях в помещении бухгалтерии техникума. По истечении сроков хранения, установленных законодательством РФ, данные сведения передаются в архив.

4.4. Конкретные обязанности по ведению, хранению личных дел работников и обучающихся, заполнению, хранению и выдаче трудовых книжек, иных документов, отражающих персональные данные работников и обучающихся, возлагается на специалиста по кадрам и секретаря учебной части.

4.5. Доступ к персональным данным работников (обучающихся) без получения специального разрешения имеют: директор техникума, его заместители, главный бухгалтер, работники бухгалтерии, работник кадровой службы, мастера производственного обучения (только с персональными данными обучающихся закрепленных групп) в соответствии со своими должностными обязанностями. Иные работники техникума могут иметь доступ к персональным данным работников и обучающихся в случае, если они получили разрешение директора в виде визы на служебной записке, обосновывающей необходимость ознакомления и использования персональных данных конкретного работника или обучающегося.

4.6. Для работников (программиста и оператора ЭВМ) право доступа к данным в процессе настройки вычислительной техники и разработки информационных систем оговаривается в должностных инструкциях.

4.7. Со сторонними работниками, сопровождающими работу информационных систем, заключаются договоры о неразглашении персональных данных работников и обучающихся.

## **5. Обеспечение безопасности персональных данных при их обработке в информационных системах**

5.1. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

5.2. Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

5.3. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

5.4. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и путем применения технических средств.

5.5. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения в эти помещения посторонних лиц.

5.6. При обработке персональных данных в информационной системе должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременное обнаружение фактов несанкционированного доступа к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

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

- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;
- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- разбирательство и составление заключений по фактам не соблюдения условий хранения носителей персональных данных, 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;
- описание системы защиты персональных данных.

5.8. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения трудовых обязанностей, допускаются к соответствующим персональным данным на основании раздела 5 настоящего Положения.

5.9. Контроль за организацией доступа к персональным данным возлагается

на работников техникума, наделенных соответствующими полномочиями приказом директора техникума.

При обнаружении нарушений порядка предоставления персональных данных лица, осуществляющие контроль за доступом к персональным данным незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

5.10. Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

## **6. Передача персональных данных**

6.1. При передаче персональных данных должны соблюдаться конкретные процедуры и способы взаимодействия работников и обучающихся техникума – собственников персональных данных с работником кадровой службы, секретарем учебной части, заместителей директоров и иных подразделений техникума по передаче информации, содержащей персональные данные.

Они заключаются в том, чтобы:

- не сообщать персональные данные третьей стороне без письменного согласия работника или обучающегося – собственника персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы их жизни и здоровью, а также в других случаях, предусмотренных действующим законодательством;
- не сообщать персональные данные в коммерческих целях без письменного согласия работника или обучающегося;
- предупреждать лиц, получающих персональные данные, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения соблюдения этого правила. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности);
- осуществлять передачу персональных данных в пределах техникума в соответствии с локальным нормативным актом;
- разрешать доступ к персональным данным только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций;
- не запрашивать информацию о состоянии здоровья работника или обучающегося, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции, либо возможности обучения по данной специальности;
- передавать персональные данные работников представителям работников в порядке, установленном Трудовым кодексом Российской Федерации и иными федеральными законами, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функций.

## **7. Права работников и обучающихся в области защиты персональных данных**

7.1. В целях обеспечения защиты персональных данных, хранящихся в техникуме, работники и обучающиеся имеют право на:

- полную информацию об их персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на

получение копий любой записи, содержащей персональные данные работника или обучающегося, за исключением случаев, предусмотренных федеральным законом;

- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением норм и требований действующего законодательства. При отказе работодателя исключить или исправить персональные данные работника он имеет право заявить в письменной форме работодателю о своем несогласии с соответствующим обоснованием такого несогласия. Персональные данные оценочного характера работник имеет право дополнить заявлением, выражающим его собственную точку зрения;
- требование об извещении работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжалование в суд любых неправомерных действий или бездействия работодателя при обработке и защите его персональных данных.

## **8. Обязанности работников и обучающихся по обеспечению достоверности его персональных данных**

8.1. Работники, обучающиеся и их представители должны быть ознакомлены с документами техникума, устанавливающими порядок обработки персональных данных работников и обучающихся, а также об их правах и обязанностях в области защиты персональных данных.

8.2. Работники и обучающиеся должны быть заранее предупреждены о необходимости предоставления достоверных сведений и о возможности ответственности в случае нарушения своей обязанности.

## **9. Порядок передачи информации о работнике и обучающемся**

9.1. Работник кадровой службы, работники бухгалтерии, секретарь учебной части, заместители директора и мастера производственного обучения ответственные за работу с персональными данными, обязаны знать случаи, при которых они могут передать информацию о работнике и обучающемся запрашивающим лицам. К таким случаям, как правило, относят запросы о получении информации о работниках и обучающихся техникума, направленные различными государственными органами.

9.2. Передача данной информации возможна только с ведома и (или) по распоряжению директора техникума.

9.3. Экземпляры передаваемой информации дублируются и хранятся в техникуме на соответствующих носителях информации в течение трех лет.

## **10. Ответственность за нарушение законодательства об охране персональных данных**

10.1. За нарушение законодательства об охране персональных данных работник может быть привлечен к дисциплинарной, административной и уголовной ответственности.

10.2. К дисциплинарной ответственности может быть привлечен работник кадровой службы, работники бухгалтерии, заместители директора и иного подразделения, использующего в своей работе персональные данные в соответствии с подпунктом

«в» пункта 6 статьи 81 Трудового кодекса РФ.

10.3. К административной ответственности могут быть привлечены как работник кадровой службы, работники бухгалтерии и иных подразделений, так и директор техникума и его заместители и техникум в целом на основании статей 2.4. КоАП РФ и 13.11. КоАП РФ.

10.4. Уголовная ответственность за нарушение неприкосновенности частной жизни предусмотрена статьей 137 УК РФ.