МАОУ "СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 10"

Подписано цифровой подписью: МАОУ "СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 10"
Дата: 2021.06.18 10:20:55 +03'00'

Приложение 1
к приказу № 41
от 01.09.2018г

УТВЕРЖДАЮ
Директор
МАОУ «Средняя школа №10»
_____В.Н.Верясов

ПОЛОЖЕНИЕ
о порядке обработки и защите персональных данных работников и обучающихся МАОУ «Средняя общеобразовательная школа №10»

1. Общие положения

1.1. Настоящее Положение о защите персональных данных обучающихся и работников (далее — Положение) разработано с целью зашиты информации, относящейся к личности и личной жизни работников и обучающихся муниципального общеобразовательного учреждения «Средняя общеобразовательная школа № 10» (далее - школа).

1.2. Положение разработано в соответствии со статьей 24 Конституции Российской Федерации, главой 14 Трудового кодекса Российской Федерации и Федеральными законами от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 года № 152-ФЗ «О персональных данных».

1.3. Настоящее Положение устанавливает цели обработки персональных данных, а также перечень персональных данных, объем, характер и способы, обработки которых полностью соответствуют установленным целям.

1.4. Настоящим Положением определяется порядок сбора, систематизации, накопления, хранения, уточнения (обновления, изменения), обезличивания, блокирования, уничтожения персональных данных работников школы, учащихся и их законных представителей.

1.5 Персональные данные относятся к категории конфиденциальной информации. Режим конфиденциальности персональных данных снимается в случае обезличивания или по истечении 75-летнего срока хранения, если иное не определено законом.

1.6. Контроль за соблюдением требований настоящего Положения осуществляет директор школы.

2. Основные понятия, используемые в настоящем положении

2.1. Блокирование персональных данных - временное прекращение сбора, систематизации, накопления, использования и распространения персональных данных, в т.ч. их передачи.

2.2. Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами,

позволяющими определить такую информацию или ее материальный носитель.

2.3. Информационная система персональных данных — совокупность персональных данных, содержащаяся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием или без использования средств автоматизации.

2.4. Использование персональных данных — действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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

2.6. Обезличивание персональных данных - действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

2.7. Обработка персональных данных — действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных,

2.8. Общедоступные персональные данные — персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

2.9. Оператор — юридическое лицо (ОУ), организующее и (или) осуществляющее обработку персональных данных, а также определяющее цели и содержание обработки персональных данных.

2.10. Персональные данные — любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

2.11. Персональные данные работника — информация, необходимая работодателю в связи с трудовыми отношениями и касающаяся конкретного работника.

2.12. Персональные данные обучающихся — информация, необходимая школе в связи с отношениями, возникающими между обучающимся, его родителями (законными представителями) и школой.

2.13. Распространение персональных данных — действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

2.14. Субъекты персональных данных ОУ (далее субъекты) — носители персональных данных, в т.ч, работники ОУ, обучающиеся и их родители (законные представители), передавшие свои персональные данные ОУ на добровольной основе и (или) в рамках выполнения требований нормативно-правовых актов для их приема, получения, поиска, сбора, систематизации, накопления, хранения, уточнения, использования, распространения (в т.ч. передачи) и обезличивания.

2.15.Укрупненный перечень персональных данных — перечень персональных данных субъектов, определённых к обработке оператором в каждом структурном подразделении ОУ.

3. Цели обработки персональных данных

3.1. Оператором, организующим и осуществляющим обработку персональных данных, является Школа.

3.2. Субъектами персональных данных являются работники школы, с которыми оператора связывают трудовые отношения, а также обучающиеся, с которыми оператора связывает деятельность, определённую Уставом школы и договорами гражданско-правового характера.

3.3. Обработка персональных данных осуществляется в целях реализации прав и обязанностей Школы в отношении субъектов персональных данных, установленных трудовым законодательством, Законом «Об образовании РФ», Гражданским Кодексом РФ с учетом положений Устава МАОУ «Средняя общеобразовательная школа №10», для решения следующих задач:

3.3.1. Организация системы кадрового учета.

3.3.2. Осуществление функции учета и отчетности по расходам, связанным с оплатой труда.

3.3.3. Организации системы учёта контингента учащихся.

3.3.4. Осуществление функции учёта и отчётности по финансово-хозяйственной деятельности школы, функционирующей в условиях нормативного (подушевого) финансирования.

3.3.5. Обеспечение воинского учета.

4. Документы, содержащие персональные данные

4.1. К документам, содержащим персональные данные работников школы, относятся:

- трудовые книжки;

- письменное заявление о поступлении на работу;

- собственноручно заполненная и подписанная анкета работника, установленной формы с приложением фотографии;

- копия паспорта;

- копии свидетельств о государственной регистрации актов гражданского состояния;

- копия трудовой книжки;

- копия документа, подтверждающего прохождение военной или иной службы;

- копии документов о профессиональном образовании, профессиональной переподготовке, повышении квалификации, стажировке, присвоении ученой степени, ученого звания (если таковые имеются);

- копии решений о награждении государственными наградами, присвоении почетных званий, присуждении государственных премий (если таковые имеются);

- экземпляр трудового договора, а также экземпляры письменных дополнительных соглашений, которыми оформляются изменения и дополнения, внесенные в трудовой договор;

- копии приказов о переводе работника на иную должность;

- копии документов воинского учета (для военнообязанных и лиц, подлежащих призыву на военную службу);

- аттестационный лист педагогического работника, прошедшего аттестацию, и отзыв об исполнении им должностных обязанностей за аттестационный период;

- копии решений о поощрении работника, а также о наложении на него дисциплинарного взыскания до его снятия или отмены;

- заявления, объяснительные и служебные записки работника;

- копии документов о начале служебной проверки, ее результатах, об отстранении работника от занимаемой должности;

- договор об оформлении допуска к сведениям, составляющим государственную или иную охраняемую законом тайну, если исполнение обязанностей по занимаемой должности связано с использованием таких сведений;

- сведения о доходах, имуществе и обязательствах имущественного характера работника;

- копия страхового свидетельства обязательного пенсионного страхования;

- копия свидетельства о постановке на учет в налоговом органе физического лица по месту жительства на территории Российской Федерации;

- копия страхового медицинского полиса обязательного медицинского страхования граждан;

- документы о состоянии здоровья (сведения об инвалидности, о беременности и т.п.);

- иные документы, которые с учетом специфики работы и в соответствии с законодательством Российской Федерации должны быть предъявлены

работником при заключении трудового договора или в период его действия (включая медицинские заключения, предъявляемые работником при прохождении обязательных предварительных и периодических медицинских осмотров);

- документы, содержащие сведения о работнике, нахождение которых в личном деле работника необходимо для документального оформления трудовых правоотношений с работником (включая приговоры суда о запрете заниматься педагогической деятельностью или занимать руководящие должности).

