Приложение № 2
к приказу СПб ГАУ «ЦГЭ»
от «24» марта 2022 г.
№ 29

Положение

о порядке обработки и обеспечения безопасности персональных данных субъектов персональных данных, не являющихся работниками Санкт-Петербургского государственного автономного учреждения «Центр государственной экспертизы»

Оглавление

1. Термины и определения

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

Персональные данные, разрешенные субъектом персональных данных для распространения – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;

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;

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;

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники;

Распространение персональных данных – действия, направленные на раскрытие персональных данных неопределенному кругу лиц;

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

Блокирование персональных данных – временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных);

Материальные носители – любой материальный объект или среда, способный длительное время сохранять в своей структуре занесённую на него информацию;

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных;

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

субъекту персональных данных;

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Информационная система персональных данных (далее – ИСПДн) – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

Администратор ИСПДн – субъект уполномоченный осуществлять управление ИСПДн, включая конфигурирование, разработку и внедрение компонентов информационной системы.

Администратор безопасности информации – субъект уполномоченный осуществлять защиту информации, содержащейся в информационной системе.

2. Общие положения

Положение о порядке обработки и обеспечения безопасности персональных данных, не являющихся работниками Санкт-Петербургского государственного автономного учреждения «Центр государственной экспертизы» (далее – Положение и СПб ГАУ «ЦГЭ» соответственно), устанавливает требования к обработке и защите персональных данных, определяет права, обязанности и ответственность руководителей структурных подразделений и работников СПб ГАУ «ЦГЭ».

Настоящее Положение подлежит применению только в отношении тех персональных данных, в отношении которых СПб ГАУ «ЦГЭ» является оператором. В случаях, когда СПб ГАУ «ЦГЭ» только выполняет отдельные функции по обработке персональных данных, следует руководствоваться требованиями по обработке и защите персональных данных, установленными соответствующим оператором. В случае отсутствия таких требований следует руководствоваться настоящим Положением и Руководством по защите конфиденциальной информации в СПб ГАУ «ЦГЭ» (далее – Руководство по защите информации). При этом выполнение мероприятий, которые должны быть выполнены оператором (классификация информационной системы персональных данных, разработка модели угроз и нарушителя персональных данных и т.д.), не требуется.

Работники СПб ГАУ «ЦГЭ» допускаются к обработке персональных данных в объеме, определяемом их должностными обязанностями.

3. Обработка персональных данных

Персональные данные обрабатываются в целях:

- осуществление финансово-хозяйственной деятельности;
- обеспечения проведения экспертизы;
- ведения образовательной деятельности;
- приема и регистрации обращений граждан и организаций;
- обеспечения соблюдения законов и иных нормативных правовых

актов;

– иных предусмотренных законодательством целях, необходимых для реализации полномочий СПб ГАУ «ЦГЭ».

Источником информации обо всех персональных данных, обрабатываемых СПб ГАУ «ЦГЭ», является непосредственно субъект персональных данных или его законный представитель.

СПб ГАУ «ЦГЭ» не вправе получать и обрабатывать сведения, относящиеся в соответствии с законодательством Российской Федерации в области персональных данных к специальным категориям персональных данных, за исключением случаев, предусмотренных законодательством Российской Федерации.

В СПб ГАУ «ЦГЭ» ведется учет обрабатываемых персональных данных. Примерная форма соответствующего перечня и его заполнение приведены в Приложении № 1 к настоящему Положению.

Согласие на обработку персональных данных может быть дано субъектом персональных данных или его законным представителем в любой позволяющей подтвердить факт его получения форме. Форма согласия на обработку персональных данных, предоставляемого с использованием информационных ресурсов СПб ГАУ «ЦГЭ», расположенных в сети Интернет, приведена в Приложении № 2 к настоящему Положению. Форма письменного согласия на обработку персональных данных приведена в Приложении № 3 к настоящему Положению.

Обработка персональных данных может осуществляться и без получения такого согласия в следующих случаях:

– обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

– обработка персональных данных осуществляется на основании закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке;

– обработка персональных данных осуществляется для статистических или иных научных целей, при условии обязательного обезличивания персональных данных;

– по требованию полномочных государственных органов - в случаях, предусмотренных федеральными законами.

При обработке персональных данных соблюдаются следующие общие требования:

– при определении объема и содержания обрабатываемых персональных данных СПб ГАУ «ЦГЭ» руководствуется федеральными законами;

– при принятии решений, затрагивающих интересы субъекта

персональных данных, СПб ГАУ «ЦГЭ» не вправе основываться на сведениях, полученных исключительно в результате автоматизированной обработки персональных данных;

– персональные данные при их обработке, осуществляемой без использования средств автоматизации, обособляются от иной информации, в частности путем фиксации их на разных материальных носителях;

– СПб ГАУ «ЦГЭ» обеспечивается защита персональных данных субъектов персональных данных от их неправомерного использования, утраты;

Обработка персональных данных включает в себя следующие действия: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

Способы обработки персональных данных включают в себя:

– копирование оригиналов документов;

– внесение сведений в учетные формы (на бумажных и электронных носителях);

– формирование персональных данных в ходе их обработки;

– внесение персональных данных в ИСПДн СПб ГАУ «ЦГЭ»;

– непосредственное получение оригиналов необходимых документов.

В СПб ГАУ «ЦГЭ» ведется учет информационных систем персональных данных, оператором которых является СПб ГАУ «ЦГЭ». Примерная форма соответствующего перечня и его заполнения приведены в Приложении № 4 к настоящему Положению.

Для ИСПДн определяется их уровень защищенности в соответствии с регламентирующими документами. Соответствующее решение принимается постоянно действующей технической комиссией по обеспечению безопасности информации, создаваемой на основании приказа СПб ГАУ «ЦГЭ». По результатам работы комиссии утверждается акт. Примерная форма акта приведена в Приложении № 5 к настоящему Положению.

Все персональные данные и их носители уничтожаются в порядке, предусмотренном для уничтожения документов, по достижении цели, для которой они собирались и использовались, если иное не установлено действующим законодательством Российской Федерации.

Все работники СПб ГАУ «ЦГЭ», допущенные к обработке персональных данных, подписывают обязательство о неразглашении конфиденциальной информации (форма обязательства приведена в Приложение № 12 к настоящему Положению).

