Приложение №1
к Приказу от 20.10.17.г. № 255

ПОЛИТИКА
обработки персональных данных в Государственном бюджетном учреждении Псковской области «Многофункциональный центр предоставления государственных и муниципальных услуг Псковской области»

I. Общие положения

1.1 Политика Государственного бюджетного учреждения Псковской области «Многофункциональный центр предоставления государственных и муниципальных услуг Псковской области» (далее – Учреждение) в отношении организации обработки и обеспечения безопасности персональных данных (далее – Политика) разработана в целях реализации требований законодательства Российской Федерации в области обработки и обеспечения безопасности персональных данных.

1.2 Политика разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг», Трудовым кодексом Российской Федерации от 30 декабря 2001 г. № 197-ФЗ и иными нормативными правовыми актами Российской Федерации в области обработки и защиты персональных данных.

1.3 Целью политики является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

1.4 Политика раскрывает способы и принципы обработки персональных данных в Учреждении, права и обязанности Учреждения при обработке персональных данных, права субъектов персональных данных, и включает перечень мер, применяемых Учреждением в целях обеспечения безопасности персональных данных при их обработке.

1.5 Политика является общедоступным документом, декларирующим концептуальные основы деятельности Учреждения при обработке и обеспечении безопасности персональных данных.

1.6 Учреждением направляется уведомление об обработке персональных данных в уполномоченный орган по защите прав субъектов персональных данных.

1.7 Учреждением добросовестно и в соответствующий срок осуществляется актуализация сведений, указанных в уведомлении.

II. Категории субъектов и состав персональных данных

2.1 В Учреждении осуществляется обработка персональных данных следующих категорий субъектов персональных данных:

2.1.1 работники Учреждения;

2.1.2 кандидаты на замещение вакантных должностей Учреждения;

2.1.3 заявители – физические лица и уполномоченные представители физических или юридических лиц, обратившиеся в Учреждение с запросом о предоставлении государственных или муниципальных услуг, а также физические лица, обработка персональных данных которых необходима для

предоставления государственных или муниципальных услуг заявителям или их уполномоченным представителям.

2.2 Персональные данные, обрабатываемые в информационных системах Учреждения, содержатся в следующих документах:

2.2.1 документах отдела бухгалтерского учета и кадров;

2.2.2 документах отдела приема заявителей;

2.2.3 документах центра телефонного обслуживания;

2.3 В отделе бухгалтерского учета и кадров создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

2.3.1 документы, содержащие персональные данные работников Учреждения (комплекты документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплект материалов по анкетированию, тестированию, проведению собеседований с кандидатами на должность; подлинники и копии приказов по личному составу; личные дела и трудовые книжки работников; дела, содержащие основания к приказу по личному составу; дела, содержащие материалы аттестации работников; подлинники и копии отчетных, аналитических и справочных материалов; копии отчетов, направляемых в государственные органы статистики, налоговые и другие органы).

2.3.2 документация по организации работы структурных подразделений (должностные инструкции работников, приказы, распоряжения, поручения руководства Учреждения); документы по планированию, учету, анализу и отчетности в части работы с персоналом Учреждения.

2.3.3 документы, содержащие данные о работниках в единичном или сводном виде: карточка-справка, копия паспорта, копия страхового пенсионного свидетельства, копия ИНН, копия личного счета для зачисления заработной платы, копии приказов с расчетами, отчеты в органы статистики, отчеты в налоговые органы и другие организации.

2.4 В документах отдела приема заявителей, центра телефонного обслуживания создаются и хранятся копии следующих документов - паспорта, страховые пенсионные свидетельства, ИНН, иные документы, необходимые для предоставления государственных и муниципальных услуг.

III. Правовые основания обработки персональных данных

3.1 Политика разработана в соответствии с действующим законодательством Российской Федерации в области обработки и защиты персональных данных.