- иные документы, установленные федеральными законами, иными нормативными актами Российской Федерации, муниципальными нормативными актами, представляемые при поступлении на работу и в процессе осуществления трудовой деятельности;

- личные карточки формы Т-2;

- справки-объективки;

- журнал учета движения трудовых книжек и вкладышей к ним;

- журнал учета принятых и уволенных работников школы;

- журнал учета личных дел;

- журнал учета трудовых договоров;

- журнал учета листков нетрудоспособности;

- списки работников школы, подлежащих обязательному медицинскому страхованию;

- трудовые договоры;

- табели учета рабочего времени;

- документы по индивидуальному (персонифицированному) учету в системе обязательного пенсионного страхования (в соответствии с Постановлением Правления Пенсионного фонда Российской Федерации от 31.07.2006 № 192п «О формах документов индивидуального (персонифицированного) учета в системе обязательного пенсионного страхования и инструкции по их заполнению» (в ред. Постановлений Правления ПФ РФ от 01.06.2016 N 473п);

- расчетно-платежная ведомость (форма по ОКУД 0504401);

- платежная ведомость (форма по ОКУД 0504403);

- расчетный листок;

- карточка-справка (форма по ОКУД 0504417);

- налоговая карточка по учету доходов и налога на доходы физических лиц (форма 1-НДФЛ);

- справка о доходах физического лица в инспекцию Федеральной налоговой службы (форма 2-НДФЛ);

- индивидуальные сведения о страховом стаже и начисленных страховых взносах на обязательное пенсионное страхование застрахованного лица (форма СЗВ-4-2);

-реестр застрахованных лиц, за которых перечислены дополнительные страховые взносы на накопительную часть трудовой пенсии и уплачены взносы работодателя (форма ДСВ-3);

- индивидуальная карточка учета сумм начисленных выплат и иных вознаграждений, сумм начисленного единого социального налога, страховых вносов на пенсионное страхование (налогового вычета) (приложение 1 к приказу МНС РФ от 2-0-.2004 № САЭ-3-05/443);

- справка о заработной плате работников, выдаваемая для предъявления работником по месту требования.

4.2. К документам, содержащим персональные данные обучающихся, относятся:

- заявления о приёме в школу;

- личные дела учащихся;

- документы, удостоверяющие личность обучающегося (свидетельство о рождении или паспорт);

- документы о месте проживания;

- документы о составе семьи;

- паспортные данные родителей (законных представителей) обучающегося;

- документы о получении образования, необходимого для поступления в соответствующий класс (личное дело, справка с предыдущего места учебы и т.п.);

- полис медицинского страхования;

- документы о состоянии здоровья (сведения об инвалидности, о наличии хронических заболеваний, медицинское заключение об отсутствии противопоказаний для обучения в образовательном учреждении конкретного вида и типа, о возможности изучения предметов, представляющих повышенную опасность для здоровья и т.п.);

- документы, подтверждающие права на дополнительные гарантии и компенсации по определенным основаниям, предусмотренным законодательством (родители-инвалиды, неполная семья, ребенок-сирота и т.п.);

- иные документы, содержащие персональные данные (в том числе сведения, необходимые для предоставления обучающемуся гарантий и компенсаций, установленных действующим законодательством).

- копии документов, подтверждающих наличие у учащегося наград и поощрений .

4.3. Учитывая массовость документов, содержащих персональные данные работников, регламентированные места их обработки и хранения, соответствующая отметка о конфиденциальности на данных документах не ставится.

4.4. В случае необходимости передачи документов за пределы рабочих мест сотрудников, уполномоченных на обработку персональных данных, данные документы должны быть помещены в непрозрачную папку с надписью «ДСП».

5. Организация получения и обработки персональных данных

5.1. Получение персональных данных оператором осуществляется в соответствии с нормативно-правовыми актами РФ в области трудовых

отношений и образования, нормативными и распорядительными документами Минобрнауки России, настоящим Положением, локальными актами ОУ в случае согласия субъектов на обработку их персональных данных (приложение 1-2 к настоящему Положению).

5.2. Оператор персональных данных не вправе требовать от субъекта предоставления информации о его национальности и расовой принадлежности, политических и религиозных убеждениях и частной жизни.

5.3. Без согласия субъектов осуществляется обработка общедоступных персональных данных или данных, содержащих только фамилии, имена и отчества.

5.4. Обработка и использование персональных данных осуществляется в целях, указанных в соглашениях с субъектами, а также в случаях, предусмотренных нормативно-правовыми актами РФ и локальными нормативными актами, принятыми в рамках компетенции ОУ в соответствии с законодательством РФ.

5.5. В случае увольнения или отчисления субъекта оператор обязан незамедлительно прекратить обработку персональных данных и уничтожить соответствующие персональные данные в срок, не превышающий трех рабочих дней с даты достижения цели обработки персональных данных, если иное не предусмотрено законодательством РФ.

5.6. Правила обработки и использования персональных данных устанавливаются отдельными регламентами и инструкциями и утверждаются директором ОУ**.**

5.7. Все работники ОУ должны быть ознакомлены под роспись с настоящим Положением в редакции, действующей на момент ознакомления.

5.8. Персональные данные хранятся в бумажном и (или) электронном виде централизованно или в соответствующих структурных подразделениях ОУ с соблюдением предусмотренных нормативно-правовыми актами РФ мер по защите персональных данных.

5.9. Право на обработку персональных данных предоставляется работникам ОУ, определенным укрупненным перечнем персональных данных, используемых работниками структурных подразделений и (или) должностными лицами ОУ, а также распорядительными документами и иными письменными указаниями оператора.

5.10. Осуществлять обработку и хранение конфиденциальных данных, не внесенных в укрупненный перечень персональных данных, используемых работниками структурных подразделений и (или) должностными лицами ОУ, запрещается.

5.11. Работники структурных подразделений и (или) должностные лица ОУ, проводящие сбор персональных данных на основании укрупненного перечня, обязаны сохранять их конфиденциальность.

5.12. Персональные данные при их обработке обособляются от иной информации, в частности путем фиксации их на отдельных материальных (бумажном или электронном) носителях персональных данных (далее

материальные носители), в специальных разделах или на полях форм (бланков).

5.13. При фиксации персональных данных на материальных носителях не допускается размещение на одном материальном носителе персональных данных, цели обработки которых, заведомо не совместимы.

5.14. Для обработки различных категорий персональных данных, осуществляемой без использования средств автоматизации, используются отдельные материальные носители для каждой категории.

5.15. Лица, осуществляющие обработку персональных данных без использования средств автоматизации (в т. ч. работники ОУ или лица, осуществляющие такую обработку по договору с ОУ), информируются руководителями;

- о факте обработки ими персональных данных;
- о категориях обрабатываемых персональных данных;
- об особенностях и правилах осуществления такой обработки, установленных нормативными правовыми актами федеральных органов исполнительной власти, органов исполнительной власти субъектов РФ, а также локальными актами ОУ.

5.16. При использовании типовых форм документов, характер информации в которых предполагает или допускает включение в них персональных данных (далее - типовая форма), должны соблюдаться следующие условия:

- типовая форма документа содержит сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации: наименование ОУ: адрес ОУ; фамилию, имя, отчество и адрес субъекта персональных данных; источник получения персональных данных; сроки обработки персональных данных; перечень действий с персональными данными, которые будут совершаться в процессе их обработки; общее описание используемых ОУ способов обработки персональных данных;
- при необходимости получения письменного согласия на обработку персональных данных типовая форма предусматривает поле, в котором субъект персональных данных может поставить отметку о своем согласии на обработку персональных данных, осуществляемую без использования средств автоматизации;
- типовая форма составлена таким образом, чтобы каждый из субъектов персональных данных, содержащихся в документе, имел возможность ознакомиться со своими персональными данными, не нарушая прав и законных интересов иных проектов персональных данных.

5.17. При ведении журналов (классные журналы, журналы регистрации, журналы посещений и др.), содержащих персональные данные субъектов, следует учитывать, во-первых, что необходимость их ведения предусмотрена федеральными законами и локальными актами ОУ, содержащими сведения о цели обработки персональных данных, осуществляемой без использования средств автоматизации, способах фиксации и составе информации, запрашиваемой у субъектов персональных данных, перечне лиц (поименно

или по должностям), имеющих доступ к материальным носителям и ответственных за ведение и сохранность журналов, сроках обработки персональных данных, и, во-вторых, что копирование содержащейся в них информации не допускается.

5.18. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, производится способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, зачеркивание, стирание).

5.19. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

5.20. Если персональные данные субъекта можно получить исключительно у третьей стороны, то субъект должен быть уведомлен об этом заранее и от него необходимо получить письменное согласие. ОУ должно сообщить субъекту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа субъекта представить письменное согласие на их получение.