4. Доступ к персональным данным

В СПб ГАУ «ЦГЭ» утверждается перечень должностей работников, которым необходим доступ к персональным данным для выполнения служебных обязанностей. Примерная форма перечня приведена в Приложении № 6 к настоящему Положению.

В случае если СПб ГАУ «ЦГЭ» на основании заключенных государственных контрактов, договоров, либо на иных законных основаниях оказывают услуги юридические или физические лица, и такие лица должны получить доступ к персональным данным, то соответствующие персональные данные предоставляются только после подписания указанными лицами обязательства о неразглашении конфиденциальной информации или включения в соответствующие договоры положений о неразглашении конфиденциальной информации, в том числе персональных данных.

Органам государственной власти и иным организациям, осуществляющим функции контроля (надзора), предоставляется доступ к персональным данным, обрабатываемым в СПб ГАУ «ЦГЭ», только в пределах их компетенции,в объеме и на основаниях, предусмотренных действующим законодательством Российской Федерации.

5. Передача персональных данных

Запрещается передавать персональные данные третьей стороне без письменного согласия субъекта персональных данных, за исключением случаев, когда это необходимо в целях предупреждения угрозы его жизни и здоровью, а также в случаях, установленных законодательством Российской Федерации.

Персональные данные могут передаваться с использованием защищенных в установленном порядке каналов связи.

Передача персональных данных на бумажных или иных материальных носителях информации осуществляется с оформлением сопроводительных писем, регистрируемых установленным порядком) или по акту приема-передачи, если сопроводительное письмо отсутствует. Примерная форма акта приведена в Приложении № 7 к настоящему Положению.

Между структурными подразделениями СПб ГАУ «ЦГЭ» разрешается передача (представление) персональных данных для выполнения возложенных на них функций без письменного согласия субъекта персональных данных. При этом персональные данные могут быть использованы лишь в целях, для которых они переданы (получены), а также должен соблюдаться режим конфиденциальности персональных данных, не отнесенных к разрешенным субъектом персональных данных для распространения.

6. Порядок хранения персональных данных

Хранение персональных данных осуществляется в порядке, исключающем бесконтрольный доступ к ним, их утрату или неправомерное использование. Документы, содержащие персональные данные, должны храниться в надежно запираемых хранилищах (шкафах), также допускается их хранениев незапираемых шкафах (ящиках), при условии, что бесконтрольный доступ посторонних лиц в помещения исключен.

Помещения, в которых ведется обработка персональных данных, оборудуются таким образом, чтобы обеспечивать их сохранность, исключить возможность бесконтрольного проникновения в них посторонних лиц.

По окончании рабочего времени такие помещения запираются на ключ, бесконтрольный доступ в них исключается.

Хранение персональных данных в форме, позволяющей определить субъекта персональных данных, осуществляется не дольше, чем этого требуют цели обработки персональных данных, если срок хранения персональных данных не установлен законами Российской Федерации или договором, стороной которого, выгодоприобретателем или поручителем, по которому является субъект персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено законами Российской Федерации.

По истечении сроков, определенных законодательством Российской Федерации, документы передаются на архивное хранение.

Срок хранения персональных данных, внесенных в ИСПДн, должен соответствовать сроку хранения бумажных носителей персональных данных.

7. Права субъектов на защиту своих персональных данных

В целях обеспечения защиты своих персональных данных субъект персональных данных имеет право:

– получать полную информацию о своих персональных данных и обработке этих данных (в том числе автоматизированной);

– осуществлять свободный бесплатный доступ к своим персональным данным, включая право получать копии любой записи, содержащей персональные данные, за исключением случаев, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». Факт обращения субъекта персональных данных отражается в «Журнале учета обращений субъектов персональных данных или их представителей, а также уполномоченного органа по защите прав субъектов персональных данных» (далее – Журнал обращений). Примерная форма журнала обращений приведена в Приложении № 8 к настоящему Положению.

– требовать исключения или исправления неверных, или неполных персональных данных, а также данных, обработанных с нарушением Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

– при отказе исключить или исправить персональные данные субъект вправе заявить в письменной форме о своем несогласии, обосновав соответствующим образом такое несогласие; персональные данные оценочного характера субъект вправе дополнить заявлением, выражающим его собственную точку зрения;

– обжаловать в суде любые неправомерные действия или бездействие при обработке и защите своих персональных данных;

– вносить предложения по мерам защиты персональных данных.

8. Защита персональных данных

Обеспечение безопасности персональных данных, обрабатываемых в СПб ГАУ «ЦГЭ», достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, а также принятия следующих мер по их защите:

– определение актуальных угроз безопасности персональных данных, в том числе при их обработке в ИСПДн;

– применение организационных и технических мер по обеспечению безопасности персональных данных, в том числе при их обработке в ИСПДн, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает необходимый уровень защищенности персональных данных;

– применение средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия требованиям по безопасности информации;

– учет машинных носителей персональных данных;

– обеспечение функционирования средств обработки персональных данных, а также средств защиты информации в соответствии с эксплуатационной и технической документацией;

– обнаружение и регистрация фактов несанкционированного доступа к персональным данным, несанкционированной повторной и дополнительной записи информации после ее извлечения из ИСПДн;

– восстановление персональных данных, модифицированных или удаленных (уничтоженных) вследствие несанкционированного доступа к ним;

– установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

– контроль за принимаемыми мерами по обеспечению безопасности персональных данных и защищенностью ИСПДн.

Актуальные угрозы безопасности персональных данных определяются в соответствии с моделью угроз и нарушителя безопасности персональных данных при их обработке в СПб ГАУ «ЦГЭ».

Защита персональных данных обеспечивается путем применения комплекса организационных и технических мер по обеспечению безопасности персональных данных. Меры по обеспечению защищенности персональных данных, обрабатываемых в СПб ГАУ «ЦГЭ», отражаются в Руководстве по защите информации.

Лица, ответственные за организацию обработки персональных данных, должны осуществлять контроль за соблюдением правил обработки персональных данных, в том числе в ИСПДн.

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

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

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

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

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

Работники, осуществляющие обработку персональных данных без использования средств автоматизации, должны быть:

а) ознакомлены с документами, определяющими особенности и правила обработки персональных данных, в том числе с:

– федеральным законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

– постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

– настоящим Положением.

