Согласовано
Управляющим советом
протокол от 27.08.2015 г. № 10

Утверждено
приказом директора
от 31.08.2015 г. № 75-а

Утверждено
(изменения и дополнения)
приказом директора
от 15.06.2021 г. № 69-од

ПОЛОЖЕНИЕ
ОБ ОБРАБОТКЕ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ МАОУ «ШКОЛА-КОМПЛЕКС №33»
(с изменениями и дополнениями от 15.06.2021)

1. Общие положения

1.1. Настоящее положение об обработке персональных данных (далее – Положение) работников МАОУ «Школа-комплекс №33» (далее по тексту – Учреждение) разработано в соответствии с:

– Конституцией Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020)

– Трудовым кодексом Российской Федерации (ТК РФ) от 30.12.2001 №197-ФЗ (с изменениями и дополнениями)

– Гражданским кодексом Российской Федерации (ГК РФ) часть 1 от 30.11.1994 № 51-ФЗ (с изменениями и дополнениями), часть 2 от 26.01.1996 № 14-ФЗ (с изменениями и дополнениями), часть 3 от 26.11.2001 №146-ФЗ (с изменениями и дополнениями), часть 4 от 18.12.2006 №230-ФЗ (с изменениями и дополнениями)

– Федеральным законом от 27.07.2006 №143-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями),

– Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями и дополнениями),

– Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

– Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

– Постановлением Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

– Приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 05.09.2013 N 996 «Об утверждении требований и методов по обезличиванию персональных данных»

– Письмо Федерального агентства по образованию от 29.07.2009 г. № 17-110 «Об обеспечении защиты персональных данных»,

– Уставом и локальными актами Учреждения.

1.2. Цель разработки Положения – определение порядка обработки персональных данных; обеспечение защиты прав и свобод работников Учреждения при обработке их персональных данных, а также установление ответственности должностных лиц, имеющих доступ к персональным данным работников Учреждения, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.3. Порядок ввода в действие и изменения Положения.

1.3.1. Настоящее Положение вступает в силу с 31.08.2015г. и действует бессрочно до замены его новым Положением.

1.3.2. Все изменения в Положение вносятся приказом директора Учреждения.

1.4. Все работники Учреждения должны быть ознакомлены с настоящим Положением под роспись.

1.5. Режим конфиденциальности персональных данных снимается в случаях их обезличивания и по истечении срока их хранения, или продлевается на основании заключения экспертной комиссии Учреждения, если иное не определено законом.

2. Основные понятия, используемые в Положении

2.1. Для целей настоящего Положения используются следующие основные понятия:

– персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту 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);

– 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;

– информационная система персональных данных – совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

2.2. Меры по обеспечению безопасности персональных данных при их обработке.

2.2.1 Оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

2.2.2. Обеспечение безопасности персональных данных достигается, в частности:

– определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

– применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных,

– применением прошедших в установленном порядке процедуру оценки

соответствия средств защиты информации

– обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них

– установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных,

– контролем за принимаемыми мерами по обеспечению безопасности персональных данных и др.

3. Состав персональных данных работников

3.1. К персональным данным работников, получаемым работодателем и подлежащим хранению у работодателя в порядке, предусмотренном законодательством Российской Федерации и настоящим Положением, относятся следующие документы, содержащиеся в личных делах работников, согласно перечню данных, обрабатываемых в Учреждении (приложение №1):

– копия паспорта (паспортные данные работника);

– копия страхового свидетельства государственного пенсионного страхования;

– копия документа воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

– копия документа об образовании, квалификации или наличии специальных знаний (при поступлении на работу, требующую специальных знаний или специальной подготовки);

– наличие/отсутствие судимости;

– анкетные данные, заполненные работником при поступлении на работу или в процессе работы (в т.ч. автобиография, сведения о семейном положении работника, перемене фамилии, наличии детей и иждивенцев);

– документы, которые с учетом специфики работы и в соответствии с законодательством РФ должны быть предъявлены работником при заключении трудового договора или в период его действия;

– трудовой договор (соглашения о внесении изменений и дополнений в него);

– результаты обязательных медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования;

– копии приказов о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;

– личная карточка по форме Т-2, личный листок по учету кадров;

– заявления, объяснительные и служебные записки работника;

– документы о прохождении работником аттестации, собеседования, повышения квалификации (аттестационный лист);

– документы, содержащие сведения о работнике, нахождение которых в личном деле работника необходимо для документального оформления трудовых правоотношений с работником;

– свидетельство о присвоении ИНН (при его наличии у работника).

3.2. Документы, содержащие персональные данные работников, создаются путем:

– копирования оригиналов;

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

– получения оригиналов необходимых документов.

3.3. При оформлении работника заведующим канцелярией заполняются унифицированные формы: Т-2 «Личная карточка работника» и личный листок по учету кадров, в которой отражаются следующие анкетные и биографические данные работника:

– общие сведения (ФИО работника, дата рождения, место рождения, гражданство);

– образование, профессия;

– выполняемая работа с начало трудовой деятельности;

– стаж работы;

– состояние в браке, состав семьи;
– паспортные данные;
– сведения о воинском учете;
– данные о приеме на работу;
– сведения о месте жительства и контактных телефонах.

В дальнейшем в личную карточку вносятся:

– сведения о переводах на другую работу;
– сведения об аттестации;
– сведения о повышении квалификации;
– сведения о профессиональной переподготовке;
– сведения о наградах (поощрениях), почетных званиях;
– сведения об отпусках;
– сведения о социальных гарантиях.

3.4. В Учреждении создаются и хранятся следующие группы документов, содержащие данные о работниках в единичном или сводном виде:

3.4.1. Документы, содержащие персональные данные работников (комплексы документов, сопровождающие процесс оформления трудовых отношений при приеме на работу, переводе, увольнении; комплекс материалов по анкетированию, тестированию; проведению собеседований с кандидатом 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; служебных расследований; справочно-информационный банк данных по персоналу (картотеки, журналы); подлинники и копии отчетных, аналитических и справочных материалов, передаваемых администрации Учреждения, копии отчетов, направляемых в государственные органы статистики, налоговые инспекции, вышестоящие органы управления и другие учреждения).

3.4.2. Документация по организации работы (положения, должностные инструкции работников, приказы, распоряжения, указания администрации); документы по планированию, учету, анализу и отчетности в части работы с персоналом Учреждения.

4. Сбор, обработка и защита персональных данных

4.1. Порядок получения персональных данных.

