Министерство здравоохранения Ставропольского края

Государственное бюджетное образовательное учреждение
среднего профессионального образования
Ставропольского края
«Пятигорский медицинский колледж»

УТВЕРЖДАЮ:

Директор

ГБОУ СПО СК «Пятигорский

медицинский колледж»

_____ В.В. Трунаева

«_21_» _июня_ 2016 г.

ПОЛОЖЕНИЕ
О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ И ОБУЧАЮЩИХСЯ

г. Пятигорск – 2016 г

Согласовано:
Заместитель директора по УР _____ И.В. Уварова
«21» июня 2016 г.

Главный бухгалтер _____ О.С. Шалайкина
«21» июня 2016 г.

Начальник учебного отдела _____ Е.Д. Елатонцева
«21» июня 2016 г.

Зав. отд. ДПО _____ Ю.В. Шаталова
«21» июня 2016 г.

Специалист по кадрам _____ З.В. Симонян
«21» июня 2016 г.

Программист _____ Л.В. Провоторова
«21» июня 2016 г.

Разработчик:

Юрисконсульт _____ И.Н.Коломыцева

Дата введения в действие: «21» июня 2016 г.

Настоящее Положение определяет порядок и проведение работ по обработке и защите персональных данных работников и обучающихся.

Положение о защите персональных данных работников и обучающихся является внутренним локальным актом, не может быть полностью или частично воспроизведено, тиражировано и распространено без разрешения ГБОУ СПО СК «Пятигорский медицинский колледж».

1. Общие положения

1.1. Настоящее Положение разработано на основе и во исполнение части 1 статьи 23, статьи 24 Конституции Российской Федерации, положений главы 14 Трудового кодекса Российской Федерации «Защита персональных данных работников», Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных».

1.2. Положение определяет основные требования к порядку получения, накопления, систематизации, хранения, комбинирования, уточнения (обновления, изменения), передачи, использования, распространения (в том числе передачу), обезличивания, блокирования, уничтожения персональных данных или любого другого использования персональных данных работника (далее - обработке персональных данных работников) в связи с трудовыми отношениями.

1.3. Персональные данные работника - это информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

Персональные данные обучающегося – это информация, необходимая образовательному учреждению в связи с осуществлением образовательного процесса и касающаяся конкретного обучающегося.

1.4. К персональным данным работника, обучающегося относятся: биографические и опознавательные данные, личные характеристики, сведения о семейном положении, социальном положении, образовании, навыках, профессии, служебном положении, финансовом положении, состоянии здоровья и др.

1.5. К субъектам персональных данных (далее – субъекты) относятся лица, персональные данные которых переданы ГБОУ СПО СК «Пятигорский медицинский колледж» (далее – Колледж), как на добровольной основе, так и в рамках выполнения требований нормативно-правовых актов для обработки (в том числе передачи).

1.6. Персональные данные работников, обучающихся могут храниться на бумажном носителе, а также в электронном виде в локальной компьютерной сети.

1.7. Обработка персональных данных работников и обучающихся без письменного согласия не допускается, если иное не определено законодательством Российской Федерации. Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности снимается в случаях обезличивания или по истечении сроков хранения, если иное не определено законодательством Российской Федерации.

1.8. Должностные лица Колледжа, в обязанности которых входит обработка персональных данных работников и обучающихся, обязаны обеспечить каждому субъекту возможность ознакомления со своими персональными данными, если иное не предусмотрено законодательством Российской Федерации.

1.9. Персональные данные не могут быть использованы в целях:

- причинения имущественного и морального вреда гражданам;
- затруднения реализации прав и свобод граждан Российской Федерации.

1.20. Настоящее Положение и изменения к нему утверждаются директором Колледжа, являются обязательными для исполнения всеми сотрудниками, имеющими доступ к персональным данным работников и обучающихся.

2. Состав информации персонального характера

2.1. Персональные данные работника, обучающегося содержатся в документах персонального учета и других документах, отражающих процедуру документирования трудовых отношений. Персональные данные обучающегося содержатся в документах персонального учета и других документах, отражающих процедуру документирования образовательного процесса.

