УТВЕРЖДЕНО
приказом директора техникума
от «27» апреля 2023г.
№ 93.1-ОД

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Армавирский техникум технологии и сервиса»

1.ОБЩИЕ ПОЛОЖЕНИЯ

1.1.НастоящееПоложение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Армавирский техникум технологии и сервиса»(далее – Положение, Техникум) 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 июля2006 г. № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»,Постановлением Правительства РФ от 15 сентября 2008г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», 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.ДОКУМЕНТЫ, СОДЕРЖАЩИЕ СВЕДЕНИЯ, СОСТАВЛЯЮЩИЕ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

2.1. Документы работников техникума:

- документы, предъявляемые работником при заключении трудового договора: паспорт или документ, удостоверяющий личность, трудовая книжка, страховое свидетельство государственного пенсионного страхования, документы воинского учета, документ об образовании; документы о составе семьи работника, необходимые для предоставления

гарантий, связанных с выполнением семейных обязанностей (например: свидетельство о заключении брака, свидетельство о рождении ребенка);
- документы о состоянии здоровья детей и других близких родственников (например: справки об инвалидности), когда с наличием таких документов связано предоставление работнику каких-либо гарантий и компенсаций;
- документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным в законодательстве (об инвалидности, ограничении к труду в определенных условиях, донорстве, нахождении в зоне воздействия радиации в связи с аварией на Чернобыльской АЭС и т.п.).

2.2. Документы обучающихся в техникуме:

- документы, предъявляемые в Приемную комиссию при заполнении заявления о приеме в техникум: паспорт или документ, удостоверяющий личность, документы воинского учета, документ об образовании;

- документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным действующим законодательством (об инвалидности, нахождении в зоне воздействия радиации в связи с аварией на Чернобыльской АЭС и т.п.);

- медицинская справка;

- договор об образовании;

- квитанции об оплате по договору.

3. ТРЕБОВАНИЯ, ПРЕДЪЯВЛЯЕМЫЕ К СБОРУ, ХРАНЕНИЮ И РАСПРОСТРАНЕНИЮ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. 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 4 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 получения;

- 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 подпись с документами работодателя, устанавливающими порядок обработки персональных данных работником, а также об их правах и обязанностях в этой области;

- 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.

4. РАБОТА С ДОКУМЕНТАМИ, СОДЕРЖАЩИМИ ПЕРСОНАЛЬНЫЕ ДАННЫЕ

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

4.2. Персональные данные обучающихся содержатся в основном документе персонального учета обучающихся - в личном деле, которое формируется работниками учебной части техникума после издания приказа о его зачислении на учебу и хранится в специально оборудованном шкафу.

4.3. Для уничтожения 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 с применением офисной техники «Уничтожение документов».

5. ХРАНЕНИЕ И ИСПОЛЬЗОВАНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. Документы, содержащие информацию о персональных данных работников и обучающихся, хранятся на бумажном и электронном носителях в кадровой службе техникума, бухгалтерии, на отделениях и в учебной части.

Доступ к такой информации без получения специального разрешения имеют директор техникума, его заместители, ведущий экономист, работник кадровой службы, заведующие отделениями в соответствии со своими должностными обязанностями. Иные работники техникума могут иметь доступ к персональным данным работников и обучающихся в случае, если 6 они получили разрешение директора техникума в виде визы на служебной записке, обосновывающей необходимость ознакомления и использования персональных данных конкретного работника или обучающегося.

5.2. Для работников лаборатории электронно-вычислительной техники и информационных технологий право доступа к данным в процессе настройки вычислительной техники и разработки информационных систем оговаривается в должностных инструкциях и закрепляется дополнительным трудовым соглашением.

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

6. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

6.1. 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.

6.2. 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.

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

6.4. 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.

6.5. Размещение информационных систем, специальное оборудование и охрана помещений (с помощью систем сигнализации), 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.

6.6. 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.

6.7. 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;

- 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;

- 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;

- организацию учета лиц, допущенных к работе с персональными данными в информационной системе на основании служебных записок и дополнительных трудовых соглашений (учет возложить на специалиста по кадрам);

- контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

-разбирательство и составление заключений по фактам несоблюдения 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.