б) проинформированы о факте обработки ими персональных данных, обработка которых осуществляется без использования средств автоматизации, и категориях обрабатываемых персональных данных.

При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных, должны соблюдаться требования пункта 7 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств

автоматизации».

Не допускается совместное хранение персональных данных различной категории.

Обеспечивается раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях.

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, принимаются меры по обеспечению раздельной обработки персональных данных, в частности меры, приведенные в пункте 9 Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, утвержденного постановлением Правительства Российской Федерации от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

При хранении материальных носителей персональных данных должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним. Места хранения документов, содержащие персональные данные, должен размещаться в пределах контролируемой зоны.

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.

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).

В целях уничтожения документов, содержащих персональные данные, создается комиссия по уничтожению персональных данных на материальных носителях.

Уничтожение производится с оформлением акта об уничтожении материальных носителей, содержащих персональные данные. Примерная форма приложения приведена в Приложении № 10 к настоящему Положению.

10. Порядок взаимодействия с субъектами персональных данных

Организация и проведение работ по взаимодействию с субъектами персональных данных (ответы на запросы, устранение нарушений, уточнение, блокирование, уничтожение персональных данных и т.п.) возлагается на лицо,

ответственное за обработку персональных данных.

Субъект персональных данных или его законный представитель имеет право на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

– подтверждение факта обработки персональных данных оператором;

– правовые основания и цели обработки персональных данных;

– цели и применяемые оператором способы обработки персональных данных;

– наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального закона;

– обрабатываемые персональные данные, относящиеся к соответствующему субъекту персональных данных, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законом;

– сроки обработки персональных данных, в том числе сроки их хранения;

– порядок осуществления субъектом персональных данных прав, предусмотренных законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»;

– информацию об осуществленной или о предполагаемой трансграничной передаче данных;

– наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка поручена или будет поручена такому лицу;

– иные сведения, предусмотренные законом Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных» или другими законами Российской Федерации.

Субъект при наличии оснований вправе требовать уточнения, блокирования, уничтожения персональных данных о себе.

Субъект вправе обратиться в СПб ГАУ «ЦГЭ» повторно или направить повторный запрос в целях получения сведений, указанных выше, и ознакомления с ними не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен законами Российской Федерации или договором, стороной которого либо выгодоприобретателем или поручителем является субъект персональных данных.

Основанием для отказа в предоставлении информации, касающейся обработки персональных данных субъекта может быть:

– нарушение прав и законных интересов третьих лиц при доступе субъекта к его персональным данным;

– несоответствие требованиям подачи запроса или обращения и др.

Порядок и сроки обработки обращений и запросов субъектов персональных данных, их законных представителей и представителей уполномоченного органа по защите прав субъектов персональных данных регламентируются Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных».

Поступивший запрос субъекта персональных данных или его законного представителя либо уполномоченного органа по защите прав субъектов персональных данных необходимо зарегистрировать в соответствующем журнале учета обращений.

При личном обращении субъекта персональных данных в СПб ГАУ «ЦГЭ» ответственный работник принимает запрос, который может быть составлен в произвольной форме. После принятия обращения ответственный работник сверяет сведения в обращении с предоставленными ему документами.

Необходимые сведения о субъекте персональных данных, которые должны присутствовать в подаваемом запросе:

– фамилия, имя и отчество субъекта персональных данных;

– номер основного документа, удостоверяющего личность субъекта персональных данных или его законного представителя;

– сведения о дате выдачи указанного документа и выдавшем его органе;

– сведения, подтверждающие участие субъекта персональных данных в отношениях с СПб ГАУ «ЦГЭ», либо сведения, подтверждающие факт обработки СПб ГАУ «ЦГЭ» персональных данных субъекта,

– собственноручную подпись субъекта персональных данных или его законного представителя.

Запрос может быть направлен в форме электронного документа и подписан электронной подписью.

В случае отсутствия документов, удостоверяющих личность субъекта персональных данных или его законного представителя, ответственный работник вправе отказать в приеме обращения.

Форма справки о порядке обработки обращений субъектов персональных данных, их законных представителей или уполномоченного органа по защите прав субъектов персональных данных представлена в Приложении № 9 к настоящему Положению.

11. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных

Работник СПб ГАУ «ЦГЭ», имеющий доступ к персональным данным, несет ответственность за нарушение режима защиты персональных данных в соответствии с законодательством Российской Федерации.

За неисполнение или ненадлежащее исполнение работником обязанностей по соблюдению установленного порядка работы с персональными данными или порядка обеспечения безопасности персональных данных могут быть применены дисциплинарные взыскания, предусмотренные статьями 81 и 192 Трудового кодекса Российской Федерации.

Утрата документов, содержащих персональные данные, либо незаконное использование, получение и разглашение таких сведений влечет за собой ответственность, предусмотренную законодательством Российской Федерации.

12. Контроль выполнения требований настоящего Положения

Повседневный контроль соблюдения порядка обращения с персональными данными осуществляют руководители структурных подразделений СПб ГАУ «ЦГЭ», в которых обрабатываются персональные данные.

Периодический контроль выполнения требований, установленных настоящим Положением, осуществляется постоянно действующей технической комиссией по обеспечению безопасности информации в СПб ГАУ «ЦГЭ». В состав данной комиссии в обязательном порядке должны входить лицо, назначенное ответственным за организацию обработки персональных данных, а также администратор безопасности информации. Работа комиссии организуется с учетом Регламента осуществления внутреннего контроля соответствия обработки персональных данных (Приложение № 11 к настоящему Положению).

Приложение № 1
к Положению о порядке обработки
и обеспечения безопасности персональных
данных субъектов персональных данных,
не являющихся работниками СПб ГАУ «ЦГЭ»

Примерная форма
перечня персональных данных, обрабатываемых в Санкт-Петербургском
государственном автономном учреждении «Центр государственной экспертизы»

№ п/п	Персональные данные работников СПб ГАУ «ЦГЭ»	Цель обработки персональных данных
1	Фамилия, имя, отчество	- осуществление финансово-хозяйственной деятельности; - обеспечение проведения экспертизы; - ведение образовательной деятельности; - прием и регистрации обращений граждан и организаций; - обеспечения соблюдения законов и иных нормативных правовых актов
2	Пол	- осуществление финансово-хозяйственной деятельности; - обеспечение проведения экспертизы; - ведение образовательной деятельности; - прием и регистрации обращений граждан и организаций; - обеспечение соблюдения законов и иных нормативных правовых актов
3	и. т.д.	