6. Использование персональных данных

6.1. Внутренний доступ (доступ внутри организации). Право доступа к персональным данным имеют:

- администрация школы;
- классные руководители (доступ к личным данным учащихся своего класса);
- руководство профессионального союза;
- технические специалисты, ведущие электронные версии баз данных; субъект персональных данных.

6.2. Другие сотрудники организации имеют доступ к персональным данным только с письменного согласия самого субъекта — носителя данных.

6.3. Внешний доступ. Потребителями персональных данных вне школы являются государственные и негосударственные функциональные структуры:

- налоговые инспекции;
- органы статистики;
- страховые агентства;
- военные комиссариаты;
- органы социального страхования;
- пенсионные фонды;
- подразделения муниципальных органов управления.

6.4. Контролирующие органы имеют доступ к информации только в сфере своей компетенции.

6.5. Организации, в которые сотрудник может осуществлять перечисления денежных средств (страховые компании, негосударственные пенсионные фонды, благотворительные организации, кредитные учреждения), могут получить доступ к персональным данным работника только в случае его письменного разрешения.

6.6. Иные организации могут получить сведения о работающем или уволенном сотруднике только на основании письменного запроса на бланке организации, с приложением копии нотариально заверенного заявления работника.

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

7. Меры по обеспечению безопасности персональных данных при их обработке

7.1. При обработке персональных данных в отношении каждой категории персональных данных определяются места хранения, а также устанавливается перечень лиц, осуществляющих их обработку либо имеющих к ним доступ (как с использованием средств автоматизации, так и без них).

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

7.3. Комплекс мер по защите персональных данных направлен на предупреждение нарушений доступности, целостности, достоверности и конфиденциальности персональных данных и обеспечивает безопасность информации в процессе у правленческой и производственной деятельности ОУ.

7.4. Порядок конкретных мероприятий по защите персональных данных с использованием или без использования ЭВМ определяется приказами директора ОУ и иными локальными нормативными актами.

8. Права, обязанности и ответственность субъекта персональных данных и оператора при обработке персональных данных

8.1. В целях обеспечения защиты своих персональных данных субъект персональных данных в соответствии с Законом № 152-ФЗ за исключением случаев, предусмотренных данным Федеральным законом, имеет право:

- на получение сведений об операторе, о месте его нахождения, наличии у него персональных данных, относящихся к нему (т. е, субъекту персональных данных), также на ознакомление с такими данными;

- требование от оператора уточнения своих персональных данных, их блокирования или уничтожения, в случае если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- получение при обращении или запросе информации, касающейся обработки персональных данных.

8.2. Оператор обязан:

- безвозмездно предоставлять субъекту персональных данных или его законному представителю возможность ознакомления с персональными данными, относящимися к соответствующему субъекту персональных данных;

- вносить в персональные данные субъекта необходимые изменения;

- уничтожать или блокировать соответствующие персональные данные при предоставлении субъектом персональных данных или его законным представителем сведений, подтверждающих, что персональные данные, которые относятся к соответствующему субъекту и обработку которых осуществляет оператор являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки;

- уведомлять субъекта персональных данных или его законного представителя и третьих лиц, которым персональные данные этого субъекта были переданы, о внесенных изменениях и предпринятых мерах;

- в случае выявления неправомерных действий с персональными данными субъекта устранять допущенные нарушения в срок, не превышающий трех рабочих дней с даты такого выявления;

- в случае невозможности устранения допущенных нарушений уничтожать персональные данные субъекта в срок, не превышающий трех рабочих дней с даты выявления неправомерности действий с персональными данными;

- уведомлять субъекта персональных данных или его законного представителя об устранении допущенных нарушений или об уничтожении персональных данных;

- в случае отзыва субъектом персональных данных согласия на обработку своих персональных данных прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий трех рабочих дней с даты поступления указанного отзыва, если иное не предусмотрено соглашением между оператором и субъектом персональных данных;

— уведомить субъекта персональных данных об уничтожении его персональных данных.

8.3. Оператор не вправе без письменного согласия (приложение 3 к настоящему Положению) субъекта персональных данных передавать обрабатываемые персональные данные третьим лицам, за исключением случаев, предусмотренных законодательством РФ.

8.4. Ответственность за соблюдение требований законодательства РФ при обработке и использовании персональных данных возлагается на руководителей структурных подразделений и конкретных должностных лиц, обрабатывающих персональные данные, в приказе об утверждении настоящего Положения и в других соответствующих приказах.

9. Ответственность за разглашение сведений, содержащих персональные данные, подлежащие защите, утрату документов, содержащих такую информацию, и нарушение порядка работы с ней

9.1. Разглашение сведений, содержащих персональные данные, подлежащие защите, или утрата носителей таких сведений влечет за собой последствия, установленные действующим законодательством Российской Федерации.

9.2. Ответственность за разглашение сведений, содержащих персональные данные, подлежащие защите, или утрату носителей таких сведений несут персонально должностные лица, имеющие доступ к этой информации и допустивший ее разглашение или утрату.

9.3. О фактах утраты должностным лицом носителей сведений, содержащих персональные данные, подлежащих защите, либо разглашения этих сведений ставится в известность его непосредственный руководитель, директором школы назначается комиссия для проведения служебной проверки обстоятельств утраты или разглашения. По результатам служебной проверки составляется акт.

9.4. По решению комиссии к виновным должностным лицам могут быть применены дисциплинарные взыскания в соответствии с Трудовым кодексом Российской Федерации.

9.5. При обнаружении в действиях лица, разгласившего сведения или утратившего носители информации, содержащей персональные данные, признаков административного правонарушения в адрес правоохранительных органов могут быть направлены материалы по результатам расследования комиссии для установления признаков административного правонарушения и привлечения виновного лица к ответственности в соответствии с действующим законодательством Российской Федерации.

10. Заключительные положения.

10.1. Изменения в Положение вносятся согласно установленному в ОУ порядку. Право ходатайствовать о внесении изменений в Положение имеет директор и заместители директора.

Приложение 1

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«Средняя общеобразовательная школа №10»

СОГЛАСИЕ
на обработку персональных данных работника
МАОУ «Средняя общеобразовательная школа №10»

Я,_____
(Ф.И.О.)
Дата рождения:_____
(число, месяц, год)
Паспорт:_____
_____
(серия, номер, когда и кем выдан)
в соответствии с Федеральным законом Российской Федерации от 26.07.2006 года №152-ФЗ «О персональных данных» даю письменное согласие на обработку моих персональных данных:

1. Фамилия, имя, отчество.
2. Дата и место рождения.
3. Паспортные данные (серия и номер, дата выдачи, выдавший орган и код подразделения).
4. Адрес регистрации по проживанию и по фактическому пребыванию (с указанием индекса и контактного телефона).
5. Состав семьи (фамилия, имя, отчество и дата рождения, членов семьи, степень родства).
6. Данные по образованию (дипломы и аттестаты – серия и номер, выдавший орган, дата выдачи, специальность и квалификация).
7. Автобиография.
8. Общий стаж работы, стаж работы в данной организации, научно-педагогический стаж, стаж работы в занимаемой должности и др.
9. Данные по владению иностранным языком (степень его владения).
10. Сведения о воинском учете.
11. Сведения о предыдущих местах работы.
12. Должность, подразделение, табельных номер, оклад, доплаты и надбавки.
13. Сведения о доходах, налогах и социальных льготах.
14. Адрес электронной почты (в Школе) и идентификатор для доступа в компьютерную сеть Школы.
15. Сведения о ИНН, страховом свидетельстве государственного пенсионного страхования и медицинском страховании.
16. Наличие судимости.
17. Содержание трудового договора и дополнений к нему (в том числе срочного).
18. Подлинники и копии приказов по личному составу.
19. Основания к приказам по личному составу.
20. Личные дела и трудовые книжки.
21. Материалы по повышению квалификации и переподготовке сотрудников, их аттестации, поощрениях и наложенных дисциплинарных взысканиях.
22. Результаты медицинского обследования.
23. Фотографии для личного дела, удостоверения сотрудника и снимки общественных мероприятий.
24. Рекомендации характеристики.
25. Администрирование и контроль трафика Интернета.