2.2. К документам, содержащим информацию персонального характера, относятся следующие документы и их комплексы:

- документы персонального характера, удостоверяющие личность работника, обучающегося или содержащие сведения о работнике (об образовании, состоянии здоровья, трудовом стаже и др.): паспорт работника, обучающегося или иной документ, удостоверяющий личность, военный билет, страховое свидетельство Пенсионного фонда Российской Федерации, документы об образовании (аттестаты, дипломы, свидетельства, сертификаты), трудовая книжка работника, медицинские справки и заключения и др.;
- учетные документы по личному составу: личная карточка (форма Т-2, Т-2ГС (МС), Т-4), личное дело работника, личное дело обучающегося, вспомогательные регистрационно-учетные формы (книги, журналы, картотеки, базы данных), содержащие сведения персонального характера: журнал (книга) регистрации приказов по личному составу, книга учета движения трудовых книжек и вкладышей к ним, журнал учета отпусков, журнал учета выдачи справок с места работы, книги учета работников, прибывающих и выбывающих в командировки и др.;
- трудовые договоры с работниками, изменения к трудовым договорам, договоры о материальной ответственности с работниками;
- договоры с обучающимися, дополнительные соглашения к ним
- распорядительные документы по личному составу (подлинники и копии): приказы (распоряжения) о приеме (заключении трудового договора), переводе, увольнении (прекращении трудового договора), отчислении (студентов) предоставлении отпуска, поощрении, взыскании и др.;
- документы по оценке деловых и профессиональных качеств работников при приеме на работу (тесты, анкеты, резюме и др.);
- документы, отражающие деятельность аттестационных и конкурсных комиссий: протоколы заседаний, аттестационные листы, решения, представления и др.);
- документы, отражающие результаты служебных расследований: докладные и объяснительные записки, акты, справки, протоколы и др.;
- подлинники и копии отчетных, аналитических и справочных материалов, передаваемых руководству Колледжа, руководителям структурных подразделений и служб;
- копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения;
- документы бухгалтерского учета, содержащие информацию о расчетах с персоналом: лицевые счета, расчетно-платежные ведомости, платежные ведомости и др.

Если сведения персонального характера содержатся в других документах, на них распространяются положения данного документа.

3. Получение персональных данных работника и гарантии их защиты

3.1. Получение, хранение, анализ, передача или любое другое использование персональных данных работника осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении, карьерном росте, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы, охраны труда работников.

3.2. Все персональные данные работника предоставляются самим работником. Если персональные данные работника могут быть получены только у третьей стороны, то работник должен быть уведомлен об этом заранее, и от него должно быть получено письменное согласие. Специалист по кадрам или иной сотрудник Колледжа должны сообщить работнику о целях, предполагаемых источниках и способах получения

персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

3.3. Работник предоставляет работодателю, обучающийся представляет администрации Колледжа достоверные персональные сведения. При изменении персональных данных работник, обучающийся обязан письменно уведомить об этом работодателя в срок, не превышающий 14 дней. Работодатель имеет право запрашивать у работника дополнительные сведения и документы, подтверждающие их достоверность.

3.4. Не допускается получение и обработка персональных данных работников о политических, религиозных и иных убеждениях, частной жизни, а также о членстве работников в общественных организациях, объединениях, в том числе профсоюзной деятельности работников, за исключением случаев, предусмотренных законодательством Российской Федерации.

3.5. При принятии решений относительно работника на основании его персональных данных не допускается использование данных, полученных исключительно в результате их автоматизированной обработки или электронного получения.

3.6. В соответствии со статьей 24 Конституции Российской Федерации, в случаях, непосредственно связанных с вопросами трудовых отношений, с письменного согласия работника возможно получение и обработка данных о его частной жизни.

4. Хранение, использование и передача персональных данных работников и обучающихся

4.1. Документы, содержащие персональные данные работников, обучающихся являются документами «для внутреннего использования».

4.2. Специалист по кадрам Колледжа и иные подразделения (бухгалтерия, учебный отдел) организуют хранение и использование персональных данных работников, обучающихся в соответствии с Трудовым кодексом Российской Федерации, иными федеральными законами, настоящим Положением и другими локальными нормативными актами организации, регламентирующими порядок работы с персональными данными работников и обучающихся.

4.3. Доступ к персональным данным работников, обучающихся разрешается только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, обучающего, которые необходимы для выполнения конкретных управленческих функций.