Сотрудники Учреждения, осуществляющие в ходе выполнения своих трудовых обязанностей обработку персональных данных, обязаны соблюдать настоящее Положение, знать и соблюдать требования «Инструкции по обработке персональных данных, осуществляемой без использования средств автоматизации» (Приложение № 10) и «Инструкции по обеспечению безопасности персональных данных» (Приложение № 11).

4.1.1. 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 (Приложение №2). Должностное лицо работодателя должно сообщить работнику о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа работника дать письменное согласие на их получение.

4.1.2. Работодатель не имеет права получать и обрабатывать персональные данные работника о его расовой, национальной принадлежности, политических взглядах, религиозных или философских убеждениях, состоянии здоровья, интимной жизни. В случаях, непосредственно связанных с вопросами трудовых отношений, в соответствии Конституцией Российской Федерации работодатель вправе получать и обрабатывать данные о частной жизни работника только с его письменного согласия.

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

– персональные данные являются общедоступными;
– персональные данные относятся к результатам состояния 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;

– по требованию полномочных государственных органов в случаях, предусмотренных федеральным законом.

4.1.3. Обработка персональных данных без средств автоматизации осуществляется в соответствии и «Инструкцией по обработке персональных данных, осуществляемой без использования средств автоматизации» (Приложение № 10).

4.1.4. Работодатель вправе обрабатывать персональные данные работников только с их письменного согласия.

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

– фамилию, имя, отчество, дату рождения (число, месяц, год), адрес субъекта персональных данных, семейное положение, телефон домашний и сотовый, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, ИНН, страховое свидетельство;

– наименование (фамилию, имя, отчество) и адрес оператора, получающего согласие субъекта персональных данных;

– цель обработки персональных данных;

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

– 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 (Приложение №3).

4.1.6. Согласие работника не требуется в следующих случаях:

– обработка персональных данных осуществляется на основании ТКРФ или иного Федерального закона, устанавливающего ее цель, условия получения персональных данных и круг субъектов, персональные данные которых подлежат обработке, а также определяющего полномочия работодателя;

– обработка персональных данных осуществляется в целях исполнения трудового договора;

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

– обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов работника, если получение его согласия невозможно.

4.1.7. В случае отзыва или отказа предоставлять Учреждению персональные данные работнику вручаются разъяснения юридических последствий (Приложение № 4).

4.2. Порядок обработки, передачи и хранения персональных данных.

4.2.1. Работник Учреждения предоставляет заведующей канцелярией достоверные сведения о себе. Заведующий канцелярией проверяет достоверность сведений, сверяя данные, предоставленные работником, с имеющимися у работника документами.

4.2.2. В соответствии с ТК РФ в целях обеспечения прав и свобод человека и гражданина директор Учреждения (Работодатель) и его представители при обработке персональных данных работника должны соблюдать следующие общие требования:

4.2.2.1. 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.

4.2.2.2. При определении объема и содержания, обрабатываемых персональных данных Работодатель должен руководствоваться Конституцией Российской Федерации, Трудовым кодексом Российской Федерации и иными федеральными законами.

4.2.2.3. При принятии решений, затрагивающих интересы работника, Работодатель не имеет права основываться на персональных данных работника, полученных исключительно в результате их автоматизированной обработки или электронного получения.

4.2.2.4. Защита персональных данных работника от неправомерного их использования или утраты обеспечивается Работодателем за счет его средств в порядке, установленном федеральным законом.

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

4.2.2.6. Во всех случаях отказ работника от своих прав на сохранение и защиту тайны недействителен.

5. Передача, хранение, защита, уничтожение персональных данных

5.1. При передаче персональных данных работника Работодатель должен соблюдать следующие требования:

5.1.1. Не сообщать 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 законом.

5.1.2. Не сообщать персональные данные работника в коммерческих целях без его письменного согласия. Обработка персональных данных работников в целях продвижения товаров, работ, услуг на рынке путем осуществления прямых контактов с потенциальным потребителем с помощью средств связи допускается только с его предварительного согласия (Приложение № 5).

5.1.3. Предупредить лиц, получивших персональные данные работника, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получившие персональные данные работника, обязаны соблюдать режим секретности (конфиденциальности). (Приложение №6) Данное Положение не распространяется на обмен персональными данными работников в порядке, установленном федеральными законами.

5.1.4. Осуществлять передачу персональных данных работников в пределах Учреждения в соответствии с настоящим Положением.

5.1.5. Разрешать доступ к персональным данным работников только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные работника, которые необходимы для выполнения конкретной функции (приложение № 8).

5.1.6. Не запрашивать информацию о состоянии здоровья работника, за исключением тех сведений, которые относятся к вопросу о возможности выполнения работником трудовой функции.

5.1.7. Передавать персональные данные работника представителям работников в порядке, установленном Трудовым кодексом Российской Федерации, и ограничивать эту информацию только теми персональными данными работника, которые необходимы для выполнения указанными представителями их функции.

5.2. Хранение и использование персональных данных работников, уничтожение персональных данных:

5.2.1. Персональные данные работников обрабатываются и хранятся в канцелярии, в сейфе и/или шкафу с замком.

5.2.2. Персональные данные работников могут быть получены, проходить дальнейшую обработку и передаваться на хранение, как на бумажных носителях, так и в электронном виде – локальной компьютерной сети, разрешённых к использованию компьютерных программ (продуктов), защищённых каналов связи.

5.2.3. После увольнения (прекращение трудовых отношений) работника персональные данные хранятся в архиве Учреждения в течение срока хранения документов, предусмотренных действующим законодательством Российской Федерации.

5.2.4. По истечении срока хранения документов в архиве персональные данные подлежат уничтожению в течение 30 дней или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством Российской Федерации.

5.2.5. В случае отсутствия возможности уничтожения персональных данных в течение вышеуказанного срока оператор осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем 6 месяцев.

5.2.6. Уничтожение бумажных носителей должно осуществляться сотрудниками, допущенными к обработке персональных данных, путем, не допускающим дальнейшую возможность ознакомления с данными документами (сожжение или размол на бумагорезательной машине). Уничтожение информации на автоматизированных рабочих местах должно осуществляться комиссией способами, не позволяющими восстановить персональные данные.

5.2.7. При уничтожении данных составляется акт с указанием, какие документы и файлы были уничтожены.

5.3. При получении персональных данных не от работника (за исключением случаев, если персональные данные были предоставлены работодателю на основании федерального закона или если персональные данные являются общедоступными) работодатель до начала обработки таких персональных данных обязан предоставить работнику следующую информацию:

– наименование (фамилия, имя, отчество) и адрес оператора или его представителя;

– цель обработки персональных данных и ее правовое основание;

– предполагаемые пользователи персональных данных;

– установленные настоящим Федеральным законом права субъекта персональных данных (Приложение №7).