3.2 Во исполнение Политики, в целях организации обработки персональных данных в ГБУ ПО «МФЦ» введены в действие следующие документы:

3.2.1 приказ об утверждении мест хранения материальных носителей персональных данных;

3.2.2 приказ о создании комиссии по уничтожению персональных данных;

3.2.3 приказ о создании комиссии для проведения проверок соответствия обработки персональных данных Политике обработки персональных данных в Учреждении;

3.2.4 типовая форма заявления работника Учреждения о согласии на перевод части персональных данных в общедоступные источники персональных данных;

3.2.5 типовая форма обязательства работника Учреждения о неразглашении персональных данных заявителей;

3.2.6 типовая форма согласия законного представителя на обработку персональных данных;

3.2.7 типовая форма заявления работника Учреждения о согласии на обработку персональных данных;
3.2.8 типовая форма отзыва согласия на обработку персональных данных;
3.2.9 перечень обрабатываемых в Учреждении персональных данных работников;
3.2.10 перечень обрабатываемых в Учреждении персональных данных заявителей;
3.2.11 перечень должностей по которым предусмотрена работа с персональными данными;
3.2.12 журнал учета обращений граждан-субъектов персональных данных о выполнении их законных прав в области защиты персональных данных, обрабатываемых в Учреждении;
3.2.13 журнал учета мероприятий по контролю обеспечения защиты персональных данных, обрабатываемых в Учреждении;
3.2.14 журнал учета инцидентов информационной безопасности;
3.2.15 журнал проведения инструктажей по информационной безопасности в Учреждении;
3.2.16 журнал уничтожения носителей персональных данных;
3.2.17 журнал ознакомления работников Учреждения с Политикой обработки персональных данных в Учреждении;
3.2.18 инструктаж о мерах по обеспечению безопасности персональных данных;
3.2.19 правила рассмотрения запросов субъектов персональных данных и их представителей;
3.2.20 правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;
3.2.21 расписка об ознакомлении работников Учреждения с федеральными и локальными нормативными актами в области защиты персональных данных;
3.2.22 частные модели угроз безопасности персональных данных;
3.2.23 акты определения уровней защищенности информационных систем персональных данных.

IV. Принципы и цели обработки персональных данных

4.1 Учреждение в своей деятельности обеспечивает соблюдение принципов обработки персональных данных, указанных в статье 5 Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4.2 Учреждение осуществляет сбор и дальнейшую обработку персональных данных в следующих целях:

4.2.1 выполнение требований трудового законодательства, обязанностей по выплате работникам заработной платы, компенсаций и премий, осуществлению пенсионных и налоговых отчислений;
4.2.2 обучение и повышение квалификации работников;
4.2.3 сохранение жизни и здоровья работников в процессе трудовой деятельности, в целях выявления нарушений требований в сфере охраны здоровья работников и наличия медицинских противопоказаний к работе, а также в целях выполнения требований действующего законодательства по расследованию и учету несчастных случаев, происшедших с работниками и иными лицами;
4.2.4 обеспечение личной безопасности работников, иных лиц, посещающих объекты недвижимости (помещения, здания, территория) Учреждения, обеспечения сохранности материальных и иных ценностей, находящихся в ведении Учреждения;
4.2.5 предоставление государственных и муниципальных услуг;
4.2.6 создание кадрового резерва;

4.2.7 поиск и отбор кандидатов на замещение вакантных должностей Учреждения;
4.2.8 другие цели, предусмотренные действующим законодательством Российской Федерации.

V. Порядок сбора и обработки персональных данных

5.1 Порядок получения персональных данных о работниках Учреждения.

5.1.1 Все персональные данные работника Учреждения следует получать у него самого. Если персональные данные работника возможно получить только у третьей стороны, то работник должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Должностное лицо Учреждения должно сообщить работнику Учреждения о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

5.1.2 Должностные лица Учреждения не имеют права получать и обрабатывать персональные данные работника Учреждения о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, частной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии со ст. 24 Конституции Российской Федерации должностные лица Учреждения вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

5.1.3 Обработка персональных данных работников возможна только с их согласия либо без их согласия в следующих случаях:

5.1.3.1 персональные данные являются общедоступными;

5.1.3.2 персональные данные относятся к состоянию здоровья работника и их обработка необходима для защиты его жизни, здоровья или иных жизненно важных интересов либо жизни, здоровья или иных жизненно важных интересов других лиц и получение согласия работника невозможно;

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

5.1.4 Письменное согласие работника на обработку своих персональных данных должно включать в себя:

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

5.1.4.2 наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;

5.1.4.3 цель обработки персональных данных;

5.1.4.4 перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

5.1.4.5 перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных; срок, в течение которого действует согласие, а также порядок его отзыва.