4.4. Доступ к персональным данным работника имеют директор Колледжа, заместитель директора, главный бухгалтер, а к тем данным, которые необходимы для выполнения конкретных функций, - непосредственный руководитель работника, специалист отдела кадров, юрисконсульт, специалисты бухгалтерии. Перечень лиц указан в приложении №4 к Положению. Доступ специалистов других отделов к персональным данным осуществляется на основании письменного разрешения директора Колледжа или его заместителя. Доступ к персональным данным обучающихся имеют члены приемной комиссии (в период проведения приема в Колледж), сотрудники учебного отдела, кураторы, заведующие отделениями, специалист по кадрам в пределах выполнения конкретных служебных функций.

4.5. Выдача личных дел работников для ознакомления директору Колледжа, заместителям директора, другим лицам, имеющим право доступа к персональным данным, производится специалистом отдела кадров по их запросу на срок не более двух рабочих дней с отметкой в журнале выдачи персональных данных.

4.6. При передаче персональных данных работника третьим лицам необходимо предупреждать их 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 работника, обязаны соблюдать

режим конфиденциальности, за исключением обмена персональными данными работников в порядке, установленном законодательством Российской Федерации.

4.8. Хранение персональных данных работников в период их работы в Колледже осуществляется специалистом по кадрам в оборудованных для этих целей помещениях и железных закрываемых шкафах.

4.9. Договоры о материальной ответственности хранятся в бухгалтерии.

4.10. Расписки об ознакомлении работника с должностной инструкцией, об ознакомлении с положением об охране персональных данных хранятся в у специалиста по кадрам.

4.11. Специалист по кадрам Колледжа, учебный отдел, бухгалтерия может вести обработку и использование персональных данных работников и обучающихся Колледжа на бумажных и магнитных носителях, в электронной форме (с обеспечением защиты от несанкционированного доступа) в целях количественного и качественного учета и анализа данных о персонале, обучающихся, подготовки статистической отчетности, представления руководству Колледжа оперативной информации и для других целей, указанных в пункте 2.1. положения.

4.10. После увольнения работника из Колледжа документы, содержащие его персональные данные, хранятся в архиве Колледжа.

5. Права и обязанности работника в области защиты его персональных данных

5.1. Работник обязуется предоставлять персональные данные, соответствующие действительности.

5.2. Работник имеет право на:

- полную информацию о своих персональных данных и обработке этих данных;
- свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей персональные данные работника, за исключением случаев, предусмотренных законодательством Российской Федерации;
- определение своих представителей для защиты своих персональных данных;
- требование об исключении или исправлении неверных или неполных персональных данных, а также данных, обработанных с нарушением требований (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 работника, 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.
-

6. Обязанности и ответственность работодателя за нарушение норм, регулирующих обработку и защиту персональных данных работника

6.1. Колледж в лице уполномоченных должностных лиц и работников при обработке персональных данных работника несет ответственность за:

- передачу персональных данных работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законом;

- передачу персональных данных работника, учащегося в коммерческих целях без его письменного согласия;
- отказ в ознакомлении работника с установленным в Колледже порядком обработки персональных данных, установленных настоящим Положением, а также другими дополняющими либо конкретизирующими данное Положение локальными нормативными актами организации, с которыми работник должен быть ознакомлен под подпись;
- разрешение доступа к персональным данным работников, обучающихся должностным лицам, которым персональные данные не требуются для выполнения конкретных функций;
- запрашивание информации о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- отказ в предоставлении персональных данных работников их законным представителям в порядке, установленном Трудовым кодексом Российской Федерации и настоящим положением.

6.2. Персональные данные работников используются работодателем для решения вопросов о продвижении работников по службе, очередности предоставления ежегодного отпуска, установления размера заработной платы, допуска работников к конфиденциальной информации, составляющей служебную или коммерческую тайну.

6.3. При принятии решений, затрагивающих интересы работника, обучающегося, работодатель не должен основываться на персональных данных работника, обучающегося, полученных по электронным каналам или исключительно в результате их автоматизированной обработки.

6.4. Работодатель не вправе принимать решения, затрагивающие интересы работника, основываясь на данных, допускающих двоякое толкование. Если на основании персональных данных работника невозможно достоверно установить какой-либо факт, работодатель предлагает работнику представить письменные разъяснения.

6.5. Защита персональных данных работников, обучающихся от их неправомерного использования или утраты обеспечивается работодателем за счет его средств в порядке, установленном федеральным законом.