Приложение № 2

к Положению о порядке обработки
и обеспечения безопасности персональных
данных субъектов персональных данных,
не являющихся работниками СПб ГАУ «ЦГЭ»

Согласие на обработку персональных данных предоставляемых
с использованием информационных ресурсов СПб ГАУ «ЦГЭ»

Пользователь (субъект персональных данных), заполняя данную форму на официальном сайте spbexp.ru СПб ГАУ «ЦГЭ» (далее – сайт), действуя свободно, а также подтверждая свою дееспособность, дает настоящее согласие.

1. Настоящее Согласие дается на обработку следующих персональных данных Пользователя (субъекта персональных данных):

– фамилия, имя, отчество, пол, возраст, СНИЛС, ИНН, почтовые и электронные адреса, телефонные номера Пользователя (субъекта персональных данных);

– вся информация, содержащаяся в направляемых Пользователем (субъектом персональных данных) посредством сайта файлах с резюме;

– системная информация, данные из браузеров Пользователя (субъекта персональных данных);

– файлы cookie Пользователя (субъекта персональных данных);

– IP-адреса Пользователя (субъекта персональных данных);

– сведения об установленных на устройствах операционных системах и типах браузеров Пользователя (субъекта персональных данных);

– сведения об установленных на устройствах расширениях и настройках цвета экрана Пользователя (субъекта персональных данных);

– сведения об установленных и используемых на устройствах Пользователя (субъекта персональных данных) языках;

– сведения о типах, используемых Пользователем (субъектом персональных данных) мобильных устройствах;

– географическое положение Пользователя (субъекта персональных данных);

– количество посещений Пользователем (субъектом персональных данных) сайта и просмотров страниц;

– длительность пребывания Пользователя (субъекта персональных данных) на сайте;

– запросы Пользователя (субъекта персональных данных), в том числе осуществленные Пользователем (субъектом персональных данных) при переходе на сайт;

– страницы, с которых Пользователем (субъектом персональных данных) были совершены переходы.

2. Персональные данные не являются персональными данными, разрешенными субъектом персональных данных для распространения.

3. Цель обработки персональных данных:

– обработка входящих запросов физических лиц, в том числе, представляющих интересы юридических лиц;

– аналитика действий физического лица на сайте;

– проведение новостных рассылок (в случае подписки на них Пользователя);

– организация подбора персонала (в случае направления Пользователем резюме).

4. В ходе обработки персональных данных будут производиться следующие действия:

– сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение);

– извлечение, использование (для целей, указанных в п.3), удаление, уничтожение.

5. Обработка персональных данных может быть прекращена по запросу Пользователя (субъекта персональных данных). Согласие может быть отозвано Пользователем (субъектом персональных данных) или его уполномоченным представителем путем направления письменного заявления в адрес СПб ГАУ «ЦГЭ».

6. В случае отзыва Пользователем (субъектом персональных данных) или его представителем данного Согласия, СПб ГАУ «ЦГЭ» вправе продолжить обработку его персональных данных только при наличии оснований, предусмотренных действующим законодательством Российской Федерации.

Приложение № 3
к Положению о порядке обработки
и обеспечения безопасности персональных
данных субъектов персональных данных,
не являющихся работниками СПб ГАУ «ЦГЭ»

Согласие на обработку персональных данных

Я , _____,
(фамилия, имя, отчество)

Документ, удостоверяющий личность _____ № _____,
(вид документа)

выдан
_____,
(кем и когда)

зарегистрированный (ая) по адресу: _____,

даю свое согласие СПб ГАУ «ЦГЭ» на обработку моих персональных данных:
_____
(перечислить персональные данные)
_____

Субъект дает согласие на обработку Оператором своих персональных данных, то есть совершение, в том числе, следующих действий: обработку (включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, обезличивание, блокирование, уничтожение персональных данных), при этом общее описание вышеуказанных способов обработки данных приведено в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», а также на передачу такой информации третьим лицам, в случаях, установленных нормативными документами вышестоящих органов и законодательством Российской Федерации.

Настоящее согласие действует бессрочно.

Настоящее согласие может быть отозвано мною в любой момент по соглашению сторон. В случае неправомерного использования предоставленных данных согласие отзывается письменным заявлением.

«____»_____ 20 г. _____ _____
Подпись *ФИО*

Подтверждаю, что ознакомлен (а) с положениями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

«____»_____ 20 г. _____ _____
Подпись *ФИО*

Приложение № 4
к Положению о порядке обработки
и обеспечения безопасности персональных
данных субъектов персональных данных,
не являющихся работниками СПб ГАУ «ЦГЭ»

Примерная форма
перечня информационных систем персональных данных в Санкт-Петербургском государственном автономном учреждении «Центр государственной экспертизы»

№	Наименование информационной системы	Состав	Назначение
1.	Информационная система персональных данных Санкт-Петербургского государственного автономного учреждения «Центр государственной экспертизы» (ИСПДн СПб ГАУ «ЦГЭ»)	1С: Бухгалтерия 8	Включает платформу системы программ «1С: Предприятие» и готовое прикладное решение - конфигурацию «Бухгалтерия» Программный продукт для автоматизации бухгалтерского учета и подготовки регламентированной отчетности
		1С: Зарплата и кадры	Включает платформу системы программ «1С: Предприятие» и готовое прикладное решение - конфигурацию «Зарплата и кадры» Программный продукт для расчета заработной платы и кадрового учета
		Информационный портал СПб ГАУ «ЦГЭ»	Корпоративный портал на платформе Битрикс 24 для организации единого рабочего и информационного пространства, включающий в себя функционал проектов, задач, справочников, управления персоналом.