26. Результаты посещения школьной библиотеки.

Целью обработки персональных данных является обеспечение исполнения трудовых отношений между работником и МАОУ «Средняя общеобразовательная школа №10», подготовки отчетности в соответствии с действующим законодательством.

Обработка персональных данных осуществляется как на бумажных носителях, так и с использованием средств автоматизации.

Срок действия согласия на обработку персональных данных: с момента заключения трудовых отношений, и в течение года, следующего за годом расторжения трудовых отношений.

Оператор, осуществляющий обработку персональных данных, - муниципальное автономное общеобразовательное учреждение «Средняя общеобразовательная школа № 10».

Я ознакомлен с «Положением о порядке обработки и защите персональных данных работников и обучающихся МАОУ «Средняя общеобразовательная школа № 10», Перечнем сведений конфиденциального характера в МАОУ «Средняя общеобразовательная школа № 10, Инструкцией о порядке обеспечения конфиденциальности при обработке информации, содержащей персональные данные в МАОУ «Средняя общеобразовательная школа № 10», Инструкцией пользователя при обработке конфиденциальной информации на вычислительной техники МАОУ «Средняя общеобразовательная школа № 10»

Дата заполнения: «___»_____ 20____ г. Личная подпись_____

Приложение 2

Директору МАОУ «Средняя
общеобразовательная школа №10»
Верясов В.Н.

ЗАЯВЛЕНИЕ – СОГЛАСИЕ
на обработку персональных данных обучающегося

В соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», я,_____
Ф.И.О. родителя (законного представителя)

паспорт_____выдан_____
_____
дата выдачи «_____»_____

являясь законным представителем, даю согласие на обработку своих персональных данных и персональных данных моего ребенка

_____
(Ф.И.О.)

муниципальному общеобразовательному учреждению «Средняя общеобразовательная школа № 10» г.о. Саранск в целях уставной деятельности МАОУ «Средняя общеобразовательная школа № 10» г.о. Саранск, в том числе для:

— заключения договоров об оказании образовательных услуг;

— ведения классного журнала и дневников обучающихся в электронном и бумажном виде, личных дел обучающихся, другой учетной документации;

— оформления и выдачи справок, характеристик, документов об образовании и т.п.;

— обеспечения питанием, медицинского сопровождения, организации отдыха и оздоровления;

— оформления участия в олимпиадах, конкурсах, соревнованиях и т.п., учета занятости обучающихся во внеурочное время, ведения портфолио обучающихся в составе: ФИО, пол, класс обучения, дата и место рождения, адрес регистрации и проживания, данные паспорта или свидетельства о рождении, СНИЛС, ИНН, гражданство, родной язык, сведения о составе семьи, сведения об успеваемости, сведения о результативности участия в олимпиадах, конкурсах, смотрах, соревнованиях и т.п., сведения о дополнительном образовании, сведения о состоянии здоровья, номера полисов медицинского страхования, фотографии, контактные телефоны, электронная почта, ФИО родителей (законных представителей), дата рождения родителей (законных представителей), паспортные данные (законных представителей) (данные документа, удостоверяющего личность), контактные телефоны автоматизированным способом и без использования средств автоматизации, включая действия по сбору, записи, систематизации, накоплению, хранению, уточнению (обновлению, изменению), извлечению, использованию, передаче (распространению, предоставлению, доступа), обезличиванию, блокированию, удалению, уничтожению персональных данных на срок с даты подписания до окончания обучения в МАОУ «Средняя общеобразовательная школа № 10» г.о. Саранск.

Настоящее согласие может быть отозвано мной путем предоставления в МАОУ «Средняя общеобразовательная школа № 10» г.о. Саранск заявления в простой письменной форме в соответствии с требованиями законодательства РФ.

Дата «____»_____ 20____ года Подпись _____/_____/

Согласен «____»_____20_____г. _____
(подпись) (ФИО обучающегося с 14 лет)

Приложение 3

Директору МАОУ «Средняя
общеобразовательная школа №10»
Верясову В.Н.

Заявление-согласие субъекта на передачу его персональных данных третьей стороне

Я,_____
Ф.И.О.

паспорт_____выдан_____
_____
дата выдачи «_____»_____

в соответствии со ст. 88 Трудового кодекса Российской Федерации, Федеральным законом от 27.07.2006 № 152-ФЗ "0 персональных данных_____
(согласен/несогласен)
на передачу моих персональных данных, а именно:_____
_____
(состав персональных данных: Ф.И,О., паспортные данные и т. д.)
третьей стороне - _____
(Ф.И.О. физического лица или наименование организации, которым сообщаются данные)
для обработки в целях _____
(указать цели обработки)

Дата заполнения: «___»_____ 20____ г. Личная подпись_____

Приложение 4

Директору
МАОУ «Средняя школа №10»
Юридический адрес: РМ, г.о. Саранск,
ул. Солнечная д. 27
В.Н.Верясову

ОБЯЗАТЕЛЬСТВО
о неразглашении персональных данных

Я, _____,
(фамилия, имя, отчество)
в качестве сотрудника Муниципального автономного общеобразовательного учреждения «Средняя общеобразовательная школа №10» г.о.Саранск в период трудовых (служебных) отношений с данным образовательным учреждением (его правопреемником) обязуюсь:

1. Не разглашать персональные данные субъектов персональных данных, которые мне будут доверены или станут известны по работе (службе).
2. Не передавать третьим лицам и не раскрывать публично персональные данные без письменного согласия субъекта персональных данных, за исключением случаев, когда это требуется в целях предупреждения угрозы жизни и здоровью субъекта персональных данных, а также в других случаях, предусмотренных федеральными законами.
3. Не сообщать персональные данные субъекта персональных данных в коммерческих целях без его письменного согласия.
4. Об утрате или недостаче носителей персональных данных субъектов персональных данных, ключей от помещений, сейфов (металлических шкафов), личных печатей и о других фактах, которые могут привести к разглашению персональных данных субъектов персональных данных, а также о причинах и условиях возможной утечки сведений немедленно сообщать директору школы.
5. До моего сведения доведены соответствующие положения по обеспечению сохранности персональных данных субъектов персональных данных. Мне известно, что нарушение этих положений может повлечь уголовную, административную, гражданско - правовую или иную ответственность в соответствии с законодательством РФ.

_____
(подпись)
«_____» _____20___ г.

С ПОЛОЖЕНИЕМ о порядке обработки и защите персональных данных работников и обучающихся МАОУ «Средняя общеобразовательная школа №10» ознакомлены:

№ п/п	Ф.И.О.	Должность	Подпись
1	**2**	**3**	**4**
1.	Верясов В.Н.	Директор школы, учитель-предметник	
2.	Безрукова Н.И.	Заместитель директора по ВР, учитель-предметник	
3.	Ивойлова Е.Е.	Заместитель директора по УВР, учитель-предметник	
4.	Ильин А.А.	Заместитель директора по АХЧ	
5.	Емелина Т.Б.	Воспитатель ГПД	
6.	Крылова А.С.	Педагог-психолог	
7.	Оларь К.А.	Учитель-логопед	
8.	Кеняйкина Л.В.	Педагог-организатор	
9.	Цветкова А.С.	Заведующая библиотекой	
10.	Смагина М.А.	Главный бухгалтер	
11.	Карпунькина И.Н.	Бухгалтер	
12.	Кисняшкина О.С.	Секретарь	
13.	Бочкарева Л.Ф.	Классный руководитель, учитель начальных классов	
14.	Марьина Л.В.	Классный руководитель, учитель начальных классов	
15.	Варганова А.А.	Классный руководитель, учитель начальных классов	
16.	Балмаева С.А.	Классный руководитель, учитель начальных классов	
17.	Цыганова Е.А.	Классный руководитель, учитель начальных классов	
18.	Трунькина Т.А.	Классный руководитель, учитель начальных классов	
19.	Маврушкина О.Е.	Классный руководитель, учитель начальных классов	
20.	Тивикова Т.И.	Классный руководитель, учитель начальных классов	
21.	Радайкина О.П.	Классный руководитель, учитель-предметник	
22.	Максимкин А.Э.	Классный руководитель, учитель-предметник	
23.	Чумакова В.В.	Классный руководитель, учитель-предметник	
24.	Захарова С.С.	Классный руководитель, учитель-предметник	
25.	Юртаева О.Ю.	Классный руководитель, учитель-предметник	
26.	Трофимова А.В.	Классный руководитель, учитель-предметник	
27.	Сергеев А.В.	Классный руководитель, учитель-предметник	
1	**2**	**3**	**4**
28.	Прошкина Т.И	Учитель-предметник	
29.	Шурыгин Д.С.	Учитель-предметник	
30.	Рогачев А.И.	Учитель-предметник	
31.	Ибрагимова Нигара Видади кызы	Учитель-предметник	
32.	Мартиросян Л.С.	Учитель-предметник	
33.	Рыжова Ю.Н.	Учитель-дефектолог	
34.	Звездина Е.А.	Социальный педагог	
35.	Попова В.В.	Учитель-предметник	

Приложение 2
к приказу № 41
от 01.09.2018г

УТВЕРЖДАЮ
Директор
МАОУ «Средняя школа № 10»
_____ В.Н.Верясов

Перечень сведений конфиденциального характера в МАОУ «Средняя общеобразовательная школа № 10»

В настоящем Перечне предусматриваются категории сведений, представляющих конфиденциальную информацию (персональные данные) в МАОУ «Средняя общеобразовательная школа № 10», разглашение которых может нанести материальный, моральный или иной ущерб интересам данного учреждения, его работникам и обучающимся.

№ п/п	Перечень сведений	Срок действия
1	**Финансы**	
1.1	Сведения о бухгалтерском учете (за исключением годового баланса).	3 года
1.2	Сведения о финансовых операциях.	3 года
1.3	Сведения о величине доходов и расходов, о состоянии дебиторской и кредиторской задолженностях (за исключением годового баланса).	3 года
1.4	Сведения, содержащиеся в финансово - договорных схемах Учреждения.	+ 1 год после окончания действия договора
2	**Личная безопасность сотрудников**	
2.1	Персональные данные, сведения о фактах, событиях и обстоятельствах частной жизни сотрудника.	постоянно
2.2	Сведения об используемой в коллективе системе стимулов, укрепляющих дисциплину, повышающих производительность труда.	на период действия
2.3	Информация о личных отношениях специалистов, как между собой, так и с руководством, сведения о возможных противоречиях, конфликтах внутри коллектива.	3 года
3	**Персональные данные об обучающихся**	
3.1	Персональные данные обучающегося.	постоянно
3.2	Персональные данные родителей (законных представителей).	постоянно
3.3	Сведения, необходимые для предоставления обучающемуся гарантий и компенсаций, установленных действующим законодательством.	постоянно
4	**Персональные данные о детях, оставшихся без попечения родителей**	
4.1	Персональные данные детей, оставшихся без попечения родителей.	постоянно
4.2	Персональные данные кандидатов в усыновители, приемные родители, опекуны.	постоянно
5	**Безопасность**	
5.1	Сведения о порядке и состоянии защиты конфиденциальной информации.	постоянно
5.2	Сведения о защищаемых информационных ресурсах в локальных сетях Учреждения.	постоянно
5.2	Сведения об охране организации, пропускном и внутриобъектовом режиме, системе сигнализации, о наличии средств контроля и управления доступом.	постоянно

Приложение 3
к приказу №
от 01.09.2018г

Список
сотрудников МАОУ «Средняя общеобразовательная школа №10»,
допущенных к обработке персональных данных

№ п/п	Ф.И.О.	Должность	Подпись
1	**2**	**3**	**4**
1.	Верясов В.Н.	Директор школы, учитель-предметник	
2.	Безрукова Н.И.	Заместитель директора по ВР, учитель-предметник	
3.	Ивойлова Е.Е.	Заместитель директора по УВР, учитель-предметник	
4.	Ильин А.А.	Заместитель директора по АХЧ	
5.	Емелина Т.Б.	Воспитатель ГПД	
6.	Крылова А.С.	Педагог-психолог	
7.	Оларь К.А.	Учитель-логопед	
8.	Кеняйкина Л.В.	Педагог-организатор	
9.	Цветкова А.С.	Заведующая библиотекой	
10.	Смагина М.А.	Главный бухгалтер	
11.	Карпунькина И.Н.	Бухгалтер	
12.	Кисняшкина О.С.	Секретарь	
13.	Бочкарева Л.Ф.	Классный руководитель, учитель начальных классов	
14.	Марьина Л.В.	Классный руководитель, учитель начальных классов	
15.	Варганова А.А.	Классный руководитель, учитель начальных классов	
16.	Балмаева С.А.	Классный руководитель, учитель начальных классов	
17.	Цыганова Е.А.	Классный руководитель, учитель начальных классов	
18.	Трунькина Т.А.	Классный руководитель, учитель начальных классов	
19.	Маврушкина О.Е.	Классный руководитель, учитель начальных классов	
20.	Тивикова Т.И.	Классный руководитель, учитель начальных классов	
21.	Радайкина О.П.	Классный руководитель, учитель-предметник	
22.	Максимкин А.Э.	Классный руководитель, учитель-предметник	
23.	Чумакова В.В.	Классный руководитель, учитель-предметник	
24.	Захарова С.С.	Классный руководитель, учитель-предметник	
25.	Юртаева О.Ю.	Классный руководитель, учитель-предметник	
26.	Трофимова А.В.	Классный руководитель, учитель-предметник	
27.	Сергеев А.В.	Классный руководитель, учитель-предметник	
1	**2**	**3**	**4**
28.	Прошкина Т.И	Учитель-предметник	
29.	Шурыгин Д.С.	Учитель-предметник	
30.	Рогачев А.И.	Учитель-предметник	
31.	Ибрагимова Нигара Видади кызы	Учитель-предметник	
32.	Мартиросян Л.С.	Учитель-предметник	
33.	Рыжова Ю.Н.	Учитель-дефектолог	
34.	Звездина Е.А.	Социальный педагог	
35.	Попова В.В.	Учитель-предметник	

Приложение 4
к приказу № 41
от 01.09.2018г.

УТВЕРЖДАЮ
Директор
МАОУ «Средняя школа №10»
_____ В.Н.Верясов

Перечень
мест хранения материальных носителей персональных данных

Категория персональных данных	Место хранения	Ответственное за хранение лицо
Бумажные носители персональных данных работников, учащихся и их родителей (законных представителей).	Канцелярия	Кисняшкина О.С., секретарь
Электронные носители персональных данных работников, учащихся и их родителей (законных представителей).	Жесткий диск	
Бумажные носители персональных данных работников.	Бухгалтерия	Смагина М.А. главный бухгалтер
Электронные носители персональных данных работников.	Жесткий диск	
Бумажные носители персональных данных учащихся и их родителей (законных представителей).	Кабинеты заместителей директора	Ивойлова Е.Е.., заместитель директор по УВР, Безрукова Н.И., заместитель директор по ВР
Электронные носители персональных данных учащихся и их родителей (законных представителей).	Жесткий диск	

Приложение 5
к приказу № 41
от 01.09.2018г

УТВЕРЖДАЮ
Директор
МАОУ «Средняя школа №10»
_____ В.Н.Верясов

Иструкция о порядке обеспечения конфиденциальности при обработке информации, содержащей персональные данные в МАОУ «Средняя общеобразовательная школа №10»

1. Общие положения

1.1. Настоящая Инструкция устанавливает применяемые в МАОУ «Средняя общеобразовательная школа №10» способы обеспечения безопасности при обработке, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, защиту, распространение (в том числе передачу), обезличивание, блокирование, уничтожение, персональных данных с целью соблюдения конфиденциальности сведений, содержащих персональные данные работников и обучающихся МАОУ «Средняя общеобразовательная школа №10» (далее - Учреждение).