5.1.5 Форма заявления о согласии работника на обработку персональных данных - приложение №4 к настоящей Политике.

5.1.6 Согласие работника на обработку его персональных данных не требуется в случаях, определенных федеральным законодательством.

5.2 Порядок обработки, передачи и хранения персональных данных работников.

5.2.1 В соответствии со ст. 86 ТК РФ в целях обеспечения прав и свобод человека и гражданина сотрудники Учреждения при обработке персональных данных работника должны соблюдать следующие общие требования:

5.2.2.1 Обработка персональных данных может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

5.2.2.2 При определении объема и содержания, обрабатываемых персональных данных должностные лица Учреждения должны руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

5.2.2.3 При принятии решений, затрагивающих интересы работника, должностные лица Учреждения не имеют права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

5.2.2.4 Защита персональных данных работника от неправомерного их использования или утраты обеспечивается должностными лицами Учреждения за счет средств Учреждения в порядке, установленном нормативными правовыми документами.

5.2.2.5 Работники должны быть ознакомлены с документами Учреждения, устанавливающими порядок обработки персональных данных работников, а также об их правах и обязанностях в этой области.

5.2.2.6 Во всех случаях отказ работника от своих прав на сохранение и защиту персональных данных недействителен.

5.3 Порядок обработки, передачи и хранения персональных данных заявителей.

5.3.1 Объем и содержание обрабатываемых персональных данных заявителей определяется действующим законодательством, административными регламентами, устанавливающими порядок предоставления государственной или муниципальной услуги.

5.3.2 Право на доступ к персональным данным заявителей предоставляется работникам Учреждения, в должностные обязанности которых входят обработка, передача и хранение персональных данных заявителей в целях предоставления им государственных и муниципальных услуг.

5.3.3 Обработка персональных данных заявителей может осуществляться исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, предоставления государственной или муниципальной услуги, обеспечения их личной безопасности, контроля количества и качества предоставления услуг.

5.3.4 Обработка персональных данных при предоставлении услуг осуществляется работником учреждения в автоматизированной системе управления деятельностью МФЦ с использованием системы межведомственного электронного взаимодействия.

5.3.5 Работники Учреждения не имеют права использовать в иных целях персональные данные заявителя, полученные исключительно для предоставления государственной или муниципальной услуги.

5.3.6 Защита персональных данных заявителя от неправомерного их использования или утраты обеспечивается в порядке, установленном законодательством, нормативными правовыми документами.

VI. Обеспечение защиты персональных данных

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

6.2 Безопасность персональных данных при их обработке обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-математических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии. Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

6.3 Для обеспечения безопасности персональных данных осуществляется защита информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

6.4 При обработке персональных данных должно быть обеспечено:

6.4.1 проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

6.4.2 своевременное обнаружение фактов несанкционированного доступа к персональным данным;

6.4.3 недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

6.4.4 возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

6.4.5 постоянный контроль за обеспечением уровня защищённости персональных данных.

6.5 Мероприятия по обеспечению безопасности персональных данных включают в себя:

6.5.1 определение информационных систем, содержащих персональные данные;

6.5.2 определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

6.5.3 разработку на основе частной модели угроз безопасности персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных;

6.5.4 проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

6.5.5 установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

6.5.6 обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

6.5.7 учёт применяемых средств защиты информации эксплуатационной и технической документации к ним, носителей персональных данных;

6.5.8 учёт лиц, допущенных к работе с персональными данными в информационной системе;

6.5.9 контроль за соблюдением условий использования средств защиты информации,

предусмотренных эксплуатационной и технической документацией;

6.5.10 составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут провести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищённости персональных данных, разработку и принятие мер по предотвращению возможных опасных нарушений.