Приложение № 5
к Положению о порядке обработки
и обеспечения безопасности персональных
данных субъектов персональных данных,
не являющихся работниками СПб ГАУ «ЦГЭ»

Примерная форма
акта об определении уровня защищенности персональных данных
при их обработке в ИСПДн

Дата

А К Т
об определении уровня защищенности персональных данных
при их обработке в ИСПДн
«_____»
наименование ИСПДн

Настоящий Акт составлен постоянно действующей технической комиссии по обеспечению безопасности информации в Санкт-Петербургском государственном автономном учреждении «Центр государственной экспертизы» (далее – СПб ГАУ «ЦГЭ»), созданной в соответствии с приказом СПб ГАУ «ЦГЭ» от _____ № _____ в составе:

Председатель комиссии: _____
должность ФИО

Члены комиссии:

_____
должность ФИО

_____
должность ФИО

_____
должность ФИО

с целью определения уровня защищенности персональных данных при их обработке в информационной системе _____ (далее – ИСПДн).
наименование ИСПДн

Перечень исходных данных, необходимых для определения уровня защищенности (УЗ) персональных данных при их обработке в ИСПДн, и их описание:

1С: Бухгалтерия			
№ п/п	***Наименование исходных данных***	***Описание исходных данных***	***Вывод***
1	Категории обрабатываемых ПДн	Обрабатываются ПДн, указанные в абзацах 1-3 пункта 5 постановления Правительства Российской Федерации от 01.11.2012 № 1119.	Обрабатываются **иные** категории ПДн

2	Принадлежность обрабатываемых ПДн	Обрабатываются ПДн работников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся работниками оператора.	Обрабатываются ПДн работников оператора.
3	Тип актуальных угроз безопасности ПДн	Угрозы **не связаны** с наличием недокументированных (недекларированных) возможностей в используемом системном и прикладном программном обеспечении.	Актуальны угрозы 3-го типа
1С: Зарплата и кадры			
4	Категории обрабатываемых ПДн	Обрабатываются ПДн, указанные в абзацах 1-3 пункта 5 постановления Правительства Российской Федерации от 01.11.2012 № 1119.	Обрабатываются **иные** категории ПДн
5	Принадлежность обрабатываемых ПДн	Обрабатываются ПДн работников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся работниками оператора.	Обрабатываются ПДн работников оператора
6	Тип угроз безопасности ПДн, актуальных для ИСПДн	Угрозы **не связаны** с наличием недокументированных (недекларированных) возможностей в используемом системном и прикладном программном обеспечении.	Актуальны угрозы 3-го типа
Информационный портал СПб ГАУ «ЦГЭ»			
7	Категории обрабатываемых ПДн	Обрабатываются ПДн, указанные в абзацах 1-3 пункта 5 постановления Правительства Российской Федерации от 01.11.2012 № 1119.	Обрабатываются **иные** категории ПДн
8	Принадлежность обрабатываемых ПДн	Обрабатываются ПДн работников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся работниками оператора.	Обрабатываются ПДн работников оператора
9	Тип угроз безопасности ПДн, актуальных для ИСПДн	Угрозы **не связаны** с наличием недокументированных (недекларированных) возможностей в используемом системном и прикладном программном обеспечении.	Актуальны угрозы 3-го типа

В соответствии с абзацем «б» пункта 12 постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах» комиссия РЕШИЛА:

Персональным данным при их обработке в ИСПДн установить уровень защищенности: **УЗ 4**

Председатель комиссии:

_____ _____
подпись ФИО

Члены комиссии:

_____ _____
подпись ФИО

_____ _____
подпись ФИО

Приложение № 6
к Положению о порядке обработки
и обеспечения безопасности персональных
данных субъектов персональных данных,
не являющихся работниками СПб ГАУ «ЦГЭ»

Примерная форма
перечня должностей работников Санкт-Петербургского государственного автономного учреждения «Центр государственной экспертизы», допущенных к персональным данным в связи с исполнением ими своих должностных обязанностей

№ п/п	Наименование должности работника	Категории субъектов персональных данных	Объем персональных данных, к которым допущены работники
1	Должностное лицо	Субъект персональных данных не являющийся работником	- фамилия, имя, отчество; - пол; - контактная информация (номера домашнего, личных и служебного телефонов);
2	и. т.д.		

Приложение № 7
к Положению о порядке обработки
и обеспечения безопасности персональных
данных субъектов персональных данных,
не являющихся работниками СПб ГАУ
«ЦГЭ»

Примерная форма
акта приема-передачи документов (иных материальных носителей),
содержащих персональные данные

Акт
приема-передачи документов (иных материальных носителей), содержащих персональные данные

Во исполнение _____
(дата и № запроса, договора, иное основание)

Санкт-Петербургское государственное автономное учреждение «Центр государственной экспертизы»
в лице _____
(Ф.И.О., должность работника, передающего документы (иные материальные носители), содержащие персональные данные)

передает _____
(наименование организации, принимающей документы (иные материальные носители), содержащие персональные данные)

в лице _____
(Ф.И.О., должность представителя организации, принимающей документы (иные материальные носители), содержащие персональные данные)

документы (иные материальные носители), содержащие следующие персональные данные:
_____
(указать перечень и круг субъектов передаваемых персональных данных)

на срок _____
(указывается, если изначально известен срок окончания обработки персональных данных)

в целях: _____
(указать цель передачи/получения)

Перечень документов (иных материальных носителей), содержащих персональные данные

№ п/п	Наименование, регистрационный номер и дата документа (иного материального носителя)	Кол-во
Всего		

Полученные персональные данные могут быть использованы лишь в целях, для которых они переданы. Неправомерное использование предоставленных персональных данных влечет ответственность в соответствии с действующим законодательством Российской Федерации.

Передал _____
(Ф.И.О., должность работника, осуществляющего передачу документов (иных материальных носителей), содержащих персональные данные)

Принял _____
(Ф.И.О., должность, представителя организации, принимающей документы (иные материальные носители), содержащие персональные данные)

Приложение № 8
к Положению о порядке обработки
и обеспечения безопасности персональных
данных субъектов персональных данных,
не являющихся работниками СПб ГАУ «ЦГЭ»

Примерная форма
журнала учета обращений субъектов персональных данных или их представителей, а также уполномоченного органа по защите прав субъектов персональных данных

№	Дата обращения	Сведения о запрашивающем лице	Краткое содержание обращения	Отметка о предоставлении или об отказе в предоставлении информации (предоставлено/отказано)	Дата передачи/отказа в предоставлении информации	ФИО/подпись запросившего лица	ФИО/подпись ответственного работника
1	2	3	4	5	6	7	8