5.3. Защита персональных данных работников:

5.3.1. При обработке персональных данных должны приниматься необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

5.3.2. Средства вычислительной техники, используемые для обработки персональных данных, должны быть защищены в соответствии с действующими нормативными правовыми актами Российской Федерации, согласно перечню (Приложение № 9), инструкции по работе на вычислительной технике (Приложение № 9а) и инструкций по организации парольной защиты ИСПДн (Приложение № 12), по обеспечению антивирусной защиты ИСПДн (Приложение № 13)

5.3.3. В целях обеспечения сохранности и конфиденциальности персональных данных все операции по оформлению, формированию, ведению и хранению данной информации должны выполняться только сотрудниками, осуществляющими данную работу в соответствии со своими служебными обязанностями, зафиксированными в их должностных инструкциях.

5.3.4. В учреждении назначаются ответственные за обработку персональных данных, обязанности которых определены в должностной инструкции.

5.3.5. Ответы на письменные запросы других организаций и учреждений даются в том объеме, который позволяет не разглашать персональные сведения о гражданах.

5.3.6. Передача информации, содержащей персональные данные граждан, по телефону, факсу, электронной почте без письменного согласия гражданина запрещается.

5.3.7. Персональные данные передаются сторонним организациям в соответствии с действующим законодательством Российской Федерации или на основании договора, условием которого является обязанность обеспечения второй стороной безопасности персональных данных при их обработке.

6. Доступ к персональным данным работников

6.1. Доступ к персональным данным имеют лица согласно перечню должностей МАОУ «Школа-комплекс № 33» (Приложение № 8), замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным

данным и списку сотрудников, которые допускаются к работе с персональными данными в служебных кабинетах Учреждения. Доступ к персональным данным работников имеют:

– директор Учреждения
– заведующий канцелярией;
– сотрудники бухгалтерии;
– заместитель директора по АХР (информация о фактическом месте проживания и контактные телефоны работников);
– заместители директора, старшие воспитатели;
– оператор по работе с персональными данными.

6.2. Сотрудники Учреждения, допущенные к обработке персональных данных, имеют право получать только те персональные данные, которые необходимы им для выполнения своих должностных обязанностей.

6.3 Помещения, в которых ведется обработка персональных данных, должны исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность находящихся в этих помещениях документов и средств автоматизации.

6.4. Входные двери оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время. В конце рабочего дня помещения, в которых ведется обработка персональных данных, закрываются.

6.5. Вскрытие помещений, где ведется обработка персональных данных, производят сотрудники, работающие в этих помещениях. Их уборка осуществляется только в присутствии данных сотрудников.

6.6. Работник имеет право:

6.6.1. Получать доступ к своим персональным данным и ознакомление с ними, включая право на безвозмездное получение копий любой записи, содержащей персональные данные работника.

6.6.2. Требовать от Работодателя уточнения, исключения или исправления неполных, неверных, устаревших, недостоверных, незаконно полученных или не являющихся необходимыми для Работодателя персональных данных.

6.6.3. Получать от Работодателя:

– сведения о лицах, которые имеют доступ к персональным данным или которым может быть предоставлен такой доступ;
– перечень обрабатываемых персональных данных и источник их получения;
– сроки обработки персональных данных, в том числе сроки их хранения;
– сведения о том, какие юридические последствия для субъекта персональных данных может повлечь за собой обработка его персональных данных.

6.6.4. Требовать извещения Работодателем всех лиц, которым ранее были сообщены неверные или неполные персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях.

Обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия Работодателя при обработке и защите его персональных данных.

6.7. Копировать и делать выписки персональных данных работника разрешается исключительно в служебных целях с письменного разрешения заведующего канцелярией.

6.8. Передача информации третьей стороне возможна только при письменном согласии работников (Приложение №5).

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

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

7.2. Директор Учреждения за нарушение норм, регулирующих получение, обработку и защиту персональных данных работника, несет административную ответственность согласно ст. 5.27 и 5.39 Кодекса об административных правонарушениях Российской Федерации, а также возмещает работнику ущерб, причиненный неправомерным использованием информации, содержащей персональные данные работника.

Приложение 1

ПЕРЕЧЕНЬ
персональных данных, обрабатываемых в Муниципальном автономном общеобразовательном учреждении «Средняя общеобразовательная школа-комплекс №33 имени генерал-полковника Ивана Терентьевича Коровникова» города Великого Новгорода

ИСПДн «Сотрудники»:

фамилия, имя, отчество; дата рождения (число, месяц, год); адрес проживания и регистрации; семейное положение; иные паспортные данные; телефон домашний и сотовый; ИНН, страховое свидетельство; персональные данные, содержащиеся в: письменном заявлении с просьбой о поступлении на работу в МАОУ «Школа-комплекс № 33»; собственноручно заполнены и подписаны гражданином Российской Федерации заявление и личная карточка, форма учёта кадров Т-2; копия паспорта и свидетельства о государственной регистрации актов гражданского состояния; трудовая книжка (копия) и документ, подтверждающий прохождение военной или иной службы; копия документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются); экземпляр трудового договора, а также экземпляр письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в трудовой договор; копии распоряжения о переводе сотрудника на иную должность, о временном замещении им иной должности; копии документов воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу); копии распоряжения об освобождении сотрудника от замещаемой должности, о прекращении трудового договора или его приостановлении; аттестационный лист сотрудника, прошедшего аттестацию, копии распоряжения о поощрении сотрудника, а также о наложении на него дисциплинарного взыскания до его снятия или отмены; об отстранении сотрудника от замещаемой должности; копии страхового свидетельства обязательного пенсионного страхования; копии свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации; сведения о результатах состояния здоровья, содержащиеся в личной медицинской книжке.