6.6. Специалист по кадрам Колледжа, учебный отдел обеспечивает ведение журналов учета выданных персональных данных работников, обучающихся, в которых регистрируются запросы, фиксируются сведения о лице, направившем запрос, дата передачи персональных данных или дата уведомления об отказе в предоставлении персональных данных, а также отмечается, какая именно информация была передана.

6.7. Работники Колледжа, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных работника, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

7.Доступ к персональным данным субъекта и их передача

7.1. Внутренний доступ (доступ внутри Колледжа) к персональным данным субъектов имеют сотрудники Колледжа, которым эти данные необходимы для выполнения должностных обязанностей.

После прекращения юридических отношений с субъектом персональные данные документы, содержащие его персональные данные, хранятся в Колледже в течение сроков, установленных архивным и иным законодательством Российской Федерации.

7.2. Внешний доступ к персональным данным субъектов имеют массовые потребители персональных данных и контрольно-надзорные органы.

7.2.1. К числу массовых потребителей персональных данных вне Колледжа относятся следующие государственные и негосударственные структуры:

- ПФР, УФНС и ФСС России;
- правоохранительные органы;
- органы прокуратуры, МВД и ФСБ России.

7.2.2. Контрольно-надзорные органы имеют доступ к информации исключительно в сфере своей компетенции.

7.3. Внешний доступ со стороны третьих лиц к персональным данным субъекта осуществляется с его письменного согласия, за исключением случаев, когда такой доступ необходим в целях предупреждения угрозы жизни и здоровью субъекта или других лиц, и иных случаев, установленных законодательством.

7.4. Колледж обязан сообщать персональные данные субъекта по надлежаще оформленным запросам суда, прокуратуры иных правоохранительных органов.

7.5. Персональные данные субъекта могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого субъекта.

7.6. При передаче персональных данных Колледж должен соблюдать следующие требования:

- не сообщать персональные данные субъекта третьей стороне без его письменного согласия, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в случаях, установленных федеральными законами;
- не сообщать персональные данные субъекта в коммерческих целях без его письменного согласия;
- предупреждать лиц, получающих персональные данные субъекта, 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, за исключением случаев, когда обмен персональными данными осуществляется в порядке, установленном федеральными законами;
- не запрашивать информацию о состоянии здоровья субъекта, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции;
- разрешать доступ к персональным данным, исключительно специально уполномоченным лицам (при этом указанные лица должны иметь право получать лишь те персональные данные, которые необходимы для выполнения конкретных функций);
- в должностных инструкция уполномоченных лиц должны быть прописаны обязательства по неразглашению и выполнению требований нормативных документов по обработке и обеспечению безопасности персональных данных.

7.7. Передача персональных данных от держателя или его представителей в другие учреждения и организации может допускаться только при наличии письменного согласия субъекта персональных данных в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.

7.8. Ответы на правомерные письменные запросы других учреждений и организаций даются с разрешения директора Колледжа в письменной форме, в том объеме, который позволяет не разглашать излишний объем персональных данных.

7.9. Не допускается передача персональных данных по открытым каналам связи, в том числе по телефону.

7.10. Сведения, передаваемые в письменной форме, должны иметь пометку о конфиденциальности. В сопроводительном письме к таким документам указывается, что в прилагаемых документах содержатся персональные данные субъектов.

7.11. Колледжем не допускается осуществление трансграничной передачи персональных данных.

8. Защита персональных данных

8.1. Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе деятельности Колледжа.

8.2. Колледж при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий, в соответствии с требованиями к обеспечению безопасности персональных данных при их обработке.

8.3. Мероприятия по защите персональных данных определяются настоящим Положением, приказами, инструкциями и другими внутренними документами Колледжа.