VII. Передача персональных данных

7.1 Передача персональных данных работников Учреждения.

7.1.1 Работодатель не вправе предоставлять персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в случаях, установленных федеральным законодательством.

7.1.2 В случае если лицо, обратившееся с запросом, не уполномочено федеральным законом на получение персональных данных работника или отсутствует письменное согласие работника на предоставление его персональных данных, работодатель обязан отказать в предоставлении персональных данных. Лицу, обратившемуся с запросом, выдается письменное уведомление об отказе в предоставлении персональных данных.

7.1.3 Персональные данные работника могут быть переданы представителем работника в том объёме, в каком это необходимо для выполнения указанными представителями их функций.

7.1.4 Отдел бухгалтерского учёта и кадров Учреждения обрабатывает и предоставляет персональные данные в Отделение Пенсионного Фонда Российской Федерации по Псковской области и Управление Федеральной налоговой службы Российской Федерации по Псковской области.

7.2 При передаче персональных данных работника внутри структурного подразделения или в другое структурное подразделение Учреждения, информация ограничивается только теми персональными данными работника, которые необходимы для выполнения должностными лицами их функции.

7.3 Передача персональных данных заявителей.

7.3.1 Передача персональных данных заявителей ограничивается исключительно заключенными Учреждением соглашениями с органами власти и административными регламентами, устанавливающими порядок предоставления государственной или муниципальной услуги.

7.4 Порядок приостановки предоставления персональных данных в случае обнаружения нарушений порядка их предоставления.

7.4.1 При обнаружении нарушений порядка предоставления персональных данных работник Учреждения должен немедленно приостановить предоставление персональных данных.

7.4.2 Руководитель Учреждения назначает служебное расследование для выявления причин нарушения.

7.4.3 После устранения нарушений предоставление персональных данных возобновляется.

VIII. Хранение персональных данных

8.1 Персональные данные работников Учреждения обрабатываются и хранятся в

отделе бухгалтерского учета и кадров, как на бумажных носителях, так и в электронном виде в локальных информационных системах.

8.2 Персональные данные заявителей, полученные в результате их автоматизированной обработки или электронного получения для предоставления государственной или муниципальной услуги, обрабатываются и хранятся в электронном виде в локальных информационных системах.

IX. Доступ к персональным данным

9.1 Перечень должностей, замещение которых предусматривает работу с персональными данными и информационными системами персональных данных – приложение №8 к настоящей Политике.

9.2 Изменения и дополнения в перечень должностей вносятся на основании приказа директора Учреждения.

X. Порядок действий должностных лиц в случае обнаружения нарушений, угрожающих конфиденциальности обрабатываемых персональных данных

10.1 В случае обнаружения фактов несоблюдения условий хранения носителей персональных данных, неисправности средств защиты информации, нарушения порядка предоставления персональных данных или иных нарушений, угрожающих конфиденциальности обрабатываемых персональных данных (далее - инцидент информационной безопасности), обнаружившие инцидент работники Учреждения обязаны немедленно информировать о нем ответственного за организацию обработки персональных данных в Учреждении.

10.2 Предположение о том, что произошел инцидент информационной безопасности, может основываться на следующих признаках:

10.2.1 уведомление антивирусного средства о нарушении информационной безопасности;

10.2.2 сообщение пользователей об отклонениях в работе системных или прикладных программ;

10.2.3 сообщение пользователей о снижении производительности их рабочих станций;

10.2.4 наличие файлов с нечитаемыми названиями;

10.2.5 множественные неудачные попытки авторизации.

10.3 Ответственным за организацию обработки персональных данных проводится оценка риска и последствий инцидента, вследствие чего вырабатывается стратегия реагирования на инцидент.

10.4 В случае возможности нарушения конфиденциальности обрабатываемых персональных данных, дальнейшая работа информационных систем прекращается.

10.5 В случае возникновения нарушений на рабочей станции или сервере необходимо произвести полное дублирование информации и проводить работы по расследованию нарушения на отдельном компьютере.