Приложение 2

В муниципальное автономное общеобразовательное учреждение «Средняя общеобразовательная школа- комплекс № 33 имени генерал-полковника Ивана Терентьевича Коровникова»

СОГЛАСИЕ
на обработку персональных данных

Я, _____
(фамилия, имя, отчество)
проживающ___ по адресу _____
(адрес места регистрации)
паспорт_____
(серия и номер, дата выдачи, название выдавшего органа)
в соответствии с требованиями статьи 9 Федерального закона от 27.07.06 «О персональных данных» № 152-ФЗ подтверждаю свое согласие на обработку муниципальному автономному общеобразовательному учреждению «Средняя общеобразовательная школа- комплекс № 33 имени генерал-полковника Ивана Терентьевича Коровникова» (далее – Оператор), юридический адрес: г. Великий Новгород, ул. Коровникова, д.9, к.1 моих персональных данных:

- фамилия, имя, отчество, дата и место рождения, гражданство;
- прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);
- владение иностранными языками и языками народов Российской Федерации;
- паспортные данные работника, ИНН;
- данные страхового свидетельства государственного пенсионного страхования;
- данные документов об образовании, квалификации или наличии специальных знаний (когда и какие образовательные организации закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);
- послевузовское профессиональное образование (наименование образовательной или научной организации, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);
- выполняемая работа с начала трудовой деятельности (включая военную службу, работу по совместительству, предпринимательскую деятельность);
- государственные награды, иные награды и знаки отличия (кем награжден и когда);
- степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);
- пребывание за границей (когда, где, с какой целью);
- адрес регистрации и фактического проживания;
- дата регистрации по месту жительства;
- номер телефона;
- отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);
- номер страхового свидетельства обязательного пенсионного страхования;
- наличие (отсутствие) судимости;
- документы о результатах состояния здоровья, наличие (отсутствие) заболевания, препятствующего поступлению на работу или ее прохождению, подтвержденного заключением медицинского учреждения; сведения об инвалидности, о беременности и т.п.;
- результаты обязательных медицинских осмотров (обследований), а также обязательного психиатрического освидетельствования;

- сведения, содержащиеся в приказах о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;
- документы о прохождении работником аттестации, повышения квалификации;
- иные документы, содержащие сведения, необходимые для расчета заработной платы, выплаты компенсаций.

А также публикацию данных в соответствии с пп. а п. 3 Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации, утвержденных Постановлением Правительства РФ от 10.07.2013 № 582 «Об утверждении Правил размещения на официальном сайте образовательной организации в информационно-телекоммуникационной сети «Интернет» и обновления информации об образовательной организации».

Вышеуказанные персональные данные предоставляю для обработки в целях обеспечения соблюдения в отношении меня законодательства Российской Федерации в сфере отношений, связанных с поступлением на работу, ее прохождением и прекращением (трудовых и непосредственно связанных с ними отношений), для реализации полномочий, возложенных на оператора действующим законодательством.

Предоставляю Оператору право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение. Оператор вправе обрабатывать мои персональные данные посредством внесения их в электронную базу данных, включения в списки (реестры) и отчетные формы, предусмотренные документами, регламентирующими предоставление отчетных данных (документов), и передавать их уполномоченным органам.

Я ознакомлен(а) с тем, что:

1) согласие на обработку персональных данных действует с даты подписания настоящего согласия в течение всего срока работы;

2) согласие на обработку персональных данных может быть отозвано на основании письменного заявления в произвольной форме;

3) в случае отзыва согласия на обработку персональных данных, оператор в праве продолжить обработку персональных данных без согласия при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;

4) после увольнения с работы (прекращения трудовых отношений) персональные данные хранятся в архиве оператора в течение срока хранения документов, предусмотренных действующим законодательством Российской Федерации;

5) персональные данные, предоставляемые в отношении третьих лиц, будут обрабатываться только в целях осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.

Об ответственности за достоверность представленных сведений предупрежден (предупреждена) нужное подчеркнуть.

Подтверждаю, что ознакомлен(а) с Положением о защите персональных данных и положениями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», права и обязанности в области защиты персональных данных мне разъяснены.

Начало обработки персональных данных с момента подписания данного согласия:

«___»_____20__г. _____

(подпись)

Приложение 3

ЗАЯВЛЕНИЕ
на отзыв согласия на обработку персональных данных

В муниципальное автономное общеобразовательное учреждение «Средняя общеобразовательная школа-комплекс № 33 имени генерал-полковника Ивана Терентьевича Коровникова»

_____
Ф.И.О. субъекта персональных данных

_____
Адрес, где зарегистрирован субъект персональных данных

_____
Номер основного документа, удостоверяющего его личность

_____
Дата выдачи указанного документа

_____
Наименование органа, выдавшего документ

Заявление

Прошу Вас прекратить обработку моих персональных данных в связи с
_____
_____
_____
(указать причину)

«___» _____ 20__ г. _____ _____
(подпись) (расшифровка подписи)

Приложение 4

Разъяснения субъекту персональных данных юридических последствий отказа предоставить свои персональные данные

Уважаемый(ая), _____ !

Администрация МАОУ «Школа-комплекс №33» (далее - Учреждение)уведомляет Вас, что обязанность предоставления Вами персональных данных установлена в соответствии с требованиями Федерального закона Российской Федерации от 27 июля2006 года № 152-ФЗ «О персональных данных» уведомляет Вас, что_____(пункт) названного Федерального закона, а также следующими локальными актами «Положение об обработке персональных данных работников МАОУ «Школа – комплекс № 33», утвержденного приказом директора Учреждения № 75 –а от 31.08.2015 г.

В случае Вашего отказа предоставить свои персональные данные Администрация Учреждения не сможет на законных основаниях осуществлять такую обработку, что приведет к следующим для Вас юридическим последствиям:_____
_____
_____
(перечисляются юридические последствия для субъекта ПД, то есть случаи возникновения, изменения или прекращения личных, либо имущественных прав гражданина или случаи, иным образом, затрагивающие его права, свободы и законные интересы)

В соответствии с действующим законодательством Российской Федерации в области персональных данных Вы имеете право: на получение сведений от Учреждения (в объеме, необходимом для защиты своих прав и законных интересов по вопросам обработки своих персональных данных), о месте нахождения Учреждения, о наличии у Учреждения Ваших персональных данных, а также на ознакомление с такими персональными данными; подавать запрос на доступ к своим персональным данным; требовать безвозмездного предоставления возможности ознакомления со своими персональными данными, а также внесения в них необходимых изменений, их уничтожения или блокирования при предоставлении сведений, подтверждающих, что такие персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки; получать уведомления по вопросам обработки персональных данных в установленных действующим законодательством Российской Федерации случаях и сроки; требовать от Учреждения, разъяснения порядка защиты субъектом персональных данных своих прав и законных интересов; обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке; на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

Директор МАОУ «Школа-комплекс №33» _____/_____

С уведомлением ознакомлен(а) _____
(дата) (подпись) (расшифровка подписи)