8.4. Для защиты персональных данных в Колледже применяются следующие принципы и правила:

- ограничение и регламентация состава сотрудников, функциональные обязанности которых требуют доступа к информации, содержащей персональные данные;
- строгое избирательное и обоснованное распределение документов и информации между сотрудниками;
- рациональное размещение рабочих мест сотрудников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание сотрудниками требований нормативно-методических документов по защите персональных данных;
- распределение персональной ответственности между сотрудниками, участвующими в обработке персональных данных, за выполнение требований по обеспечению безопасности персональных данных.
- установление режима конфиденциальности в соответствии с требованиями по обеспечению безопасности персональных данных при работе с конфиденциальными документами и базами данных;
- исключение бесконтрольного пребывания посторонних лиц в помещениях, в которых ведется обработка персональных данных и находится соответствующая вычислительная техника;
- организация порядка уничтожения информации;
- своевременное выявление нарушений требований разрешительной системы доступа;
- воспитательная и разъяснительная работа с сотрудниками по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- регулярное обучение работников по вопросам, связанным с обеспечением безопасности персональных данных;
- ограничение доступа к техническим средствам и системам обработки информации, на которых содержатся персональные данные.
- создание целенаправленных неблагоприятных условий и труднопреодолимых препятствий для лица, пытающегося совершить несанкционированный доступ и овладение информацией;
- резервирование защищаемых данных (создание резервных копий).

9. Допуск персонала к обработке персональных данных

9.1. При допуске к обработке персональных данных необходимо руководствоваться Приказом о допуске к обработке персональных данных.

8.2. Перечни должностных лиц составляются и ведутся владельцами информационных систем персональных данных и процессов обработки персональных данных, на основании данных о должностных лицах, допущенных к персональным данным.

Доступ конкретных лиц к персональным данным и информационным системам персональных данных осуществляется на основании служебных записок (заявок). Служебные записки на доступ учитываются и хранятся администратором информационной безопасности информационных систем персональных данных.

8.3. Конкретный регламент предоставления доступа определен в «Инструкции по внесению изменений в списки пользователей и наделению их полномочиями доступа к ресурсам информационных систем персональных данных».

10. Обучение персонала, участвующего в обработке персональных данных

10.1. Должно проводиться регулярное обучение работников по вопросам, связанным с обеспечением безопасности персональных данных.

10.2. В общем случае, для различных категорий сотрудников форматы обучения должны отличаться.

Определены следующие форматы обучения:

- полные курсы (длительностью 5 дней и более);
- кратковременные курсы (длительностью от 1 до 3 дней);
- внешние и внутренние семинары;
- конференции;
- инструктажи.

10.2.1. Полные и кратковременные курсы, конференции, внешние семинары проводятся во внешних специализированных организациях для следующих категорий сотрудников:

- ответственный за обеспечение безопасности и обработки персональных данных;
- администратор информационной безопасности информационных систем персональных данных.

10.2.2. Для обучения остальных категорий персонала, участвующих в процессах обработки персональных данных, должны проводиться:

- внутренние семинары;
- инструктажи.

Внутренние семинары проводятся ответственным за обеспечение безопасности и обработки персональных данных, администратором информационной безопасности информационных систем персональных данных, а также могут проводиться приглашенными специалистами или другими подготовленными лицами. На всех семинарах следует использовать презентации.

10.3. Обучение каждой категории сотрудников должно проводиться не реже одного раза в год.

Проведения инструктажей должно фиксироваться в «Журнале учета проведения инструктажей по вопросам защиты информации».

10.4. Для проведения семинаров создаются учебные группы по структурным подразделениям. Состав группы не должен превышать 5-10 человек.

Инструкторы учебных групп должны в первый год, а в дальнейшем не реже 1 раза в 3 года проходить подготовку в специализированных учебно-методических центрах по вопросам защиты персональных данных.

11. Организация работы с носителями персональных данных

11.1. Для организации документооборота связанного с персональными данными в Колледже должны быть упорядочены и регламентированы следующие работы, связанные с персональными данными:

- учет носителей, содержащих персональные данные;
- обращение с носителями, содержащими персональные данные;
- систематизация носителей, содержащих персональные данные;
- хранение носителей, содержащих персональные данные;
- подготовка носителей, содержащих персональные данные для передачи их в архив;
- подготовка носителей, содержащих персональные данные для их уничтожения;
- проверка наличия носителей, содержащих персональные данные;
- распечатка персональных данных.

Должны регламентироваться работы с персональными данными в виде документов на следующих носителях:

- бумажных носителях;
- электронных съемных носителях;
- электронных несъемных носителях, используемых в технических средствах информационных системах персональных данных.

11.2. Порядок работ с носителями персональных данных должен быть регламентирован в соответствующих внутренних нормативных документах.

