Государственное автономное учреждение дополнительного профессионального образования Республики Башкортостан «Центр повышения квалификации»

УТВЕРЖДЕНО
Приказом ГАУ ДПО РБ
«Центр повышения квалификации»
от «14» марта 2019 г. № 48

ПОЛОЖЕНИЕ
о защите конфиденциальной информации в ГАУ ДПО РБ «Центр повышения квалификации»

г. Уфа
2019 год

ПОЛОЖЕНИЕ
О ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
В ГОСУДАРСТВЕННОМ АВТОНОМНОМ УЧРЕЖДЕНИИ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
РЕСПУБЛИКИ БАШКОРТОСТАН
«ЦЕНТР ПОВЫШЕНИЯ КВАЛИФИКАЦИИ»

1. Общие положения

1.1. Настоящее Положение о защите конфиденциальной информации в Государственном автономном учреждении дополнительного профессионального образования Республики Башкортостан «Центр повышения квалификации» (далее по тексту – Положение и Центр) определяет комплекс организационных и технических мероприятий в части защиты конфиденциальной информации при ее обработке.

1.2. Настоящее Положение разработано в соответствии с Конституцией Российской Федерации, Гражданским кодексом Российской Федерации, Трудовым кодексом Российской Федерации, Федеральным законом от 27.07.2006 г. N 152-ФЗ (ред. от 31.12.2017) "О персональных данных", Федеральным законом от 27.07.2006г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 29.07.2004 N 98-ФЗ (ред. от 18.04.2018) "О коммерческой тайне", Уставом Центра и другими нормативно – правовыми актами Российской Федерации, регулирующими отношения в области информации (Приложение №1).

1.3. Действие настоящего Положения распространяется на штатных сотрудников Центра, сотрудников, работающих по трудовому договору, заключенному с Центром, которые дали обязательство о неразглашении конфиденциальной информации, а также на лиц (контрагентов), работающих по гражданско-правовым договорам, заключенным с Центром, взявших на себя обязательство о неразглашении конфиденциальной информации, в порядке и на условиях, предусмотренных настоящим Положением.

1.4. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

1.5. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

1.6. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

1.7. Федеральными законами устанавливаются условия отнесения

информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

1.8. К информации, доступ к которой ограничен законодательством (информация ограниченного доступа), относятся: государственная тайна, коммерческая тайна, персональные данные, сведения, связанные с профессиональной деятельностью, служебная тайна.

1.9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

1.10. За разглашение информации с ограниченным доступом предусмотрена административная или уголовная ответственность.

1.11. Режим конфиденциальности снимается в случаях обезличивания или по истечении 25 лет срока хранения конфиденциальной информации, если иное не предусмотрено законодательством РФ.

1.12. В настоящем Положении используются следующие термины и определения:

Информация - сведения (сообщения, данные) независимо от формы их представления;

информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

Конфиденциальная информация - любые сведения, составляющие служебную, коммерческую, врачебную, профессиональную тайну, включая персональные данные сотрудников и обучающихся.

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

Электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

Оператор информационной системы - гражданин или юридическое лицо,

осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

Общедоступная информация - сведения и информация, доступ к которой не ограничен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности. В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги).

Обладатель конфиденциальной информации - лицо, которое владеет информацией, относящейся к конфиденциальной на законном основании, ограничило доступ к этой информации и установило в отношении ее режим конфиденциальной информации. Обладателем информации, составляющей конфиденциальную информацию, является Центр.

Служебная тайна - научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании, и в отношении которой обладателем такой информации введен режим коммерческой тайны. Информация может быть отнесена к служебной тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений и не влечет (не может повлечь) получения прибыли обладателем такой информации. Служебную тайну организации составляют любые сведения, в том числе сведения, содержащиеся в служебной переписке, телефонных переговорах, почтовых отправлениях, телеграфных и иных сообщениях, передаваемых по сетям электрической и почтовой связи, которые стали известны работнику организации в связи с исполнением им возложенных на него трудовых обязанностей. К служебной тайне не относится информация, разглашенная образовательным учреждением самостоятельно или с её согласия, а также иная информация, ограничения доступа к которой не допускаются в соответствии с законодательством РФ.

Коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду; научно-техническая, технологическая, производственная, финансово-экономическая или иная информация (в том числе составляющая секреты производства), которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны. Информация может быть отнесена к коммерческой тайне в том, случае, если она получена, разработана в процессе осуществления трудовых правоотношений, либо в результате гражданско-правовых отношений, влекущая или могущая повлечь получение прибыли обладателем такой информации.

Профессиональная тайна - информация, полученная гражданами при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных;

Предоставление персональных данных - действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц;

Доступ к конфиденциальной информации - ознакомление определенных лиц с конфиденциальной информацией, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации.

Передача конфиденциальной информации - передача конфиденциальной информации ее обладателем контрагенту на основании договора в объеме и на условиях, которые предусмотрены договором, включая условие о принятии контрагентом установленных договором мер по охране ее конфиденциальности.

Предоставление конфиденциальной информации — передача конфиденциальной информации ее обладателем органам государственной власти, иным государственным органам, органам местного самоуправления в целях выполнения их функций.

Разглашение (распространение) конфиденциальной информации - действие или бездействие, в результате которых конфиденциальная информация в любой возможной форме (устной, письменной, иной форме, в том числе с использованием технических средств) становится известной третьим лицам без согласия обладателя такой информации либо вопреки трудовому или гражданско-правовому договору.

Информационная система персональных данных - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;

Обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных;

Режим конфиденциальности - организационные, технические и иные меры по защите конфиденциальной информации, принимаемые ее обладателем на основании закона или договора.

1.13. В Центре обработка конфиденциальной информации может осуществляться исключительно в целях оказания образовательных услуг надлежащего качества и объёма, выполнения трудового договора, в иных, предусмотренных законодательством случаях.

1.14. Перечень конфиденциальной информации Центра указан в Приложении №2.

1.15. Работу по организации и защите персональных данных Центра координирует заместитель директора по заочному, дистанционному обучению и

информационным технологиям.

1.16. Ответственность за обеспечение безопасности персональных данных в информационной системе персональных данных Центра возлагается на начальника отдела атоматизированной системы управления (ОАСУ).

1.17. Каждый работник, получающий доступ к конфиденциальной информации, в том числе к персональным данным, подписывает обязательство о неразглашении конфиденциальной информации, в том числе сведений о персональных данных, а также об ответственности в случае нарушения требований действующего законодательства в сфере защиты конфиденциальной информации.

1.18. Список работников, допущенных к работе с конфиденциальной информацией, утверждается Приказом директора Центра.

2. Цели защиты конфиденциальной информации

Основными целями защиты конфиденциальной информации в Центре являются:

- предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения работниками;
- предотвращение несанкционированного уничтожения, искажения, подделки, копирования, распространения, блокирования информации в информационных системах, установленных в Центре;
- предотвращение утрат, уничтожения или сбоев функционирования носителей информации;
- предотвращение неправомерного или случайного доступа к защищаемой информации; обеспечение полноты, целостности, достоверности защищаемой информации;
- сохранение возможности управления процессом обработки и пользования защищаемой информацией.

3. Меры, принимаемые для защиты конфиденциальной информации

3.1. В целях установления режима ограниченного доступа и конфиденциальности сведений в Центре постоянно действующая комиссия по организации информационной безопасности и защите персональных данных, обрабатываемых в Центре, а также специально уполномоченные и должностные лица, принимает следующие меры:

- осуществляет разработку локальных нормативных актов и инструкций по обеспечению защиты конфиденциальной информации и регламентации конфиденциального делопроизводства;
- заключает договоры (в том числе трудовые) с условием о сохранении и обеспечении конфиденциальности информации;
- обеспечивает ограничение доступа к защищаемой информации, оформляет допуск к такой информации, а также осуществляет учёт лиц, получающих доступ к такой информации;
- организует работу персонала с конфиденциальной информацией, в том числе с материальными носителями такой информации;