Приложение 5

В муниципальное автономное общеобразовательное учреждение «Средняя общеобразовательная школа-комплекс № 33 имени генерал-полковника Ивана Терентьевича Коровникова»

Заявление-согласие субъекта на передачу его персональных данных третьей стороне

Я, _____, паспорт серии _____, номер _____, выданный _____ _____ « ___ » _____ _____ года, в соответствии со ст.88 Трудового Кодекса Российской Федерации _____ на передачу моих персональных данных, а именно: согласен /не согласен (нужное подчеркнуть)
– паспортные данные работника, ИНН;
– данные страхового свидетельства государственного пенсионного страхования;
– данные документов об образовании, квалификации или наличии специальных знаний;
– анкетные данные, (в том числе сведения о семейном положении, перемене фамилии, наличии детей и иждивенцев);
– документы о возрасте малолетних детей и месте их обучения;
– документы о результатах состояния здоровья (сведения об инвалидности, о беременности и т.п.);
– сведения, содержащиеся в приказах о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;
– документы о прохождении работником аттестации, повышения квалификации;
– иные документы, содержащие сведения, необходимые для расчета заработной платы, выплаты компенсаций.

Для обработки в целях обеспечения расчета и начисления заработной платы, уплаты налогов и выполнения иных обязанностей в соответствии с действующим законодательством следующим лицам _____
_____
_____
(указать Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их передачу.

« ___ » _____ 20__ г. _____ / _____
(подпись) ФИО

Приложение 6

Соглашение о неразглашении персональных данных субъекта

Я, _____, паспорт серии _____, номер _____, выданный _____ _____

« ___ » _____ _____ года, понимаю, что получаю доступ к персональным данным работников и/или обучающихся муниципального автономного общеобразовательного учреждения “Средняя общеобразовательная школа-комплекс № 33 имени генерал-полковника Ивана Терентьевича Коровникова”

Я также понимаю, что во время исполнения своих обязанностей, мне приходится заниматься сбором, обработкой и хранением персональных данных.

Я понимаю, что разглашение такого рода информации может нанести ущерб субъектам персональных данных, как прямой, так и косвенный.

В связи с этим, даю обязательство, при работе (сбор, обработка и хранение) с персональными данными соблюдать все описанные в «Положении об обработке и защите персональных данных» требования.

Я подтверждаю, что не имею права разглашать сведения:

- анкетные и биографические данные;
- сведения об образовании;
- сведения о трудовом и общем стаже;
- сведения о составе семьи;
- паспортные данные;
- сведения о воинском учете;
- сведения о заработной плате сотрудника;
- сведения о социальных льготах;
- специальность;
- занимаемая должность;
- наличие/отсутствие судимостей;
- адрес места жительства;
- домашний телефон;
- содержание трудового договора;
- подлинники и копии приказов по личному составу;
- личные дела и трудовые книжки сотрудников;
- основания к приказам по личному составу;
- дела, содержащие материалы по повышению квалификации и переподготовке, их аттестации;
- копии отчетов, направляемые в органы статистики и пр.

Я предупрежден (а) о том, что в случае разглашения мной сведений, касающихся персональных данных или их утраты я несу ответственность в соответствии со ст. 90 Трудового Кодекса Российской Федерации.

« ___ » _____ 20__ г. _____ / _____

(подпись) ФИО

Приложение 7

В Муниципальное автономное общеобразовательное учреждение «Средняя общеобразовательная школа-комплекс № 33 имени генерал-полковника Ивана Терентьевича Коровникова»

Заявление-согласие субъекта на получение его персональных данных у третьей стороны

Я, _____, паспорт серии _____, номер _____, выданный _____ _____ « ___ » _____ _____ года, в соответствии со ст.86 Трудового Кодекса Российской Федерации _____ на получение моих персональных данных, а именно: согласен /не согласен (нужное подчеркнуть)

– паспортные данные работника, ИНН;
– данные страхового свидетельства государственного пенсионного страхования;
– данные документов об образовании, квалификации или наличии специальных знаний;
– анкетные данные, (в том числе сведения о семейном положении, перемене фамилии, наличии детей и иждивенцев);
– документы о возрасте малолетних детей и месте их обучения;
– документы о состоянии здоровья детей и других родственников (включая справки об инвалидности, о наличии хронических заболеваний);
– документы о результатах состояния здоровья (сведения об инвалидности, о беременности и т.п.);
– сведения, содержащиеся в приказах о приеме, переводах, увольнении, повышении заработной платы, премировании, поощрениях и взысканиях;
– документы о прохождении работником аттестации, повышения квалификации;
– иные документы, содержащие сведения, необходимые для расчета заработной платы, выплаты компенсаций.

Для обработки в целях обеспечения расчета и начисления заработной платы, уплаты налогов и выполнения иных обязанностей в соответствии с действующим законодательством у следующих лиц _____
_____
_____

(указать Ф.И.О. физического лица или наименование организации, которым сообщаются данные)

Я также утверждаю, что ознакомлен с возможными последствиями моего отказа дать письменное согласие на их получение.

« ___ » _____ 20__ г. _____ / _____
(подпись) ФИО

Приложение 8

ПЕРЕЧЕНЬ
должностей, допустимых и замещение которых предусматривает осуществление обработки персональных данных либо осуществление доступа к персональным данным

№ п/п	Наименование должностей	Количество штатных единиц	Виды работы с персональными данными (далее – ПД)
1	Директор учреждения	1	Доступ к ПД
2	Заместители директора	5	Обработка ПД
3	Старшие воспитатели	1	Обработка ПД
4	Главный бухгалтер, заместитель главного бухгалтера, бухгалтер	3	Обработка ПД
5	Заведующий канцелярией, делопроизводитель	2	Обработка ПД

Приложение 9

ПЕРЕЧЕНЬ
защищаемых ресурсов информационной системы персональных данных Муниципального автономного общеобразовательного учреждения «Средняя общеобразовательная школа-комплекс №33 имени генерал-полковника Ивана Терентьевича Коровникова»

Место расположения ИСПДн «Сотрудники», ИСПДн «Дети»:
173024, Великий Новгород, ул. Коровникова, д.9, к.1;
Место расположения ИСПДн «Дети»:
173024, Великий Новгород, ул. Кочетова, д.6, к.4;

Защищаемый ресурс	Реализация ресурса	Степень конфиденциальности информации
Сведения, включенные в перечень персональных данных подлежащих защите	Файлы и архивы файлов, расположенные на несъемном жестком магнитном диске персональных компьютеров, съемных магнитных носителях, учтенных в «Журнале учета машинных носителей, содержащих персональные данные	Конфиденциально

Приложение 9 а

ИНСТРУКЦИЯ
пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники в МАОУ «Школа-комплекс №33»

I. Общие положения

1.1. Настоящая Инструкция разработана в соответствии Приказа ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (ред. от 14.05.2020) и является дополнением к «Положению об обработке персональных данных работников в МАОУ школа-комплекс №33» (далее по тексту – Учреждение).
1.2. Инструкция пользователя, осуществляющего обработку персональных данных на объектах вычислительной техники (далее – Инструкция), регламентирует основные обязанности, права и ответственность пользователя, допущенного к автоматизированной обработке персональных данных и иной конфиденциальной информации на объектах вычислительной техники (ПЭВМ) образовательного учреждения (далее - ОУ).
1.3.Инструкция регламентирует деятельность пользователя, который имеет допуск к обработке соответствующих категорий персональных данных и обладает необходимыми навыками работы на ПЭВМ.