6.8. 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.

6.9. Контроль за организацией доступа к персональным данным возлагается на работников техникума, наделенных соответствующими полномочиями приказом по техникуму. 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.

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

6.11. Для обеспечения безопасности персональных данных информационные системы, предназначенные для хранения и обработки персональных данных, должны располагаться на сервере техникума. Обслуживание сервера возлагается наэлектроника.

7. ПЕРЕДАЧА ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1. При передаче персональных данных должны соблюдаться конкретные процедуры и способы взаимодействия работников и обучающихся техникума и работников кадровой службы, а также иных подразделений техникума по передаче информации, содержащей персональные данные работников и обучающихся:

- не сообщать персональные данные третьей стороне без письменного согласия работника или обучающегося, 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 того, что это правило соблюдено. Лица, получающие персональные данные, обязаны соблюдать режим секретности (конфиденциальности);

-осуществлять передачу персональных данных в пределах техникума в соответствии с локальным нормативным актом, с которым работники и обучающиеся должны быть ознакомлены под роспись;

- 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.

8. ПРАВА РАБОТНИКОВ И ОБУЧАЮЩИХСЯ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

8.1. 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;

- доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;

-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.

9. ОБЯЗАННОСТИ РАБОТНИКОВ И ОБУЧАЮЩИХСЯ ПО ОБЕСПЕЧЕНИЮ ДОСТОВЕРНОСТИ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

9.1. Работники, обучающиеся и их представители должны быть ознакомлены под подпись с документами техникума, устанавливающими

порядок обработки персональных данных работников и обучающихся, а также об их правах и обязанностях в области защиты персональных данных.

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

10. ПОРЯДОК ПЕРЕДАЧИ ИНФОРМАЦИИ О РАБОТНИКЕ И ОБУЧАЮЩЕМСЯ

10.1. Работники кадровой службы техникума, бухгалтерии, учебной части и отделений, 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.

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

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

11. ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ ЗАКОНОДАТЕЛЬСТВА ОБ ОХРАНЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

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

11.2. К дисциплинарной ответственности может быть привлечен работник кадровой службы, бухгалтерии, иного подразделения, использующего в своей работе персональные данные в соответствии с подпунктом «в» пункта 6 статьи 81 Трудового кодекса РФ.

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

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

Положение введено взамен Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных в государственном бюджетном профессиональном образовательном учреждении Краснодарского края «Армавирский техникум технологии и сервиса», утвержденного приказом директора техникума от 22.01.2014 г. № 21-ОД.

Приложение 1
к Положению об обеспечении
безопасности персональных данных
при их обработке в информационных
системах персональных данных

Персональные данные работников

-Фамилия

-Имя

-Отчество

-Год, месяц, дата и место рождения

-Паспортные данные (серия, №, дата выдачи, кем выдан)

-Адрес, телефоны

-Семейное положение

-Социальное положение

-Сведения о детях

-Гражданство

-Образование

-Регистрационные данные документа об образовании

-Профессия

-Должность

-Место работы

-Доходы

-Документы, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям (об инвалидности, к труду и т.п.)

- Документы о состоянии здоровья детей и других близких родственников

- Данные о предыдущем месте работы

Приложение 2
к Положению об обеспечении
безопасности персональных данных
при их обработке в информационных
системах персональных данных

Персональные данные обучающихся

-Фамилия

-Имя

-Отчество

-Год, месяц, дата и место рождения

-Паспортные данные (серия, №, дата выдачи, кем выдан, код подразделения)

-Домашний адрес, телефоны

- Семейное положение

-Социальное положение

-Сведения о детях

-Образование

-Регистрационные данные документа об образовании

-Регистрационные данные свидетельства ЕГЭ

-Стаж работы

-Национальность

-Гражданство

-Данные о родителях

Дополнительные данные для обучающихся по договору:

-Номер договора об образовании

- На кого заключен договор об образовании

-Суммы оплат по договору об образовании

-Паспортные данные для физических лиц, на кого заключен договор об образовании

- Названия организаций (для юридических лиц)

-Срок оплаты