Приложение № 9
к Положению о порядке обработки
и обеспечения безопасности персональных
данных субъектов персональных данных,
не являющихся работниками СПб ГАУ «ЦГЭ»

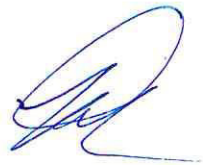
Справка о порядке обработки обращений субъектов персональных данных, их законных представителей или уполномоченного органа по защите прав субъектов персональных данных

№	Запрос	Действия	Срок	Ответ
1. Запрос субъекта персональных данных или его представителя				
1.1	Наличие ПДн	Подтверждение обработки ПДн	30 дней (согласно п. 1, ст. 20 152-ФЗ)	Подтверждение обработки ПДн
		Отказ подтверждения обработки		Уведомление об отказе подтверждения обработки
1.2	Ознакомление с ПДн	Предоставление информации по ПДн	30 дней (согласно п. 1, ст. 20 152-ФЗ)	1. Подтверждение обработки ПДн, правовые основания и цели обработки 2. Способы обработки ПДн 3. Сведения о лицах, которые имеют доступ к ПДн 4. Перечень обрабатываемых ПДн и источник их получения 5. Сроки обработки ПДн, в том числе сроки их хранения 6. Информация об осуществленных или о предполагаемой трансграничной передаче
		Отказ предоставления информации по ПДн		Уведомление об отказе предоставления информации по ПДн

1.3	Уточнение ПДн	Изменение ПДн	7 рабочих дней со дня предоставления уточняющих сведений (согласно п. 3 ст. 20 152-ФЗ)	Уведомление о внесенных изменениях
		Отказ изменения ПДн	30 дней	Уведомление об отказе предоставления изменения ПДн
1.4	Уничтожение ПДн	Уничтожение ПДн	7 рабочих дней со дня предоставления сведений о незаконном получении ПДн или отсутствии необходимости ПДн для заявленной цели обработки (согласно п. 3 ст. 20 152-ФЗ)	Уведомление об уничтожении
		Отказ уничтожения ПДн	30 дней	Уведомление об отказе уничтожения ПДн
1.5	Отзыв согласия на обработку ПДн	Прекращение обработки и уничтожение ПДн	30 рабочих дней (согласно п. 5 ст. 21 152-ФЗ)	Уведомление о прекращении обработки и уничтожении ПДн
		Отказ прекращения обработки и уничтожения ПДн	30 дней	Уведомление об отказе прекращения обработки и уничтожения ПДн

1.6	Недостоверность ПДн субъекта	Блокировка ПДн	С момента обращения субъекта ПДн о недостоверности или с момента получения запроса на период проверки (согласно п. 1 ст. 21 152-ФЗ)	Уведомление о внесенных изменениях
		Изменение ПДн	7 рабочих дней со дня предоставления уточненных сведений (согласно п. 2 ст. 21 152-ФЗ)	
		Снятие блокировки ПДн		
		Отказ изменения ПДн		Уведомление об отказе изменения ПДн
1.7	Неправомерность действий с ПДн субъекта	Прекращение неправомерной обработки ПДн	3 рабочих дня (согласно п. 3 ст. 21 152-ФЗ)	Уведомление об устранении нарушений
		Уничтожение ПДн в случае невозможности обеспечения правомерности обработки	10 рабочих дней (согласно п. 3 ст. 21 152-ФЗ)	Уведомление об уничтожении ПДн
1.8	Достижение целей обработки	Прекращение обработки ПДн	30 дней (согласно п. 4 ст. 20 152-ФЗ)	Уведомление об уничтожении ПДн
		Уничтожение ПДн		
2. Запрос уполномоченного органа по защите прав субъектов персональных данных				
2.1	Информация для обеспечения деятельности	Предоставление затребованной информации по ПДн	30 дней (согласно п. 4 ст. 20 152-ФЗ)	Предоставление затребованной информации по ПДн

	уполномоченного органа			
2.2	Недостоверность ПДн субъекта	Блокировка ПДн	С момента обращения уполномоченного органа о недостоверности или с момента получения запроса на период проверки (согласно п. 1 ст. 21 152-ФЗ)	Уведомление о внесенных изменениях
		Изменение ПДн	7 рабочих дней со дня предоставления уточненных сведений (согласно п. 2 ст. 21 152-ФЗ)	
		Снятие блокировки ПДн		
		Отказ изменения ПДн	30 дней	Уведомление об отказе изменения ПДн
2.3	Неправомерность действий с ПДн субъекта	Прекращение неправомерной обработки ПДн	3 рабочих дня (согласно п. 3 ст. 21 152-ФЗ)	Уведомление об устранении нарушений
		Уничтожение ПДн в случае невозможности правомерной обработки	10 рабочих дней (согласно п. 3 ст. 21 152-ФЗ)	Уведомление об уничтожении ПДн
2.4	Достижение целей обработки ПДн субъекта	Блокировка ПДн	30 дней (согласно п. 4 ст. 21 152-ФЗ)	Уведомление об уничтожении ПДн
		Уничтожение ПДн		



Приложение № 10
к Положению о порядке обработки
и обеспечения безопасности персональных
данных субъектов персональных данных,
не являющихся работниками СПб ГАУ «ЦГЭ»

Примерная Форма
акта уничтожения носителей, содержащих персональные данные

Акт №___
уничтожения носителей, содержащих персональные данные
от ___.___.20___г.

Комиссия в составе: Должность	ФИО
Председатель:	
Члены комиссии:	

провела отбор носителей персональных данных и установила, что в соответствии с _____ *(указать документы, на основании которых принимается решение)* информация, записанная на них, подлежит уничтожению:

№ п/п	Дата	Тип носителя	Рег.№ носителя информации (бумажного, небумажного)	Примечание
1.	2.	3.	4.	5.

Всего подлежит уничтожению _____носителей
(цифрами и прописью)

Согласно нормативному правовому акту: «Методический документ. Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014) на указанных носителях персональные данные уничтожены путем:

_____.
(указать способ: стирание на устройстве гарантированного уничтожения информации и т.п.)

Согласно нормативному правовому акту: «Методический документ. Меры защиты информации в государственных информационных системах» (утв. ФСТЭК России 11.02.2014)

_____.
(указать способ: разрезание, сжигание, механическое уничтожение, сдача предприятию по утилизации вторичного сырья)

Уничтоженные носители с книг и журналов учета списаны.