- организует обучение и проверку знаний по обеспечению режима конфиденциальности информации;
- принимает необходимые технические меры, направленные на ограничение доступа посторонних лиц к защищаемой информации.
- организует уничтожение конфиденциальной информации;
- принимает в установленном порядке меры по приостановлению или прекращению обработки конфиденциальной информации, осуществляемой с нарушением требований законодательства;
- проводит служебные проверки в целях установления виновных лиц, допустивших нарушение законодательства о защите конфиденциальной информации, и последующего привлечения их к дисциплинарной ответственности;
- обеспечивает невозможность несанкционированного доступа к документам, содержащим конфиденциальную информацию;
- обеспечивает хранение конфиденциальной информации в порядке, исключающем их утрату или их неправомерное использование.

3.2. Допуск к информации ограниченного доступа включает в себя:
- ознакомление работника с законодательством о защите конфиденциальной информации, об ответственности за его нарушение и с локальными нормативными актами о защите конфиденциальной информации в Центре; принятие работником на себя обязанности по обеспечению конфиденциальности информации, полученной при осуществлении своей трудовой функции в Центре, а также после прекращения трудовых отношений на период действия режима конфиденциальности данной информации;
- прохождение обучения и проверки знаний требований по обеспечению конфиденциальности защищаемой информации.

3.3. Для получения доступа к защищаемой информации необходимо пройти процедуру допуска.

3.3.1. Процедура допуска осуществляется администратором информационной безопасности и защите персональных данных Центра и защите персональных данных до подписания трудового договора директором:
- руководитель структурного подразделения составляет служебную записку с указанием Ф.И.О., должности работника для прохождения процедуры допуска, соответствующей функциональным обязанностям;
- администратор информационной безопасности и защите персональных данных Центра знакомит под роспись работника с законодательством о защите конфиденциальной информации, об ответственности за его нарушение и с локальными нормативными актами о защите конфиденциальной информации в Центре;
- работник знакомится и подписывает: согласие работника на обработку его персональных данных (Приложение № 3), обязательство о неразглашении конфиденциальной информации (Приложение № 4), расписку об ознакомлении с нормативными правовыми актами в сфере защиты конфиденциальной информации (Приложение № 5);
- работник проходит регистрацию доступа к информационным системам обработки конфиденциальной информации у начальника ОАСУ.

3.3.2. Документы, указанные в п.3.3.1., хранятся в личном деле сотрудника в

отделе кадров.

3.4. В трудовые договоры с лицами, принимаемыми на работу, связанную с получением, обработкой, хранением, передачей и использованием информации ограниченного доступа, включается условие об обеспечении конфиденциальности таких сведений.

Обязанности работника об обеспечении конфиденциальности оформляются также обязательством о неразглашении конфиденциальной информации.

4. Обязанности работников по защите конфиденциальной информации

4.1. Работники Центра, получившие доступ к конфиденциальной информации, обязуются обеспечивать защиту такой информации.

4.2. В целях обеспечения конфиденциальной информации, работник обязан:

- знать и соблюдать требования по получению, обработке, передаче, хранению, конфиденциальной информации, предусмотренные нормативными правовыми актами, соглашениями, должностной инструкцией, локальными нормативными актами о защите конфиденциальной информации в Центре и трудовым договором;
- знать какие конкретно сведения подлежат защите, а также строго соблюдать правила пользования ими; принимать меры по установлению и сохранению режима конфиденциальности, предусмотренные нормативными правовыми актами о защите конфиденциальной информации в Центре;
- не использовать конфиденциальную информацию ограниченного доступа в целях, не связанных с осуществлением трудовой функции;
- не разглашать конфиденциальную информацию, а также не совершать иных деяний, влекущих уничтожение или утрату такой информации;
- не допускать передачу конфиденциальной информации по телефону или факсу; незамедлительно сообщать об утрате или несанкционированном уничтожении конфиденциальной информации своему непосредственному руководителю, а также об иных обстоятельствах, создающих угрозу сохранения конфиденциальности такой информации.