10.6 Электронные журналы должны быть тщательно изучены и проанализированы.

10.7 События инцидента подлежат документированию. Документирование необходимо для сбора и последующего обобщения свидетельств расследования. Документированию подлежат все факты и доказательства злонамеренного воздействия.

10.8 Фиксация событий инцидента ведется в журнале учета инцидентов информационной безопасности (Приложение №11 настоящей Политики).

10.9 В ходе расследования инцидента все свидетельства должны быть защищены от

дискредитации, поскольку данные могут содержать информацию о действенных уязвимостях информационной системы.

10.10 Ответственным за организацию обработки персональных данных составляется заключение по факту инцидента информационной безопасности, включающее в себя:

10.10.1 исходное протоколирование инцидента;

10.10.2 причины и следствия возникновения инцидента;

10.10.3 меры, предпринятые для ликвидации инцидента и его последствий;

10.10.4 предложения по внесению изменений в систему обеспечения безопасности информации.

10.11 Ответственным за организацию обработки персональных данных должен быть классифицирован и описан каждый инцидент, произошедший в Учреждения, а также классифицированы и описаны возможные инциденты, предположения о которых были сделаны на основе анализа рисков.

XI. Обязанности должностных лиц по обеспечению безопасности персональных данных

11.1 Ответственный за организацию обработки персональных данных в Учреждения назначается приказом директора Учреждения.

11.2 Безопасность персональных данных при их обработке обеспечивают должностные лица Учреждения, обеспечивающие эксплуатацию информационной системы.

11.3 Работники Учреждения, допущенные к обработке персональных данных обязаны:

11.3.1 Строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами информационных систем;

11.3.2 Хранить в тайне свой пароль (пароли);

11.3.3 Выполнять требования части XIV «Правила антивирусной защиты» настоящей Политики в части касающейся действий пользователей рабочих станций информационных систем;

11.3.4 Немедленно ставить в известность ответственного за организацию обработки персональных данных в Учреждении при обнаружении следующих нарушений:

11.3.4.1 нарушений целостности пломб (наклеек, печатей) на аппаратных средствах рабочих станций или иных фактов совершения в его отсутствие попыток несанкционированного доступа к защищённой рабочей станции;

11.3.4.2 несанкционированных изменений в конфигурации программных или аппаратных средств рабочей станции;

11.3.4.3 нарушений в работе средств защиты информации;

11.3.4.4 отклонений в работе системных или прикладных программных программ, затрудняющих эксплуатацию рабочей станции, выхода их строя или неустойчивого функционирования узлов рабочей станции или периферийных устройств (дисководов, принтера и т.п.), а также перебоях в системе электроснабжения;

11.3.4.5 некорректного функционирования установленных на рабочей станции технических средств защиты;

11.3.4.6 непредусмотренных отводов кабелей и подключенных устройств.

XII. Правила учета средств защиты информации и носителей персональных данных

12.1 Средства защиты информации, используемые в информационных системах Учреждения, содержащих персональные данные, подлежат учёту.

12.2 Ответственным за организацию обработки персональных данных должна организовываться периодическая проверка защиты информации и носителей персональных данных.

12.3 Результаты контроля заносятся ответственным за организацию обработки персональных данных в журнал учета мероприятий по контролю обеспечение защиты персональных данных (Приложение №10 настоящей Политики), с указанием мероприятия, даты проведения проверки и результатов контроля.

XIII. Правила парольной защиты

13.1 Контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на ответственного за организацию обработки персональных данных.

13.2 Пароли должны генерироваться и распределяться централизованно с учетом следующих требований:

13.2.1 Длина пароля должна быть не менее 8 символов;

13.2.2 В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы;

13.2.3 Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, номера телефонов, даты рождения и другие сочетания);

13.2.4 При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;

13.2.5 Личный пароль пользователь не имеет права сообщать никому.

13.3 Работники Учреждения, имеющие доступ к персональным данным, должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

13.4 Ответственность за правильность формирования и распределения паролей возлагается на ответственного за организацию обработки персональных данных.