1.2. Настоящая Инструкция разработана на основании Конституции Российской Федерации, Трудового кодекса Российской Федерации, Федерального закона от 19.12.2005 г. №160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных», Федерального закона РФ от 27.07.2006 № 152-ФЗ «О персональных данных», постановлений Правительства Российской Федерации от 17 ноября 2007 г. № 781 "Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных" и от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации" и иных нормативных правовых актов Российской Федерации, а также Положения о порядке обработки и защите персональных данных работников и обучающихся МАОУ «Средняя общеобразовательная школа №10».

1.3. В соответствии с законодательством РФ под персональными данными понимается любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация, необходимая Учреждению в связи с трудовыми отношениями и организацией образовательного процесса.

1.4. Требование обеспечения конфиденциальности при обработке персональных данных означает обязательное для соблюдения должностными лицами Учреждения, допущенными к обработке персональных данных, иными получившими доступ к персональным данным лицами требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

1.5. Обеспечение конфиденциальности персональных данных не требуется в случае:

- обезличивания персональных данных;
- для общедоступных персональных данных.

1.6. Перечни персональных данных и ответственных за хранение и обработку персональных данных утверждается приказом директора Учреждения. Обработка и хранение конфиденциальных данных лицами, не указанными в приказе, запрещается.

1.7. В целях обеспечения требований соблюдения конфиденциальности и безопасности при обработке персональных данных Учреждение предоставляет должностным лицам, работающим с персональными данными, необходимые условия для выполнения указанных требований:

- знакомит работника под роспись с требованиями Положения о порядке обработки и защите персональных данных работников и обучающихся;
- работников и обучающихся Учреждения, с настоящей Инструкцией, с должностной инструкцией и иными локальными нормативными актами Учреждения в сфере обеспечения конфиденциальности и безопасности персональных данных;
- предоставляет хранилища для документов, средства для доступа к информационным ресурсам (ключи, пароли и т.п.);
- обучает правилам эксплуатации средств защиты информации;
- проводит иные необходимые мероприятия.

1.8. Должностным лицам Учреждения, работающим с персональными данными, запрещается сообщать их устно или письменно кому бы то ни было, если это не вызвано служебной необходимостью. После подготовки и передачи документа файлы черновиков и вариантов документа переносятся подготовившим их сотрудником на маркированные носители, предназначенные для хранения персональных данных.

Без согласования с руководителем структурного подразделения формирование и хранение баз данных (картотек, файловых архивов и др.), содержащих конфиденциальные данные, запрещается.

1.9. Должностные лица Учреждения, работающие с персональными данными, обязаны использовать информацию о персональных данных исключительно для целей, связанных с выполнением своих трудовых обязанностей.

1.10. При прекращении выполнения трудовой функции, связанной с обработкой персональных данных, все носители информации, содержащие персональные данные (оригиналы и копии документов, машинные и бумажные носители и пр.), которые находились в распоряжении должностного

лица в связи с выполнением должностных обязанностей, данный работник должен передать своему непосредственному руководителю.

1.11. Передача персональных данных третьим лицам допускается только в случаях, установленных законодательством РФ, в соответствии с Положения о порядке обработки и защите персональных данных работников и обучающихся МАОУ «Средняя общеобразовательная школа №10», работников и обучающихся МАОУ «Средняя общеобразовательная школа №10» с настоящей Инструкцией, должностными инструкциями и иными локальными нормативными актами Учреждения. Передача персональных данных осуществляется ответственным за обработку персональных данных должностным лицом Учреждения на основании письменного или устного поручения руководителя структурного подразделения.

1.12. Передача сведений и документов, содержащих персональные данные, оформляется путем составления акта по установленной настоящей Инструкцией форме (Приложение № 1).

1.13. Должностное лицо, предоставившее персональные данные третьим лицам, направляет письменное уведомление субъекту персональных данных о факте передачи его данных третьим лицам.

1.14. Запрещается передача персональных данных по телефону, факсу, электронной почте за исключением случаев, установленных законодательством и действующими в Учреждении локальными нормативными актами.

Ответы на запросы граждан и организаций даются в том объеме, который позволяет не разглашать в ответах персональные данные, за исключением данных, содержащихся в материалах заявителя или опубликованных в общедоступных источниках.

1.15. Должностные лица Учреждения, работающие с персональными данными, обязаны немедленно сообщать своему непосредственному руководителю и (или) директору Учреждения по безопасности обо всех ставших им известными фактах получения третьими лицами несанкционированного доступа либо попытки получения доступа к персональным данным, об утрате или недостаче носителей информации, содержащих персональные данные, удостоверений, пропусков, ключей от сейфов (хранилищ), личных печатей, электронных ключей и других фактах, которые могут привести к несанкционированному доступу к персональным данным, а также о причинахи условиях возможной утечки этих сведений.

1.16. Должностные лица, осуществляющие обработку персональных данных, за невыполнение требований конфиденциальности, защиты персональных данных несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством РФ.

1.17. Отсутствие контроля со стороны Учреждения за надлежащим исполнением работником своих обязанностей в области обеспечения конфиденциальности и безопасности персональных данных не освобождает работника от таких обязанностей и предусмотренной законодательством РФ ответственности.

2. Порядок обеспечения безопасности при обработке персональных данных, осуществляемой без использования средств автоматизации

2.1. Обработка персональных данных, в том числе содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такая обработка осуществляется при непосредственном участии человека.

2.2. Руководитель структурного подразделения, осуществляющего обработку персональных данных без использования средств автоматизации:

- определяет места хранения персональных данных (материальных носителей);

- осуществляет контроль наличия в структурном подразделении условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный к ним доступ;

- информирует лиц, осуществляющих обработку персональных данных без использования средств автоматизации, о перечне обрабатываемых персональных данных, а также об особенностях и правилах осуществления такой обработки;

- организует раздельное, т.е. не допускающее смешение, хранение материальных носителей персональных данных (документов, дисков, дискет, USB флеш-накопителей, пр.), обработка которых осуществляется в различных целях.

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

2.4. При несовместимости целей обработки персональных данных, зафиксированных на одном материальном носителе, если материальный носитель не позволяет осуществлять обработку персональных данных отдельно от других зафиксированных на том же носителе персональных данных, руководитель структурного подразделения должен обеспечить раздельную обработку персональных данных, исключающую одновременное копирование иных персональных данных, не подлежащих распространению и использованию.

2.5. Уничтожение или обезличивание части персональных данных, если это допускается материальным носителем, должно производиться способом, исключающим дальнейшую обработку этих персональных данных с сохранением возможности обработки иных данных, зафиксированных на материальном носителе (удаление, вымарывание).

2.6. Уточнение персональных данных при осуществлении их обработки без использования средств автоматизации производится путем обновления или изменения данных на материальном носителе, а если это не допускается техническими особенностями материального носителя, - путем фиксации на

том же материальном носителе сведений о вносимых в них изменениях либо путем изготовления нового материального носителя с уточненными персональными данными.