II. Обязанности пользователя

2.1. При выполнении работ в пределах своих функциональных обязанностей пользователь несет персональную ответственность за соблюдение требований нормативных документов по защите информации.
2.2. Пользователь обязан:

- выполнять требования Инструкции по обеспечению режима конфиденциальности проводимых работ;
- при работе с персональными данными исключать присутствие в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц, а также располагать во время работы экран видеомонитора так, чтобы отображаемая на нем информации была недоступна для просмотра посторонними лицами;
- соблюдать правила работы со средствами защиты информации, а также установленный режим разграничения доступа к техническим средствам, программам, данным и файлам с персональными данными при ее обработке;
- после окончания обработки персональных данных в рамках выполнения одного задания, а также по окончании рабочего дня производить стирание остаточной информации с жесткого диска ПЭВМ;
- оповещать обслуживающий ПЭВМ персонал, а также непосредственного руководителя обо всех фактах или попытках несанкционированного доступа к информации, обрабатываемой в ПЭВМ;
- не допускать "загрязнения" ПЭВМ посторонними программными средствами;
- знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, меры предотвращения ухудшения ситуации;
- знать и соблюдать правила поведения в экстренных ситуациях, порядок действий при ликвидации последствий аварий;
- помнить личные пароли и персональные идентификаторы;
- знать штатные режимы работы программного обеспечения, пути проникновения и распространения компьютерных вирусов;
- при применении внешних носителей информации перед началом работы проводить их проверку на наличие компьютерных вирусов.

2.3. 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.) пользователь должен провести внеочередной антивирусный контроль своей рабочей станции. В случае обнаружения зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов своего непосредственного руководителя, администратора системы, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

2.4. Пользователю ПЭВМ запрещается:

- записывать и хранить персональные данные на неучтенных в установленном порядке машинных носителях информации;
- удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;
- самостоятельно подключать к ПЭВМ какие-либо устройства, а также вносить изменения в состав, конфигурацию и размещение ПЭВМ;
- самостоятельно устанавливать и/или запускать на ПЭВМ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;
- осуществлять обработку персональных данных в условиях, позволяющих просматривать их лицами, не имеющими к ним допуска, а также нарушающих требования к эксплуатации ПЭВМ;
- сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ПЭВМ;
- отключать (блокировать) средства защиты информации;
- производить какие-либо изменения в подключении и размещении технических средств;
- производить иные действия, ограничения на исполнение которых предусмотрены утвержденными регламентами и инструкциями;
- бесконтрольно оставлять ПЭВМ с загруженными персональными данными, установленными маркированными носителями, электронными ключами и выведенными на печать документами, содержащими персональные данные.

III. Права пользователя

3.1. Пользователь ПЭВМ имеет право:

- обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленных ему полномочий;
- обращаться к обслуживающему ПЭВМ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным в ПЭВМ, а также со средствами защиты информации.

IV. Заключительные положения

4.1. Особенности обработки персональных данных пользователями отдельных автоматизированных систем могут регулироваться дополнительными инструкциями.

4.2. Работники подразделений учреждения и лица, выполняющие работы по договорам и контрактам и имеющие отношение к обработке персональных данных на объектах вычислительной техники, должны быть ознакомлены с Инструкцией под расписку.

Приложение 10

Инструкция
по обработке персональных данных, осуществляемых
без использования средств автоматизации

1 Общие положения

Настоящая Инструкция разработана в соответствии с «Положением об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утвержденным Постановлением Правительства РФ от 15.09.2008 № 687, является дополнением к «Положению об обработке персональных данных работников в МАОУ школа-комплекс №33» (далее по тексту – Учреждение) и определяет правила работы с персональными данными и их материальными носителями без использования средств автоматизации.

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

Документ, содержащий персональные данные - материальный носитель с зафиксированной на нем в любой форме информацией, содержащей персональные данные работников (или граждан в договорах с физическими лицами) в виде текста, фотографии и (или) их сочетания.

С учетом большого объема (массовости) документов, содержащих персональные данные, и строго регламентированного порядка их хранения пометка конфиденциальности на них не ставится.

С настоящей инструкцией должны быть ознакомлены под роспись работники, допускаемые к обработке персональных данных без использования средств автоматизации. Листы ознакомления хранятся у ответственного за систему защиты информации в информационной системе персональных данных.

2 Порядок обработки персональных данных

Персональные данные должны обособляться от иной информации путем фиксации их на отдельных материальных носителях, в специальных разделах или на полях форм (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, для каждой категории персональных данных должен использоваться отдельный материальный носитель.

Работники, осуществляющие обработку персональных данных, информируются непосредственным руководителем о факте обработки ими персональных данных, категориях обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки.

Типовые формы документов должны быть составлены таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, содержащимися в документе, не нарушая прав и законных интересов иных субъектов персональных данных.

Хранение документов, содержащих персональные данные, осуществляется в шкафах или сейфах под замком.

Уничтожение документов, содержащих персональные данные, осуществляется способом, не позволяющим в дальнейшем ознакомиться с персональными данными.

3 Обязанности сотрудника, допущенного к обработке персональных данных

При работе с документами, содержащими персональные данные, сотрудник обязан исключить возможность ознакомления, просмотра этих документов лицами, не

допущенными к работе с ними (в том числе другими работниками своего структурного подразделения).

При выносе документов, содержащих персональные данные, за пределы территории Учреждения по служебной необходимости сотрудник должен принять все возможные меры, исключающие утрату (утерю, хищение) таких документов.