4.3. При прекращении трудовых отношений с Центром работник обязан сдать все материальные носители защищаемой информации, а также ключи от помещений и шкафов, в которых они хранятся.

4.4. Непосредственный руководитель структурного подразделения, в котором уволился работник, обязан в письменном виде сообщить об увольнении специалисту по информационной безопасности и защите персональных данных.

5. Требования по получению, обработке, хранению и использованию конфиденциальной информации

5.1. Обработка и хранение конфиденциальной информации осуществляется в таком порядке и таким способом, которые исключают возможность доступа к ней неуполномоченных лиц.

5.2. Не допускается передача и выдача документов, содержащих сведения конфиденциального характера неуполномоченным лицам без законных на то

оснований.

5.3. Использование конфиденциальной информации допускается только в служебных целях.

5.4. Хранение конфиденциальной информации осуществляется в порядке, исключающем ее утрату, неправомерное использование или получение доступа неуполномоченными лицами.

5.5. Все документы, содержащие сведения конфиденциального характера должны храниться в сейфах, шкафах, оборудованных замками либо закрытых и опечатанных помещениях.

5.6. В случаях, предусмотренных федеральным законом, обработка персональных данных осуществляется только с согласия в письменной форме субъекта персональных данных. Равнозначным содержащему собственноручную подпись субъекта персональных данных согласию в письменной форме на бумажном носителе признается согласие в форме электронного документа, подписанного в соответствии с федеральным законом электронной подписью. Согласие в письменной форме субъекта персональных данных на обработку его персональных данных должно включать в себя, в частности:

1) фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;

2) фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);

3) цель обработки персональных данных;

4) перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5) перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;

6) подпись субъекта персональных данных.

6. Организация конфиденциального делопроизводства

6.1. Сведения, составляющие конфиденциальную информацию могут быть выражены в письменной, устной и электронной формах. Конфиденциальная информация, ставшая известной работнику из письменных, устных и электронных источников, охраняется равным образом.

6.2. Все документы, содержащие конфиденциальную информацию должны сохраняться в режиме конфиденциальности и быть доступными только тем лицам, которые имеют допуск к такой информации в силу исполнения ими своих должностных обязанностей.

6.3. Организация конфиденциального делопроизводства должна исключать ознакомление с информацией иных лиц, не имеющих такого доступа.

6.4. Приказом директора по каждому структурному подразделению назначается лицо, ответственное за учет, хранение и использование

конфиденциальной информации.

6.5. Контроль за порядком допуска и работы с конфиденциальной информацией осуществляет руководитель структурного подразделения, в котором осуществляется работа и хранение информации, относящейся к конфиденциальной.

6.6. Движение документов, содержащих сведения конфиденциального характера, в обязательном порядке отражается в Журнале учета движения документов, содержащие сведения конфиденциального характера (Приложение №6).

6.7. При осуществлении контроля лицо, указанное в п. 6.5 настоящего Положения, проверяет:

- ведение журналов учета при работе с конфиденциальной информацией;
- состояние помещения, предназначенного для работы с конфиденциальной информацией;
- наличие носителей конфиденциальной информации.

6.8. В случае необходимости оперативного доведения до заинтересованных лиц сведений конфиденциального характера руководителем структурного подразделения ставится резолюция, которая должна содержать: перечень фамилий работников, обязанных ознакомиться с документами или их исполнить, срок исполнения, другие указания, подпись руководителя и дату. Руководитель может при необходимости предусмотреть ограничения в доступе конкретных работников к определенным сведениям.