12. Уничтожение персональных данных

12.1. В соответствии с нормативными актами Российской Федерации персональные данные должны быть уничтожены:

- по требованию субъекта персональных данных, в определенных законодательством Российской Федерации случаях;
- при истечении срока хранения;
- в случае выявления неправомерных действий с персональными данными и невозможности устранения допущенных нарушений;
- в случае достижения цели обработки персональных данных;
- в случае утраты необходимости достижения цели обработки.

Контроль сроков хранения, целей обработки персональных данных производится на основании допустимых сроков хранения и допустимых целей.

12.2. Решение об уничтожении персональных данных, организацию и проведение уничтожения принимают и осуществляют владельцы информационных систем персональных данных и процессов обработки персональных данных.

12.3. Порядок уничтожения персональных данных должен быть регламентирован в нормативных документах Колледжа.

Об уничтожении персональных данных должен быть уведомлен субъект персональных данных.

12.4. После проведенного уничтожения должен быть подготовлен акт об уничтожении персональных данных. Форма акта приведена в .

13. Защита от несанкционированного физического доступа к элементам ИСПДн

13.1. Мероприятия по физическому контролю доступа включают:

- контроль доступа на территорию;
- контроль доступа в помещения с оборудованием информационных систем персональных данных;
- контроль доступа к техническим средствам информационных систем персональных данных;
- контроль перемещений физических компонентов информационных систем персональных данных.

13.2. Помещения с серверным, телекоммуникационным и сетевым оборудованием информационных систем персональных данных должны иметь прочные входные двери с надежными замками. Двери должны быть постоянно закрыты на замок и открываться только для санкционированного прохода сотрудников.

Двери помещений, в которых размещаются АРМ пользователей информационных систем персональных данных, должны быть оборудованы замками.

13.3. Нахождение в помещении лиц, не участвующих в технологических процессах обработки персональных данных (обслуживающий персонал, другие сотрудники), должно допускаться только в присутствии сотрудников, участвующих в соответствующих технологических процессах.

13.4. Расположение мониторов рабочих станций должно препятствовать их несанкционированному просмотру со стороны других лиц, не являющихся пользователями информационных систем персональных данных.

13.5. В нерабочее время, по окончании рабочего дня двери помещений должны быть закрыты на замок.

13.6. При выносе устройств, хранящих персональных данных, за пределы контролируемой зоны для ремонта, замены и т.п. должно быть обеспечено гарантированное уничтожение информации, хранимой на этих устройствах.

13.7. В отношении некоторых информационных систем персональных данных возможны дополнительные, либо более низкие требования по физической защите. Состав таких требований определяется по результатам разработки Модели угроз и нарушителя и ТЗ (СТЗ, ЧТЗ) на создание СЗПДн. Мероприятия по защите таких информационных систем персональных данных определяются эксплуатационной (проектной) документацией.

14. Резервирование персональных данных

14.1. Резервирование персональных данных должно обеспечить возможность восстановления информации при нарушении целостности основных хранилищ данных.

В регламенте процесса резервирования должны быть учтены следующие вопросы:

- порядок резервирования;
- ответственные за резервирование;
- порядок восстановления информации после аварий;
- порядок хранения резервных копий.

Резервированию должна подвергаться информация на серверах информационных систем персональных данных.

Резервирование должно осуществляться на магнитные ленты или другие носители информации с соответствующим уровнем надежности и долговечности.

14.2. Хранение резервных копий должно осуществляться в сейфах (запираемых шкафах, ящиках). Хранение (по возможности) должно осуществляться в месте, территориально удаленном от основного хранилища информации.

14.3. Доступ к резервным копиям должен быть строго регламентирован.

14.4. Резервирование должно осуществляться в соответствии с инструкцией резервного копирования Управлении.

15. Реагирование на нештатные ситуации

15.1. Для эффективного реагирования на нештатные ситуации, возникающие при обработке персональных данных, в Колледже должны быть регламентированы следующие вопросы:

- порядок определения нештатной ситуации;
- порядок оповещения сотрудников при возникновении различных нештатных ситуаций;
- порядок действий персонала в нештатных ситуациях.

В Колледже должны проводиться расследования инцидентов, связанных с несанкционированным доступом и другими несанкционированными действиями.

В рамках данного процесса должны решаться следующие задачи:

- расследование инцидентов, связанных с безопасностью персональных данных;
- ликвидация последствий инцидентов связанных с безопасностью персональных данных;
- принятие мер по недопущению возникновения подобных инцидентов в дальнейшем.