13.5 Для генерации «стойких» значений паролей могут применяться специальные программные средства.

13.6 Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 2 месяца.

13.7 Внеплановая смена личного пароля или удаление учетной записи пользователя информационной системы в случае прекращения его полномочий (увольнение, переход на другую работу внутри организации и другие изменения) должна проводиться ответственным за организацию обработки персональных данных немедленно после окончания последнего сеанса работы данного пользователя с системой.

13.8 Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу и другие изменения) работников, которым были предоставлены полномочия по управлению парольной защитой.

13.9 В случае компрометации личного пароля пользователя информационной системы должны быть немедленно предприняты меры по внеплановой смене паролей.

13.10 Хранение работником значений своих паролей на бумажном носителе допускается только в сейфе ответственного за организацию обработки персональных данных.

XIV. Правила антивирусной защиты

14.1 В Учреждения допускаются к использованию только лицензионные антивирусные средства.

14.2 Установка и настройка параметров средств антивирусного контроля на компьютерах осуществляется работниками, ответственными за установку программного обеспечения, в соответствии с руководствами по применению конкретных антивирусных средств.

14.3 Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, файлы данных, текстовые файлы любых форматов), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях. Разархивирование и контроль входящей информации необходимо проводить непосредственно после её приема. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

14.4 Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера, должна быть выполнена антивирусная проверка.

14.5 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник Учреждения самостоятельно или вместе с ответственным за организацию обработки персональных данных должен провести внеочередной антивирусный контроль компьютера. При необходимости привлечь специалистов для определения ими факта наличия или отсутствия компьютерного вируса.

14.6 В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов работники обязаны:

14.8.1 Приостановить работу.

14.8.2 Немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за организацию обработки персональных данных, владельца заражённых файлов, смежные подразделения, использующие эти файлы в работе.

14.7 Ежедневно в автоматическом режиме должно проводиться обновление антивирусных баз.

14.8 Работниками ответственными за обеспечение информационной безопасности должны проводиться периодические проверки обновлений компонент антивирусного средства не реже одного раза в месяц.

XV. Правила обновления общесистемного и прикладного программного обеспечения

15.1 Под обновлением понимается замена программного обеспечения (далее — ПО) устаревшей версии на новую версию этого же ПО. Обновление ПО допустимо лишь в той мере и в том случае, если это подтверждено производственной необходимостью и имеет непосредственное отношение к технологическому процессу обработки информации.

15.2 В процессе обновления ПО допускается ввод информации с CD-дисков и внешних магнитных носителей.

15.3 Установка и обновление ПО производится только с лицензионных носителей.

15.4 Обновления должны подвергаться антивирусному контролю в соответствии с

разделом XIV «Правила антивирусной защиты» настоящей Политики.

15.5 Установка нового автоматизированного рабочего места для пользователя информационной системы производится после выполнения требований к системе защиты персональных данных и настоящей Политики. По окончании работ производится оценка соответствия информационной системы требованиям безопасности персональных данных и вносятся необходимые изменения и дополнения в техническую документацию.

XVI. Порядок контроля за соблюдением условий использования средств защиты информации

16.1 Целями контроля за соблюдением условий использования средств защиты информации являются:

16.1.1 Установление степени соответствия принятых мер требованиям законодательных и иных нормативных правовых актов, стандартов, норм, правил и инструкций по защите информации.

16.1.2 Выявление технических каналов утечки информации, несанкционированного доступа к информации и специальных воздействий на информацию, содержащую сведения о персональных данных и выработка рекомендаций по закрытию этих каналов.

16.2 Контроль за соблюдением условий использования средств защиты информации (далее - Контроль) осуществляется ответственным за организацию обработки персональных данных посредством проведения проверок.

16.3 При Контроле необходимо проверять срок действия сертификатов используемых средств защиты информации.

16.4 Контроль должен проводиться регулярно. Результаты Контроля докладываются директору Учреждения.

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

17.1 Работники Учреждения, виновные в нарушении норм настоящей Политики, а также законодательства Российской Федерации, регулирующего получение, обработку и защиту персональных данных работника, несут дисциплинарную административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.