6.9. При работе с документами, содержащими сведения конфиденциального характера, запрещено:

- делать выписки в целях, не связанных с осуществлением трудовой функции;
- знакомить с такими документами, в том числе в электронном виде, других лиц, не имеющих соответствующего доступа;
- использовать информацию из таких документов в открытых сообщениях, докладах, переписке, рекламных изданиях (такое использование допускается только при условии обезличивания информации);
- оставлять на рабочем месте документы и иные носители конфиденциальной информации;
- не допускать к компьютерам, содержащим конфиденциальную информацию, посторонних лиц;
- не оставлять включенными компьютеры, содержащие конфиденциальную информацию.

6.10. Передача документов, содержащих конфиденциальную информацию, неуполномоченным лицам допускается, если обработка необходима:

- для исполнения гражданско-правового договора и в соответствии с условиями договора;
- для осуществления правосудия, исполнения судебного акта, акта другого органа или должностного лица;
- для защиты жизни или жизненно важных интересов гражданина;
- для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации либо научной, литературной

или иной творческой деятельности при условии, что при этом не нарушаются права и законные интересы граждан;

- в интересах гражданина и с его письменного согласия.
- для иных целей, предусмотренных законодательством РФ.

6.11. Уничтожение документов, содержащих конфиденциальную информацию осуществляется в следующими способами: сжигание, плавление, шредирование, химическая обработка. В каждом случае уничтожения составляется акт.

6.12. Проверка соблюдения требований настоящего Положения осуществляется в соответствии с Правилами осуществления внутреннего контроля.

7. Ответственность за нарушение режима конфиденциальности

7.1. К способам нарушения режима конфиденциальности относятся:

- разглашение конфиденциальной информации, обладание которыми входит в круг служебных обязанностей сотрудника, другим сотрудникам, у которых в силу своего служебного положения нет к ним доступа, а также третьим лицам, не являющимся сотрудниками Центра;
- разглашение сведений, которые были получены случайным образом, сотрудникам, не имеющим доступа к данной информации, а также третьим лицам, не являющимся сотрудниками Центра;
- неправомерное использование конфиденциальной информации;
- утрата документов и иных материальных носителей, содержащих сведения конфиденциального характера;
- неправомерное уничтожение документов, содержащих сведения конфиденциального характера;
- нарушение требований хранения документов, содержащих сведения конфиденциального характера;
- получение информации, составляющей коммерческую тайну, с использованием специальных средств или путем противоправных действий;
- другие нарушения требований законодательства и настоящего Положения.

7.2. За разглашение конфиденциальной информации, а также за нарушение порядка обращения с документами, содержащими сведения конфиденциального характера, работник организации несут предусмотренную законодательством Российской Федерации ответственность и может быть привлечен к дисциплинарной, административной или уголовной ответственности.

Заместитель директора по заочному,
дистанционному обучению и
информационным технологиям Г.В. Лашина

Помощник директора по безопасности
образовательного процесса Д. В. Халемин

Приложение № 1
к Положению о конфиденциальной
защите информации ГАУ ДПО РБ
«Центр повышения квалификации»

Документы, использованные при разработке Положения:

1. Гражданский кодекс РФ (часть четвертая) от 18.12.2006 г. № 230-ФЗ.
2.Федеральный закон РФ № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон РФ № 98-ФЗ от 29.07.2004 г. «О коммерческой тайне».
4. Федеральный закон РФ № 152-ФЗ от 27.07.2006 г. «О персональных данных».
5. Федеральный закон РФ № 208-ФЗ от 26.12.1995 г. «Об акционерных обществах».
6. Постановление правительства РФ № 781 от 17.11.2007 г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
7. Постановление правительства РСФСР № 35 от 05.12.1991 г. «О перечне сведений, которые не могут составлять коммерческую тайну".
8. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».
9. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 г. №1119.
10.ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
11.ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
12.ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».
13. Указ Президента РФ №188 от 06.03.1997 года «Об утверждении перечня сведений конфиденциального характера».
14. О перечне сведений, которые не могут составлять коммерческую тайну: Постановление правительства РСФСР от 05.12.1991 г. №35.
15. ГОСТ Р ИСО/МЭК 27002-2012 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