3. Порядок обеспечения безопасности при обработке персональных данных, осуществляемой с использованием средств автоматизации

3.1. Обработка персональных данных с использованием средств автоматизации означает совершение действий (операций) с такими данными с помощью объектов вычислительной техники в локально-вычислительное сети Учреждения (далее - ЛВС).

Безопасность персональных данных при их обработке в ЛВС обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации, а также используемые в ЛВС информационные технологии.

Технические и программные средства защиты информации должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации. Средства защиты информации, применяемые в ЛВС, в установленном порядке проходят процедуру оценки соответствия.

3.2. Допуск лиц к обработке персональных данных с использованием средств автоматизации осуществляется на основании приказа директора Учреждения при наличии ключей (паролей) доступа.

Работа с персональными данными, содержащимися в ЛВС, осуществляется в соответствии с «Положением о локально-вычислительной сети МАОУ «Средняя общеобразовательная школа №10», «Инструкцией пользователя при работе в локально-вычислительной сети МАОУ «Средняя общеобразовательная школа №10», «Инструкцией пользователя при обработке конфиденциальной информации на объектах вычислительной техники МАОУ «Средняя общеобразовательная школа №10»», с которыми работник, в должностные обязанности которого входит обработка персональных данных, знакомится под роспись.

3.3. Работа с персональными данными в ЛВС должна быть организована таким образом, чтобы обеспечивалась сохранность носителей персональных данных и средств защиты информации, а также исключалась возможность неконтролируемого пребывания в этих помещениях посторонних лиц.

3.4. Компьютеры и (или) электронные папки, в которых содержатся файлы с персональными данными, для каждого пользователя должны быть защищены индивидуальными паролями доступа, состоящими из 6 и более символов. Работа на компьютерах с персональными данными без паролей доступа, или под чужими или общими (одинаковыми) паролями, запрещается.

3.5. Пересылка персональных данных без использования специальных средств защиты по общедоступным сетям связи, в том числе Интернет, запрещается.

3.6. При обработке персональных данных в ЛВС пользователями должно быть обеспечено:

а) использование предназначенных для этого разделов (каталогов) носителей информации, встроенных в технические средства, или съемных маркированных носителей;

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

в) постоянное использование антивирусного обеспечения для обнаружения зараженных файлов и незамедлительное восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

г) недопущение несанкционированных выноса из помещений, установки, подключения оборудования, а также удаления, инсталляции или настройки программного обеспечения.

3.7. При обработке персональных данных в ЛВС разработчиками и администраторами систем должны обеспечиваться:

а) обучение лиц, использующих средства защиты информации, применяемые в ЛВС, правилам работы с ними;

б) учет лиц, допущенных к работе с персональными данными в ЛВС, прав и паролей доступа;

в) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним;

г) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;

д) описание системы защиты персональных данных.

3.8. Специфические требования по защите персональных данных в отдельных автоматизированных системах Учреждения определяются утвержденными в установленном порядке инструкциями по их использованию и эксплуатации.

4. Порядок учета, хранения и обращения со съемными носителями персональных данных, твердыми копиями и их утилизации

4.1. Все находящиеся на хранении и в обращении в Учреждении съемные носители (диски, дискеты, USB флеш-накопители, пр.), содержащие персональные данные, подлежат учёту. Каждый съемный носитель с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный учетный номер.

4.2. Учет и выдачу съемных носителей персональных данных осуществляют работники структурных подразделений, указанные в приказе директора Учреждения.

Работники Учреждения получают учтенный съемный носитель от уполномоченного сотрудника для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале персонального учета съемных носителей персональных данных (далее - журнал учета), который ведется в каждом структурном подразделении Учреждения, осуществляющем работу со съемными носителями персональных данных (Приложение № 2).

По окончании работ пользователь сдает съемный носитель для хранения уполномоченному сотруднику, о чем делается соответствующая запись в журнале учета.

4.3. При работе со съемными носителями, содержащими персональные данные, запрещается:

- хранить съемные носители с персональными данными вместе с носителями открытой информации, на рабочих столах, либо оставлять их без присмотра или передавать на хранение другим лицам;

- выносить съемные носители с персональными данными из служебных помещений для работы с ними на дому, в гостиницах и т. д.

4.4. При отправке или передаче персональных данных адресатам на съемные носители записываются только предназначенные адресатам данные.

Отправка персональных данных адресатам на съемных носителях осуществляется в порядке, установленном для документов для служебного пользования. Вынос съемных носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя структурного подразделения Учреждения.

4.5. О фактах утраты съемных носителей, содержащих персональные данные, либо разглашения содержащихся в них сведений должно быть немедленно сообщено руководителю соответствующего структурного подразделения Учреждения и (или) заместителю директора по УВР. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета.

4.6. Съемные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению. Уничтожение съемных носителей с конфиденциальной информацией осуществляется комиссией, созданной приказом директора Учреждения. По результатам уничтожения носителей составляется акт по прилагаемой форме (Приложение № 3).

5. Заключительные положения

5.1. С положениями настоящей Инструкции должны быть ознакомлены под роспись все работники структурных подразделений Учреждения и лица, выполняющие работы по договорам и контрактам, имеющие отношение к обработке персональных данных работников, обучающихся Учреждения и третьих лиц.

Приложение 1

УТВЕРЖДАЮ

_____

руководитель структурного подразделения

«___»_____20___г.

АКТ

передачи персональных данных

_____

(должность, Ф.И.О.)

передал(а) следующие документы, содержащие персональные данные _____:

(Ф.И.О. работника, обучающегося)

_____

(перечислить наименования передаваемых документов, содержащих персональные данные)

по запросу _____

(Ф.И.О., должность)

с целью _____

_____ _____

(подпись) (расшифровка подписи)

Документы, содержащие персональные данные принял(а), экземпляр акта получил(а)

_____ _____

(подпись) (расшифровка подписи)

«___»_____20__г.

Приложение 2

ЖУРНАЛ
учета съемных носителей персональных данных

_____
наименование структурного подразделения

Начат «___»_____20__г. на _____ листах
Окончен «___»_____20__г.

_____ _____
Должность и ФИО ответственного за хранение Подпись

№ п/п	Метка съемного носителя (учетный номер)	Фамилия пользователя	(Получил, вернул)	Подпись ответственного за хранение съемного носителя	Примечание*

* Причина и основание окончания использования (№ и дата отправки адресату или распоряжения о передаче, № и дата акта утраты, неисправность, заполнение подлежащими хранению данными)

Приложение 3

УТВЕРЖДАЮ
_____
___»_____20___г.

АКТ
уничтожения съемных носителей персональных данных

Комиссия, наделенная полномочиями приказом директора МАОУ «Средняя общеобразовательная школа №10» от «___»_____20__г. №_____ в составе:

_____
(должности, Ф.И.О.)

провела отбор съемных носителей персональных данных, не подлежащих дальнейшему хранению:

№ п/п	Дата	Учетный номер съемного носителя	Пояснения
1	2	3	4

Всего съемных носителей _____
(цифрами и прописью)

На съемных носителях уничтожена конфиденциальная информация путем стирания ее на устройстве гарантированного уничтожения информации (механического уничтожения, сжигания и т.п.).

Перечисленные съемные носители уничтожены

_____
путем (разрезания, демонтажа и т.п.),

_____
измельчены и сданы для уничтожения по утилизации вторичного сырья.

Председатель комиссии _____ _____
(подпись) (дата)

Члены комиссии _____ _____
(подпись) (дата)

(Ф.И.О.)

Приложение 6
к приказу № 41
от 01.09.2018г

УТВЕРЖДАЮ
Директор
МАОУ «Средняя школа №10»
_____В.Н.Верясов

Инструкция пользователя при обработке конфиденциальной информации на вычислительной техники МАОУ «Средняя общеобразовательная школа №10»»

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Настоящая Инструкция регламентирует основные права, обязанности и ответственность должностного лица, осуществляющего обработку охраняемой законом информации (персональных данных и иной конфиденциальной информации) на объектах вычислительной техники (далее - пользователь) МАОУ «Средняя общеобразовательная школа №10» (далее - Учреждение).