Реагирование на нештатные ситуации должно производиться в соответствии с «Инструкцией по действиям пользователей информационных систем персональных данных в нештатных ситуациях».

16. Ответственность за разглашение конфиденциальной информации, связанной с персональными данными

16.1. Персональная ответственность является одним из главных требований к организации функционирования СЗПДн и обязательным условием обеспечения эффективности функционирования данной системы.

16.2. Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность в соответствии с законодательством Российской Федерации за нарушение режима защиты, обработки и порядка использования этой информации.

16.3. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных субъекта, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.

16.4. Каждый сотрудник Колледжа, получающий для работы конфиденциальный документ, несет персональную ответственность за сохранность носителя и конфиденциальность полученной информации.

16.5. Должностные лица, в обязанность которых входит обработка персональных данных, обязаны обеспечить каждому субъекту персональных данных, возможность ознакомления с документами и материалами, если иное не предусмотрено законом.

Неправомерный отказ в предоставлении собранных в установленном порядке персональных данных, либо несвоевременное их предоставление в случаях, предусмотренных законом, либо предоставление неполной или заведомо ложной информации влечет наложение на должностных лиц административного наказания в порядке, установленном Кодексом Российской Федерации об административных правонарушениях.

16.6. В соответствии с Гражданским кодексом Российской Федерации лица, незаконными методами получившие информацию, содержащую персональные данные, обязаны возместить причиненные убытки; такая же обязанность возлагается и на работников, не обладающих правом доступа к персональным данным.

16.7. Уголовная ответственность за нарушение неприкосновенности частной жизни (в том числе незаконное собирание или распространение сведений о частной жизни лица, составляющего его личную или семейную тайну, без его согласия), неправомерный доступ к охраняемой законом компьютерной информации, неправомерный отказ в предоставлении собранных в установленном порядке документов и сведений (если эти деяния причинили вред правам и законным интересам граждан), совершенные лицом с использованием своего служебного положения влечет наложение наказания в порядке, предусмотренном Уголовным кодексом Российской Федерации.

16.8. Неправомерность деятельности органов государственной власти и организаций по сбору и использованию персональных данных может быть установлена в судебном порядке.

17. Обработка персональных данных без использования средств автоматизации

Особенности обработки персональных данных, осуществляемой без использования средств автоматизации:

17.1. 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, а также если необходимо обеспечить раздельную обработку зафиксированных на одном материальном носителе персональных данных и информации, не являющейся персональными данными, должны быть приняты меры по обеспечению раздельной обработки персональных данных, в частности:

– 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;

– 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.

17.2. 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);

17.3. 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.

17.4. При составлении типовых форм необходимо, чтобы каждый субъект персональных данных чьи персональные данные указаны в документе, имел возможность

ознакомиться со своими персональными данными, содержащими в документе, не нарушая прав и законных интересов иных лиц.

Приложение № 1

Государственное бюджетное образовательное учреждение среднего профессионального образования Ставропольского края
«Пятигорский медицинский колледж»

РАСПИСКА

Я, _____
(фамилия, имя, отчество работника)

_____
(структурное подразделение, должность)

ознакомлен с Положением о защите персональных данных работника, права и обязанности в области защиты персональных данных мне разъяснены.

"___"_____20____г. _____ _____
(подпись) И.О. Фамили

Государственное бюджетное образовательное учреждение среднего профессионального образования Ставропольского края
«Пятигорский медицинский колледж»

РАСПИСКА

Я, _____
(фамилия, имя, отчество работника)

_____
(структурное подразделение, должность)

ознакомлен с Положением о защите персональных данных работника, права и обязанности в области защиты персональных данных мне разъяснены.

"___"_____20____г. _____ _____
(подпись) И.О. Фамилия

Государственное бюджетное образовательное учреждение среднего профессионального образования Ставропольского края
«Пятигорский медицинский колледж»

РАСПИСКА

Я, _____
(фамилия, имя, отчество работника)

_____
(структурное подразделение, должность)

ознакомлен с Положением о защите персональных данных работника, права и обязанности в области защиты персональных данных мне разъяснены.