Приложение 2

Перечень конфиденциальной информации Центра

К конфиденциальной информации относятся следующие сведения и документы:

1) сведения о применяемых методах управления в организации;
2) сведения о стратегических целях Центра;
3) сведения о подготовке, принятии и исполнении решений руководителя по коммерческим, организационным, производственным, научно-техническим и иным вопросам;
4) сведения о планах расширения или сокращения реализации различных видов образовательных услуг и продукции, оказания услуг, выполнения работ и их технико-экономических обоснованиях;
5) сведения о подготовке и результатах проведения переговоров с деловыми партнерами учреждения;
6) сведения о планируемых и заключенных контрактах, договорах, соглашениях о взаимном сотрудничестве;
7) информация о финансово-хозяйственной деятельности;
8) сведения, условия конфиденциальности которых установлены в договорах, контрактах, соглашениях и других обязательствах;
9) сведения о бухгалтерской, налоговой и управленческой отчетности, сведения о движении средств, сведения о финансовых операциях, сведения о состоянии банковских счетов и производимых операциях, сведения о долговых обязательствах;
10) первичные регистры бухгалтерского, налогового и управленческого учета сведения об интеллектуальной собственности;
11) сведения о применяемых методах и средствах защиты помещений, техники, сетей, другого оборудования от утечки защищаемой информации, несанкционированного воздействия на защищаемую информацию;
12) сведения о состоянии и мерах по совершенствованию системы защиты конфиденциальной информации;
13) сведения о результатах проверок состояния защиты информации;
14) сведения о потенциальных каналах утечки информации;
15) отчетность, содержащая анализ состояния организационно-технических средств защиты информации;
16) сведения об используемых сетевых адресах и паролях автоматизированных систем;
17) содержание базы данных и программного обеспечения автоматизированных систем;

18) данные о лицах, получивших доступ к конфиденциальной информации;
19) сведения о паролях, ключах, электронных цифровых подписях;
20) сведения об установленных программных средствах, автоматизированных системах управления, системах связи и передачи данных, о серверном оборудовании осуществляющие прием, обработку, хранение и передачу информации с ограниченным доступом;
21) сведения о доходах и расходах структурного подразделения и по Центру;
22) информация об авторских программах;
23) сведения о планах по проведению антитеррористических мероприятий и мероприятий противопожарной безопасности, гражданской обороны;
24) сведения о работниках и слушателях:
- фамилия, имя, отчество;
- год, месяц и дата рождения;
- место рождения;
- адрес регистрации и фактического проживания;
- ИНН, СНИЛС;
- семейное, социальное, имущественное положение;
-данные об образовании (аттестат, диплом, сертификат и другие документы об образовании);
- ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
- профессия, специальность, занимаемая должность;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате и иных видах доходов работников Центра;
- сведения о социальных льготах;
- контактная информация: e-mail, телефон (домашний и мобильный);
- место работы или учебы членов семьи и других родственников;
- сведения о наличие (отсутствие) судимости;
- сведения о временной нетрудоспособности;
- сведения о заключенных договорах;
- сведения о прохождении конкурсов;
- сведения из личного дела;
- сведения о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении;
- данные, подтверждающие право на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством;

- сведения о родителях (законных представителях), данные паспортных данных, адресах регистрации и фактического проживания, номера домашних и мобильных телефонов;
- категория семьи для оказания материальной и других видов помощи и сбора отчетности по социальному статусу контингента;
- сведения о попечительстве, опеке, отношении к группе социально незащищенных обучающихся; документы (сведения), подтверждающие право на льготы, дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т. п.);
- сведения об инвалидности, о наличии хронических заболеваний и т.п.

Приложение 3

СОГЛАСИЕ РАБОТНИКА НА ОБРАБОТКУ ЕГО ПЕРСОНАЛЬНЫХ ДАННЫХ

Я,

(фамилия, имя, отчество)

зарегистрированный(ная) по адресу _____ .