Председатель комиссии: _____
(должность, ФИО, подпись)

Члены комиссии: _____
(должность, ФИО, подпись)

_____
(должность, ФИО, подпись)

Приложение № 11
к Положению о порядке обработки
и обеспечения безопасности персональных
данных субъектов персональных данных,
не являющихся работниками СПб ГАУ«ЦГЭ»

Регламент
осуществления внутреннего контроля соответствия обработки персональных данных в Санкт-Петербургском государственном автономном учреждении «Центр государственной экспертизы» установленным требованиям

1. Общие положения

1.1. Настоящий Регламент осуществления внутреннего контроля соответствия обработки персональных данных в Санкт-Петербургском государственном автономном учреждении «Центр государственной экспертизы» (далее - СПб ГАУ «ЦГЭ») установленным требованиям (далее - Регламент) разработан с учетом Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

1.2. Целью настоящего Регламента является обеспечение надлежащего контроля за обработкой персональных данных в СПб ГАУ «ЦГЭ» и соответствия порядка обработки персональных данных установленным требованиям.

2. Формы и методы осуществления внутреннего контроля

2.1. Внутренний контроль осуществляется в форме:

– плановых проверок;

– внеплановых проверок.

2.2. Плановые проверки проводятся ежегодно в структурных подразделениях, где осуществляется обработка персональных данных, и предполагают полную проверку соблюдения установленных требований.

2.3. Плановая проверка может проводиться в рамках ежегодного внутреннего аудита информационной безопасности так и в качестве отдельного мероприятия по контролю предусмотренного планом мероприятий по информационной безопасности.

2.4. Любая плановая проверка должна быть завершена не позднее, чем через месяц со дня её начала.

2.5. Внеплановые проверки проводятся на основании:

– поступившего письменного заявления субъекта персональных данных или его представителя о нарушениях прав субъекта

или о нарушении конфиденциальности персональных данных (предложение о проведении проверки должно исходить от работника, ответственного за организацию обработки персональных данных, на основании предварительно проведенного анализа);

– поступившей информации о нарушении или о подозрении на нарушение установленного порядка обработки персональных данных (предложение о проведении проверки должно исходить от администратора безопасности информации, на основании предварительно проведенного анализа).

2.6. При поступлении информации о нарушениях правил обработки персональных данных в течение трех рабочих дней принимается решение о проведении внеплановой проверки, которое оформляется приказом СПб ГАУ «ЦГЭ, либо решением об отсутствии такой необходимости (с соответствующим обоснованием).

3. Организация и порядок проведения внутреннего контроля

3.1. Организация проверок возлагается на работника, ответственного за организацию обработки персональных данных в СПб ГАУ «ЦГЭ».

3.2. Проверки осуществляются комиссией, формируемой по предложению ответственного за обработку персональных данных; состав комиссии, в которую в обязательном порядке включается администратор безопасности информации, утверждается приказом СПб ГАУ «ЦГЭ»; председателем комиссии является должностное лицо в должности не ниже заместителя директора СПб ГАУ «ЦГЭ».

3.3. При осуществлении проверок должны быть полностью, объективно и всесторонне исследованы процедуры обработки персональных данных.

Для этого проводится проверка:

– соответствия целей обработки персональных данных целям, определенным и заявленным при сборе персональных данных;

– соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

– достаточность (избыточность) персональных данных для целей обработки персональных данных, заявленных при сборе персональных данных.

3.4. При проведении проверок порядка обработки персональных данных с использованием средств автоматизации осуществляется контроль:

– соответствия правил доступа полномочиям пользователя;

– соблюдения порядка доступа в помещения СПб ГАУ «ЦГЭ», где расположены элементы информационных систем персональных данных;

– соблюдения пользователями информационных систем персональных данных требований парольной защиты;

– соблюдения пользователями информационных систем персональных данных правил антивирусной защиты;

– соблюдения пользователями информационных систем персональных данных правил работы со съемными носителями информации;

– соблюдение порядка резервирования баз данных и хранения резервных копий;

– соблюдения правил удаления данных с носителей информации и их утилизации;

– соблюдения порядка работы со средствами защиты информации;

– знания пользователей информационных систем персональных данных о своих действиях во внештатных ситуациях.

3.5. При проведении проверок порядка обработки персональных данных без использования средств автоматизации осуществляется контроль:

– соответствия правил доступа к носителям персональных данных полномочиям пользователя;

– организации хранения бумажных носителей с персональными данными;

– порядка проведения работ с персональными данными, обрабатываемыми без использования средств автоматизации;

– соблюдения правил утилизации бумажных носителей информации;

– доступа в помещения, где обрабатываются и хранятся бумажные носители персональных данных.

3.6. При проведении внеплановой проверки:

– должны быть тщательным образом проверены все факты, изложенные в обращении, и подготовлены корректные ответы на вопросы заявителя.

3.7. При проведении проверки комиссия имеет право:

– запрашивать у работников информацию, необходимую для реализации полномочий;

– принимать меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации, локальных правовых актов СПб ГАУ «ЦГЭ»;

– вносить предложения о совершенствовании правового, технического и организационного регулирования обработки, обеспечения безопасности персональных данных.

3.8. В случае проведения внеплановой проверки по ее результатам должны быть подготовлены рекомендации, направленные на исключение повторения событий, по факту которых проводилась проверка, общее снижение вероятности появления инцидентов информационной безопасности, минимизацию негативных последствий от возможных инцидентов информационной безопасности.

4. Оформление результатов проведения проверок

4.1. Если при проведении проверки были выявлены факты:

– несоблюдения установленного порядка обработки персональных данных;

– несоблюдения условий хранения носителей персональных данных;

– нарушения порядка учета и использования носителей информации, содержащих персональные данные;

– использования программного обеспечения, которое может привести к нарушению заданного уровня безопасности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных.

– в обязательном порядке устанавливаются причины нарушения порядка обработки персональных данных, определяется наличие (отсутствие) вины работника, осуществляющего обработку персональных данных, и разрабатываются меры и рекомендации, направленные на минимизацию негативных последствий выявленных нарушений и предотвращение подобных нарушений в будущем. Устранение выявленных нарушений проводится не позднее 30 дней с момента завершения проверки.