"___"_____20____г. _____ _____
(подпись) И.О. Фамилия

Приложение 2

Состав личного дела работника

Личное дело работника Колледжа состоит из следующих документов:

- внутренняя опись всех документов, находящихся в личном деле;
- анкета;
- автобиография;
- копии документов об образовании;
- результаты медицинского обследования на предмет годности к осуществлению трудовых обязанностей (для ряда должностей и профессий в соответствии с действующим законодательством);
- трудовой договор, изменения к трудовому договору;
- копия должностной инструкции;
- копия приказа о приеме на работу;
- документы, связанные с переводом и перемещением работника (копии приказов, заявления работника и т.п.);
- выписки (копии) из документов о присвоении почетных званий, ученой степени, награждении государственными наградами;
- копии наградных листов;
- аттестационные листы;
- копии приказов о поощрениях, взысканиях;
- характеристики и рекомендательные письма;
- заявление работника об увольнении;
- копия приказа об увольнении;
- другие документы, нахождение которых в личном деле будет признано целесообразным, например: характеристика с прежнего места работы, письмо организации с просьбой об увольнении работника в порядке перевода, дополнение к личному листку по учету кадров и др.

Документы, относящиеся к материалам служебных проверок: докладные и объяснительные записки, акты, справки, протоколы, заключения и др. (оригиналы) – хранятся у специалиста по кадрам (до окончания возможных судебных разбирательств) до особого распоряжения директора Колледжа.

Приложение 3

Состав личного дела обучающегося

Личное дело учащегося состоит из следующих документов:

- заявление;
- ксерокопия паспорта;
- копия приписного свидетельства (военного билета);
- оригинал документа об образовании;
- копия документа об образовании;
- копия сертификата прививок;
- медицинская справка формы № 086 - у;
- договор на оказание образовательных услуг,
- согласие на обработку персональных данных;
- автобиография;
- фотография 6 шт.;
- копия свидетельства о браке;
- документы, предусматривающие льготы на прием вне конкурса в колледж (категории: инвалиды, сироты)
- справка-выписка оценок из зачетной книжки;
- справка о предоставлении академического отпуска;
- характеристика о прохождении практики;
- студенческий билет;
- зачетная книжка;
- копия выданного диплома;
- копия приложения к выданному диплому;
- обходной лист;
- расписка в получении документа об образовании
- выписка из приказа о зачислении;
- выписка из приказа о переводе;
- выписка из приказа о предоставлении академического отпуска;
- выписка из приказа о восстановлении;
- выписка из приказа о вынесении взыскания;
- выписка из приказа о поощрении;
- выписка из приказа о пересдаче семестровой оценки;
- выписка из приказа о пересдаче экзаменационной оценки;
- выписка из приказа о смене фамилии;
- выписка из приказа о перезачете;
- выписка из приказа об отчислении.

Приложение 4

Перечень лиц, имеющих доступ к персональным данным
работников и обучающихся

1. Директор
2. Заместитель директора по учебной работе
3. Заместитель директора по учебно-воспитательной работе
4. Заместитель директора по учебно-практической работе
5. Заместитель директора по административно-хозяйственной части
6. Главный бухгалтер
7. Главный экономист
8. Ведущий бухгалтер
9. Юрисконсульт
10. Специалист по кадрам
11. Заведующий отделением дополнительного профессионального образования
12. Секретарь учебной части
13. Программист
14. Преподаватели

Приложение № 5

Форма акта уничтожения документов, содержащих персональные данные

У Т В Е Р Ж Д А Ю
Директор ГБОУ СПО СК
«Пятигорский медицинский
колледж»
_____ _/_____/
«____» _____ 2016 г.

АКТ
уничтожения документов, содержащих персональные данные

«___»_____20__ г. № _____

Комиссия в составе:
председатель –
_____;
и членов комиссии –
_____;
_____;
_____,
произвела отбор для уничтожения следующие документы, содержащие персональные данные:

№ п/п	Наименование документа	Регистрационный номер документа	Дата регистрации	Номер экз.	Количество листов документа/ приложения
1	2	3	4	5	6

Всего подлежит уничтожению _____ (_____) наименований
(цифрами) (прописью)
документов. Записи акта с регистрационными данными сверены.

Председатель комиссии:
_____ / _____
Члены комиссии:
_____ / _____
_____ / _____
_____ / _____

После утверждения акта, перед уничтожением отобранные документы с записями в акте сверили и полностью уничтожили путем измельчения в бумагорезательной машине.

Председатель комиссии:
_____ / _____
Члены комиссии:
_____ / _____
_____ / _____
_____ / _____