паспорт серия_____№_____, выдан_____
(дата и кем выдан)

настоящим _____ (даю свое согласие/не даю свое согласие) работодателю (оператору) Государственное автономное учреждение дополнительного профессионального образования Республики Башкортостан «Центр повышения квалификации», зарегистрированному по адресу: г. Уфа, ул. Лесной проезд, д. 3/1, на обработку моих персональных данных и подтверждаю, что, давая такое согласие, я действую в своей воле и в своих интересах.

Согласие дается мною для целей: исполнения прав и обязанностей сторон трудового договора, исполнения законодательства (передача отчетности и др.) в сфере социального страхования, законодательства в сфере воинского учета, пенсионного, налогового законодательства, бухгалтерского учета, исполнения требований других федеральных законов, а так же в образовательных целях, для информирования потребителей образовательных услуг, для награждения в Центре и в других организациях, органах государственной власти, органах местного самоуправления, для предоставления льгот и гарантий, установленных действующими нормами законодательства, для ведения кадровых документов, для публичного вручения новогодних подарков, медалей, грамот, благодарственных писем, ценных подарков, для осуществления расчетов работодателя со мной как работником и распространяется на следующую информацию:

1. фамилия, имя, отчество;
2. год, месяц и дата рождения, место рождения;
3. адрес регистрации и фактического проживания;
4. ИНН, СНИЛС;
5. семейное, социальное, имущественное положение;
6. образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому)
7. ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
8. профессия, специальность, занимаемая должность;
9. фотография;
10. сведения о трудовом и общем стаже;
11. сведения о составе семьи;
12. номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
13. сведения о воинском учете;
14. сведения о заработной плате;
15. сведения о льготах;
16. контактная информация: e-mail, телефон (домашний и мобильный);
17. анкета, автобиография;
18. место работы или учебы членов семьи и других родственников;
19. содержание трудового договора;

20. подлинники и копии приказов, а также основания к ним;
21. личное дело и трудовая книжка;
22. наличие (отсутствие) судимости;
23. дела, содержащие материалы по повышению квалификации и переподготовке, аттестации, служебных расследованиях;
24. копии отчетов, направляемые в органы статистики и другая информация;
25. сведения о поощрениях и наказаниях;
26. сведения о временной нетрудоспособности;
27. сведения о других договорах (индивидуальной, коллективной материальной ответственности, ученических);
28. результаты обязательных медицинских осмотров (обследований), а также обязательного психиатрического осмотра и освидетельствования.

Согласна(ен) на совершение работодателем следующих действий в отношении моих персональных данных, которые необходимы для достижения указанных выше целей, включая:

1. Сбор, систематизацию, накопление, хранение; уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных следующими способами: автоматизированная обработка и (или) обработка без использования средств автоматизации;
2. Указание во внутреннем телефонном справочнике Центра фамилии, имени, отчества, должности;
3. Указание под фотографией на доске почета фамилии, имени, отчества, должности;
4. Указание на пропуске на территорию Центра фамилии, имени, отчества, должности вместе с фотографией;
5. Размещение на официальном сайте Центра следующей информации обо мне: фамилии, имени, отчества, адреса электронной почты, фотографии, номера рабочего телефона; списка опубликованных трудов и статей.
6. Для публичного поздравления с днем рождения, с юбилеями, с повышением квалификации и (или) профессиональной переподготовкой, с участием в мероприятиях Центра и за его пределами размещение на мониторах, информационных стендах и официальном сайте университета следующей информации: фамилии, имени, отчества, должности, данных о повышении квалификации и (или) профессиональной переподготовки, наименования мероприятий и результаты участия в них;
7. Для награждения в Центре и в других организациях сбор, систематизация, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), уничтожение следующими способами: автоматизированная обработка и (или) обработка без использования средств автоматизации вышеуказанных персональных данных;
8. Размещение на информационных стендах моей фотографии с указанием под ней фамилии, имени, отчества, должности;

Настоящее заявление может быть отозвано мной в письменной форме.