4.2. По результатам проверки составляется Заключение о проведении внутренней проверки. Примерная форма Заключения приведена в приложении к настоящему Регламенту. При выявлении в ходе проверки нарушений в Заключении указываются рекомендуемые мероприятия по устранению нарушений и сроки их реализации.

4.3. О результатах проверки и предложениях председатель комиссии докладывает директору СПб ГАУ «ЦГЭ».

4.4. Ответственные за организацию обработки персональных данных и администратор безопасности информации осуществляет (в пределах своей компетенции) контроль своевременности и полноты устранения нарушений, выявленных в ходе проведения проверок.

4.5. Заключения о проведении проверки хранятся у ответственного за организацию обработки персональных данных в СПб ГАУ «ЦГЭ».

4.6. Уничтожение Заключений о проведении проверки производится ответственным за организацию обработки персональных данных самостоятельно по истечению установленного срока хранения таких документов, но не ранее полутора лет со дня окончания проведения соответствующей проверки и (или) до полного устранения выявленных нарушений.

Приложение
к Регламенту осуществления
внутреннего контроля соответствия
обработки персональных данных
в СПб ГАУ «ЦГЭ» установленным
требованиям

Примерная форма
заключения о проведении внутреннего контроля соответствия обработки персональных данных в Санкт-Петербургском государственном автономном учреждении «Центр государственной экспертизы» установленным требованиям

Заключение
о проведении внутреннего контроля соответствия обработки персональных данных в Санкт-Петербургском государственном автономном учреждении «Центр государственной экспертизы» установленным требованиям

Настоящее Заключение составлено в том, что в период с _____ по _____ комиссией
в составе:

1) (должность, Ф.И.О. работника);
2) (должность, Ф.И.О. работника);

проведен плановый (внеплановый) контроль соответствия обработки персональных данных СПб ГАУ «ЦГЭ» требованиям, установленным:

Федеральным законом от 27.07.2006 г. № 152-ФЗ «О персональных данных»;

постановлением Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным Законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

указать иные документы, на соответствие которым проводилась проверка.

Проверка осуществлялась в соответствии: _____
(основание проверки)

В ходе проверки
проверено:_____
В ходе проверки выявлены следующие
нарушения:_____
Виновные в выявленных нарушениях
Должность _____ ФИО
Должность _____ ФИО
Меры по устранению
нарушений:_____

Срок устранения нарушений: _____.
Председатель комиссии _____ ФИО
Члены комиссии:
Должность _____ ФИО
Должность _____ ФИО
С результатами проверки и выводами и замечаниями комиссии ознакомлены:
Должность руководителя проверяемого структурного подразделения _____ ФИО
Должность проверяемого работника _____ ФИО

Приложение № 12
к Положению о порядке обработки
и обеспечения безопасности персональных
данных субъектов персональных данных,
не являющихся работниками СПб ГАУ «ЦГЭ»

Обязательство о неразглашении информации конфиденциального характера

Я, _____,
заключая трудовой договор с Санкт-Петербургским государственным автономным учреждением «Центр государственной экспертизы» (далее – СПб ГАУ «ЦГЭ»), в период гражданско-правовых отношений с СПб ГАУ «ЦГЭ» (его правопреемником), а также в течение 2 лет после их окончания обязуюсь:

1. Не разглашать, не передавать третьим лицам сведения конфиденциального характера[1] СПб ГАУ «ЦГЭ», персональные данные работников СПб ГАУ «ЦГЭ», информацию об информационно-телекоммуникационной инфраструктуре СПб ГАУ «ЦГЭ» и планах по ее развитию, методах и средствах защиты информации, бизнес-процессах СПб ГАУ «ЦГЭ», которые мне будут доверены или станут известны, а также пресекать действия других лиц, которые могут привести к их разглашению.

2. Выполнять доводимые до моего сведения требования приказов, инструкций и иных организационно-распорядительных документов по обеспечению конфиденциальности и сохранности обрабатываемой информации и порядку работы со средствами ее обработки.

3. В случае попытки посторонних лиц получить от меня сведения конфиденциального характера немедленно сообщить своему непосредственному руководителю и в Управление информационных технологий.

4. Не использовать знание сведений конфиденциального характера для занятий любой противоправной деятельностью.

5. Выполнять только те работы и знакомиться только с теми документами,
к которым мне предоставлен доступ установленным в СПб ГАУ «ЦГЭ» порядке.

6. В случае если в моем распоряжении ошибочно окажутся материалы конфиденциального характера (по электронной почте, на съемных носителях информации или иным способом) незамедлительно сообщить непосредственному руководителю и в Управление информационных технологий.

[1] Сведения ограниченного доступа – сведения, доступ к которым ограничивается в соответствии с законодательством Российской Федерации. Отнесение сведений к сведениям ограниченного доступа осуществляется в соответствии с Перечнем сведений конфиденциального характера СПб ГАУ «ЦГЭ».

7. Строго соблюдать правила работы, в том числе учета и хранения, с документами конфиденциального характера, определенными соответствующими организационно-распорядительными документами СПб ГАУ «ЦГЭ».

8. В случае прекращения трудовых отношений с СПб ГАУ «ЦГЭ» все служебные материальные носители СПб ГАУ «ЦГЭ», которые находились в моем распоряжении, передать ответственным работникам СПб ГАУ «ЦГЭ».

9. Об утрате или недостаче материальных носителей, содержащих сведения конфиденциального характера, ключей от защищаемых помещений, хранилищ, сейфов (металлических шкафов) и о других фактах, которые могут привести к разглашению сведений конфиденциального характера, а также о причинах и условиях утечки таких сведений немедленно сообщать в Управление информационных технологий.

До моего сведения доведены с разъяснениями соответствующие положения по обеспечению конфиденциальности и сохранности сведений конфиденциального характера СПб ГАУ «ЦГЭ».

Мне известно, что нарушение этих положений может повлечь уголовную, административную или гражданско-правовую ответственность в соответствии с законодательством Российской Федерации в виде расторжения трудового договора, денежного штрафа, лишения свободы и других наказаний.

Мне известно и понятно, что я несу персональную ответственность за соблюдение установленного в СПб ГАУ «ЦГЭ» режима защиты информации конфиденциального характера.

_____ /_____/

подпись расшифровка подписи

«___» _____ 202_ г.