При утрате (утере, хищении) документов, содержащих персональные данные, работник обязан немедленно доложить о таком факте директору Учреждения либо непосредственному руководителю. Непосредственный руководитель должен сообщить заместителю директора, курирующему вопросы защиты информации о факте утраты (утере, хищении) документов, содержащих персональные данные. По каждому такому факту назначается служебное расследование.

4 Сотрудникам, допущенным к обработке персональных данных запрещается

4.1 Сообщать сведения, являющиеся персональными данными, лицам, не имеющим права доступа к этим сведениям.

4.2 Делать неучтенные копии документов, содержащих персональные данные.

4.3 Оставлять документы, содержащие персональные данные, на рабочих столах без присмотра.

4.4 Покидать помещение, не поместив документы с персональными данными в закрываемые сейфы, шкафы.

4.5 Выносить документы, содержащие персональные данные, из помещений Учреждения без служебной необходимости.

5 Ответственность

5.1 Ответственность за неисполнение или ненадлежащее выполнение требований настоящей Инструкции возлагается на работников и руководителей подразделений.

5.2 Контроль за выполнением положений настоящей Инструкции возлагается на ответственного за систему защиты информации в информационной системе персональных данных.

5.3 За нарушение правил обработки персональных данных, их неправомерное разглашение или распространение, виновные лица несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством.

5.4 В случае если в результате действий работника был причинен подлежащий возмещению работодателем ущерб третьим лицам, работник несет перед работодателем материальную ответственность в соответствии с главой 39 Трудового кодекса РФ.

5.5 В случае разглашения персональных данных, ставших известными работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника, трудовой договор с работником может быть расторгнут работодателем (подпункт «в» пункта 6 статьи 81 Трудового кодекса РФ).

Приложение 11

ИНСТРУКЦИЯ
по обеспечению безопасности персональных данных

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция разработана в соответствии со ст. 19 Федерального закона РФ от 27.07.2006 г. № 152-ФЗ «О персональных данных» является дополнением к «Положению об обработке персональных данных работников в МАОУ школа-комплекс №33» (далее по тексту – Учреждение) и определяет правила работы с персональными данными и их материальными носителями.

1.2. Для обеспечения безопасности персональных данных необходимо исключить несанкционированный, в том числе случайный, доступ к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иные несанкционированные действия.

1.3. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

1.4. Ответственность за безопасность персональных данных в Учреждении возлагается на лиц, допущенных к их обработке.

2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕД НАЧАЛОМ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Перед началом обработки персональных данных необходимо изучить настоящую Инструкцию.

Перед началом обработки персональных данных необходимо убедиться в том, что:

- средства защиты персональных данных соответствуют классу информационной системы;
- в помещении, в котором ведется работа с персональными данными, отсутствуют посторонние лица;
- носители персональных данных не повреждены;
- к персональным данным не был осуществлен несанкционированный доступ;
- персональные данные не повреждены;
- технические средства автоматизированной обработки и защиты персональных данных находятся в исправном состоянии.

3. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ВО ВРЕМЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Во время обработки персональных данных необходимо обеспечить:

- недопущения воздействия на технические средства автоматизированной обработки персональных данных, способного нарушить их функционирование;
- недопущение нахождения в помещении, в котором ведется работа с персональными данными, посторонних лиц;
- постоянный контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
- недопущение несанкционированного доступа к персональным данным;
- конфиденциальность персональных данных.

4. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В ЭКСТРЕМАЛЬНЫХ СИТУАЦИЯХ

4.1. При модификации или уничтожения персональных данных, вследствие несанкционированного доступа к ним необходимо обеспечить возможность их незамедлительного восстановления.

4.2. При нарушении порядка предоставления персональных данных пользователям информационной системы необходимо приостановить их предоставление.

4.3. При обнаружении несанкционированного доступа к персональным данным необходимо немедленно прервать этот доступ.

4.4. В случае несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных необходимо произвести разбирательство и составление заключений по данным фактам, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.
4.5. Обо всех экстремальных ситуациях необходимо немедленно поставить в известность директора учреждения и произвести разбирательство.

5. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИ ЗАВЕРШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

5.1. После завершения сеанса обработки персональных данных необходимо обеспечить:

- исключение возможности несанкционированного проникновения или нахождения в помещении, в котором размещены информационные системы и ведется работа с персональными данными;
- работоспособность средств защиты информации, функционирующих при отсутствии лиц, допущенных к обработке персональных данных;
- фиксацию всех случаев нарушения данной инструкции в журнале.

6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1. Проверка и пересмотр настоящей инструкции осуществляются в следующих случаях:

- при пересмотре межотраслевых и отраслевых требований обеспечения безопасности персональных данных;
- при внедрении новой техники и (или) технологий;
- по результатам анализа материалов расследования нарушений требований законодательства об обеспечении безопасности персональных данных;
- по требованию представителей Федеральной службы безопасности.

Приложение 12

ИНСТРУКЦИЯ
по организации парольной защиты в информационной системе персональных данных в МАОУ «Школа-комплекс №33»

1. Общие положения

1.1. Данная инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационной системе персональных данных (ИСПДн) в МАОУ «Школа-комплекс №33» (далее по тексту –Учреждение), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с идентификаторами и с личными паролями.

1.2. Настоящая Инструкция является дополнением к «Положению об обработке персональных данных работников в МАОУ школа-комплекс №33» (далее по тексту – Учреждение) в области защиты персональных данных.

1.3. Пользователем ИСПДн (далее – Пользователь) является сотрудник, участвующий в рамках выполнения своих функциональных обязанностей в процессах автоматизированной обработки персональных данных (далее – ПДн) и имеющий доступ к аппаратным средствам, программному обеспечению, данным и средствам защиты информации ИСПДн (далее – СЗИ).

1.4. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей в ИСПДн и контроль над действиями Пользователей в ИСПДн осуществляет ответственный за обеспечение безопасности персональных данных в учреждении (далее – Ответственный).

1.5. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей на автоматизированных рабочих местах (далее – АРМ) Пользователей осуществляет администратор ИСПДн в Учреждении (далее – Администратор).

2. Организация парольной защиты

2.1. Личные пароли должны создаваться Пользователями самостоятельно.

2.2. В случае формирования личных паролей Пользователей централизованно, ответственность за правильность их формирования и распределения возлагается на Ответственного и Администратора в ИСПДн и на АРМ Пользователей соответственно.

2.3. Полная плановая смена паролей в ИСПДн проводится не реже одного раза в год.