Данное согласие действует с « _____» _____ 20 _ г. и на весь период трудовых отношений с работодателем, а также в течение 75 лет после расторжения трудового договора, согласно части 1 статьи 17 Закона от 22 октября 2004 г. № 125-ФЗ «Об архивном деле в Российской Федерации».

Приложение 4

Форма обязательства о неразглашении конфиденциальной информации

ОБЯЗАТЕЛЬСТВО о неразглашении конфиденциальной информации

Я, _____
(ФИО)
(должность)

в период трудовых отношений с Государственным автономным учреждением дополнительного профессионального образования Республики Башкортостан «Центр повышения квалификации» (далее – Центр) и в течение трех лет после их прекращения обязуюсь:

1. Не разглашать сведения, составляющие конфиденциальную информацию в Центре, которые мне будут доверены или станут известны по работе.
2. Не передавать третьим лицам и не раскрывать публично сведения, составляющие конфиденциальную информацию о Центре.
3. Выполнять требования Приказов, инструкций и положений по обеспечению сохранности конфиденциальной информацию о Центре.
4. В случае попытки посторонних лиц получить от меня конфиденциальную информацию о Центре сообщить об этом факте непосредственному руководителю.
5. Сохранять конфиденциальную информацию тех юридических и физических лиц, с которыми у Центра имелись/имеются деловые отношения.
6. Не использовать знание конфиденциальной информации Центра для занятий любой деятельностью, которая может нанести ущерб Центру, за исключением случаев, установленных законодательством РФ.
7. В случае моего увольнения все носители конфиденциальной информации Центра (рукописи, черновики, машинные носители, распечатки на принтерах, изделия и пр.), которые находились в моем распоряжении в связи с выполнением мною служебных обязанностей во время работы в Центре передать непосредственному руководителю.
8. Об утрате или недостаче носителей конфиденциальной информации, ключей, специальных пропусков, удостоверений от режимных помещений, хранилищ, сейфов, архивов, личных печатей, которые могут привести к разглашению конфиденциальной информации Центра, а также о причинах и условиях возможной утечки сведений немедленно сообщать непосредственному руководителю.

Я предупрежден (а), что в случае невыполнения любого из вышеуказанных пунктов настоящего Обязательства, ко мне могут быть применены меры дисциплинарного взыскания в соответствии с трудовым законодательством РФ, вплоть до увольнения из Центра.

Я ознакомлен (а) с законодательством о защите конфиденциальной информации и с локальными нормативными актами о защите конфиденциальной информации в Центре.

Мне известно, что нарушение требований по обеспечению сохранности конфиденциальной информации Центра может повлечь уголовную, административную, гражданско-правовую или иную ответственность в соответствии с законодательством Российской Федерации, в виде лишения свободы, денежного штрафа, обязанности по возмещению ущерба Центру (убытков, упущенной выгоды) и других наказаний.

Дата подпись расшифровка

Приложение 5

Форма расписки об ознакомлении с нормативными правовыми актами в сфере защиты конфиденциальной информации

РАСПИСКА

я_____

(Ф.И.О. работника)
(структурное подразделение, должность).

ознакомлен с:

- 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»;
- Положением о защите конфиденциальной информации в Государственное автономное учреждении дополнительного профессионального образования Республики Башкортостан «Центр повышения квалификации»(Центра), утвержденного _____;

Дата

Права и обязанности в области защиты конфиденциальной информации и защиты персональных данных мне разъяснены.

Подпись Расшифровка

Приложение 6

Форма журнала учета движения документов, содержащие сведения конфиденциального характера

Номер	Дата и № регистрации	Откуда (от кого) поступил или кому направлен документ	Наимеование или краткое содержание документа	Фамилия исполнителя и подразделение	Количество экземпляров и их номера	Количество листов в экземпляре	Отметка об уничтожении	Кому выдан документ и с какой целью	Расписка в получении и документа	Расписка принявшего документ и дата