2.4. Внеплановая смена личного пароля Пользователя или удаление учетной записи в случае прекращения его полномочий (увольнение, переход на другую должность в ИСПДн и т.п.) должна производиться Администратором и Ответственным немедленно после окончания последнего сеанса работы Пользователя в АРМ и в ИСПДн соответственно.

2.5. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение и другие обстоятельства) администратора безопасности информации.

2.6. В ИСПДн устанавливается ограничение на количество неуспешных попыток аутентификации (ввода логина и пароля) Пользователя, равное 7, после чего учетная запись блокируется.

2.7. Разблокирование учетной записи осуществляется Администратором и Ответственный для учетных записей Пользователя для АРМ и для ИСПДн соответственно.

2.8. После 15 минут бездействия (неактивности) Пользователя в АРМ или ИСПДн происходит автоматическое блокирование сеанса доступа в АРМ и ИСПДн соответственно.

2.9. Хранение пользователем зарегистрированных идентификаторов и значений своих паролей на бумажном носителе допускается только в сейфе у заведующего канцелярией.

2.10. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администратора безопасности информации.

3. Требования к формированию паролей

Пользователи при формировании паролей должны руководствоваться следующими требованиями:

3.1. Длина пароля должна быть не менее 8 символов.

3.2. В пароле должны обязательно присутствовать символы не менее 3-х категорий из следующих:

- буквы в верхнем регистре;
- буквы в и нижнем регистре;
- цифры;
- специальные символы, не принадлежащие алфавитно-цифровому набору (например, !, @, #, $, &, *, % и т.п.).

3.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (например, «112», «911» и т.п.), а также общепринятые сокращения (например, «ЭВМ», «ЛВС», «USER» и т.п.).

3.4. Пароль не должен содержать имя учетной записи Пользователя или наименование его АРМ, а также какую-либо его часть.

3.5. Пароль не должен основываться на именах и датах рождения Пользователя или его родственников, кличек домашних животных, номеров автомобилей, телефонов и т.д., которые можно угадать, основываясь на информации о Пользователе.

3.6. Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов (например, «1111111», «wwwww» и т.п.).

3.7. Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, «1234567», «qwerty» и т.п.).

3.8. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

4. Правила ввода паролей

Пользователи во время процедуры аутентификации (ввода логина и пароля) на АРМ и в ИСПДн должны руководствоваться следующими правилами:

4.1. Ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан.

4.2. Во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и пр.).

4.3. В случае блокировки учетной записи Пользователя после превышения попыток ввода данных аутентификации (логина и пароля) в АРМ или ИСПДн, Пользователю необходимо уведомить Администратора или Ответственный соответственно для проведения процедуры генерации нового пароля.

5. Обязанности

Пользователи ИСПДн обязаны:

5.1. Четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по парольной защите.

5.2. Своевременно сообщать Ответственному и Администратору об утере, компрометации и несанкционированном изменении сроков действия паролей в АРМ и ИСПДн соответственно.

5.3. В случае утечки информации о зарегистрированном пользователе необходимо НЕМЕДЛЕННО УДАЛИТЬ данные об этом пользователе и ЗАРЕГИСТРИРОВАТЬ ЗАНОВО его с новым идентификатором.

5.4. Ознакомиться под роспись с перечисленными в настоящей инструкции требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

6. Ответственность

6.1. Пользователь несет персональную ответственность за сохранность данных аутентификации (персонального логина и пароля) к АРМ и к ИСПДн.

Приложение 13

Инструкция по обеспечению антивирусной защиты ИСПДн

1 Общие положения

Данный документ определяет правила и основные требования по обеспечению антивирусной защиты ИСПДн в МАОУ «Школа-комплекс №33» (далее - Учреждения) и устанавливает ответственность за их выполнение.

Действие настоящей инструкции распространяется в полном объеме на Учреждение и обязательна для выполнения всеми сотрудниками.

2 Инструкция по применению средств антивирусной защиты

2.1. Защита программного обеспечения ИСПДн от вредоносного ПО осуществляется путем применения специализированных средств антивирусной защиты.
2.2. К использованию допускаются только лицензионные антивирусные средства, обладающие сертификатами регулирующих органов РФ.
2.3. Решение задач по установке и сопровождению средств антивирусной защиты возлагается на ответственного за СЗИ ИСПДн.
2.4. Частота обновления баз данных средств антивирусной защиты устанавливается не реже 1 раза в сутки.
2.5. Все впервые вводимое в эксплуатацию программное обеспечение должно проходить обязательный антивирусный контроль.
2.6. Контроль системы управления средствами антивирусной защиты осуществляется централизованно с рабочего места ответственного за СЗИ ИСПДн.
2.7. Средства антивирусной защиты устанавливаются на всех рабочих станциях и серверах Учреждения.
2.8. Ежедневно в установленное время в автоматическом режиме проводится антивирусный контроль всех дисков и файлов рабочих станций и серверов.
2.9. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы, архивы), получаемая и передаваемая по телекоммуникационным каналам (включая электронную почту), а также информация на съемных носителях.
2.10. Контроль входящей информации необходимо проводить непосредственно после ее приема.
2.11. Контроль исходящей информации необходимо проводить непосредственно перед отправкой.
2.12. Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль.
2.13. 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.) пользователь, обнаруживший проблему, должен провести внеочередной антивирусный контроль рабочей станции либо обратиться к ответственному за СЗИ ИСПДн.
2.14. При получении информации о возникновении вирусной эпидемии вне Учреждения должно быть осуществлено информирование пользователей о возможной эпидемии и рекомендуемых действиях.
2.15. В случае обнаружения зараженных компьютерными вирусами файлов пользователи обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения вируса ответственного за СЗИ ИСПДн;
- провести лечение зараженных файлов;
- в случае невозможности лечения обратиться к сотруднику, ответственному за СЗИ ИСПДн;

2.16. По факту обнаружения зараженных вирусом файлов сотрудник, ответственный за СЗИ ИСПДн, должен составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.
2.17. Пользователям запрещается отключать, выгружать или деинсталлировать средства антивирусной защиты на рабочих станциях.
2.18. Настройка параметров средств антивирусной защиты осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.
2.19. Ответственный за СЗИ ИСПДн должен проводить расследования случаев появления вирусов для выявления причин и принятия соответствующих действий по их предотвращению.
2.20. Пользователи должны быть ознакомлены с данной инструкцией под роспись.
2.21. Проводить периодическое тестирование функций средств антивирусной защиты.
2.22. Проводить тестирование функций средств антивирусной защиты при изменениях (внедрении новых средств, их обновлении, изменениях в системе).