1.2 Обработка конфиденциальной информации на объектах вычислительной техники (далее-ОВТ) осуществляется пользователем, допущенным к такой обработке приказом директора Учреждения и обладающим навыками работы на ОВТ.

1.3 Пользователь при обработке охраняемой законом информации на ОВТ обеспечивает конфиденциальность обрабатываемой на ОВТ информации в соответствии с «Инструкцией о порядке обеспечения конфиденциальности при обработке информации, содержащей персональные данные в МАОУ «Средняя общеобразовательная школа №10», иными локальными нормативными актами Учреждения и несет персональную ответственность за несоблюдение требований законодательства РФ, локальных нормативных актов, определяющих порядок обработки данной информации.

2 ПОЛЬЗОВАТЕЛЬ ОБЯЗАН:

2.1 выполнять требования «Инструкции пользователя при работе в локально-вычислительной сети Учреждения»;

2.2 при работе с конфиденциальной информацией не допускать присутствия в помещении, где расположены средства вычислительной техники, не допущенных к обрабатываемой информации лиц или располагать во время работы экран монитора так, чтобы исключалась возможность просмотра посторонними лицами отображаемой на нем информации;

2.3 соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам,

программам, данным, файлам с конфиденциальной информацией при ее обработке;

2.4 после окончания обработки конфиденциальной информации в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ОВТ, а файлы, необходимые в дальнейшем, хранить только в специально предназначенной для этого папке на отведённом сервере; данная папка подключена в виде сетевого диска с определенным названием («меткой») (в отношении персональных данных это - ПДн, а в отношении конфиденциальной информации, не содержащей персональные данные - Дн); назначение доступа к папке персональных данных осуществляется лишь должностными лицами Учреждения, обрабатывающими персональные данные, в соответствии с приказом директора о назначении ответственных лиц по работе с персональными данными;

2.5 оповещать обслуживающий ОВТ персонал, а также своего непосредственного руководителя о всех фактах или попытках несанкционированного доступа к конфиденциальной информации, обрабатываемой на ОВТ;

2.6 знать способы выявления нештатного поведения используемых операционных систем и пользовательских приложений, последовательность дальнейших действий в случае выявления нештатного поведения;

2.7 знать штатные режимы работы программного обеспечения, пути проникновения и распространения компьютерных вирусов;

2.8 знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий;

2.9 помнить личные пароли, персональные идентификаторы, не оставлять без присмотра записи, содержащие личные пароли, хранить их в запирающемся ящике стола или сейфе;

2.10 при применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов.

3 ПОЛЬЗОВАТЕЛЮ ЗАПРЕЩАЕТСЯ:

3.1 записывать и хранить конфиденциальную информацию на локальном компьютере;

3.2 записывать и хранить конфиденциальную информацию на неучтенных в установленном в Учреждении порядке съемных носителях информации;

3.3 удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

3.4 самостоятельно подключать к ОВТ какие-либо устройства и вносить изменения в состав, конфигурацию, размещение ОВТ;

3.5 самостоятельно устанавливать и/или запускать (выполнять) на ОВТ любые системные или прикладные программы, загружаемые по сети Интернет или с внешних носителей;

3.6 осуществлять обработку конфиденциальной информации в условиях, позволяющих осуществлять их просмотр лицами, не имеющими к ним допуска;

3.7 сообщать кому-либо устно или письменно личные атрибуты доступа к ресурсам ОВТ;

3.8 отключать (блокировать) средства защиты информации;

3.9 производить какие-либо изменения в подключении и размещении технических средств;

3.10 производить иные действия, ограничения, на выполнение которых предусмотрены действующими в Учреждении локальными нормативными актами;

3.11 оставлять бесконтрольно ОВТ с загруженными персональными данными, иной конфиденциальной информацией, с установленными маркированными носителями, электронными ключами, а также с распечатываемыми документами на бумажных носителях, содержащих персональные данные или иную конфиденциальную информацию.

4 ПОЛЬЗОВАТЕЛЬ ИМЕЕТ ПРАВО:

4.1 обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать и пр.) информацию, содержащую персональные данные и иную конфиденциальную информацию, в пределах, определенных должностными полномочиями данного пользователя;

4.2 обращаться к обслуживающему ОВТ персоналу с просьбой об оказании технической и методической помощи при работе с общесистемным и прикладным программным обеспечением, установленным на ОВТ, а также со средствами защиты информации.

5 ОТВЕТСТВЕННОСТЬ ПОЛЬЗОВАТЕЛЯ:

5.1 Пользователь несет ответственность в соответствии с законодательством РФ за:

- неисполнение и ненадлежащее выполнение требований настоящей Инструкции;

- несоблюдение требований инструкций и иных локальных нормативных актов, определяющих порядок обработки конфиденциальной информации на ОВТ и использования информационных ресурсов Учреждения.

Приложение 7
к приказу № 41
от 01.09.2018г

УТВЕРЖДАЮ
Директор
МАОУ «Средняя школа №10»
_____В.Н.Верясов

Инструкция по проведению мониторинга информационной безопасности и организации работ по сопровождению ЛВС МАОУ «Средняя общеобразовательная школа № 10»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет порядок планирования и проведения мониторинга информационной безопасности автоматизированных систем и порядок организации работ по техническому сопровождению корпоративной компьютерной сети муниципального автономного общеобразовательного учреждения «Средняя общеобразовательная школа №10» (далее - Учреждение).

1.2. Мониторинг информационной безопасности автоматизированных систем и организацию работ по техническому сопровождению локально-вычислительной сети осуществляет городской информационно-вычислительный центр.

2. МОНИТОРИНГ АППАРАТНОГО ОБЕСПЕЧЕНИЯ

2.1. Мониторинг работоспособности аппаратных компонентов автоматизированных систем осуществляется в процессе их обслуживания и при проведении работ по техническому обслуживанию оборудования. Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны контролироваться постоянно.

3. МОНИТОРИНГ ПАРОЛЬНОЙ ЗАЩИТЫ

3.1. Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают:

- установление сроков действия паролей (3 месяца) на основании «Инструкции об организации парольной защиты на объектах вычислительной техники МАОУ «Средняя общеобразовательная школа №10»;

-периодическую (не реже 1 раза в месяц) проверку пользовательских паролей на количество символов и очевидность с целью выявления слабых паролей, которые легко угадать или дешифровать с помощью специализированных программных средств (взломщиков паролей).

4. МОНИТОРИНГ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

4.1. Предупреждение и своевременное выявление попыток несанкционированного доступа осуществляется с использованием средств операционной системы, специальных программных средств и предусматривает:

- фиксацию неудачных попыток входа в систему в системном журнале;
- протоколирование работы сетевых сервисов;
- выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

5. МОНИТОРИНГ ПРОИЗВОДИТЕЛЬНОСТИ

5.1. Мониторинг производительности автоматизированных систем производится по обращениям пользователей в ходе обслуживания систем и при проведении профилактических работ.

6. СИСТЕМНЫЙ АУДИТ

6.1. Системный аудит производится ежеквартально и в особых ситуациях. Он включает проведение обзоров безопасности с занесением записей в Журнал обзоров безопасности (Приложение №1), тестирование системы, контроль внесения изменений в системное программное обеспечение.

6.2. Журналы обзоров безопасности должны включать:

- отчеты о безопасности пользовательских ресурсов, включающие наличие
- повторяющихся пользовательских имен и идентификаторов, неправильных форматов
- регистрационных записей, пользователей без пароля, неправильной установки домашних каталогов пользователей и уязвимостей пользовательских окружений;
- проверку содержимого файлов конфигурации на соответствие списку для проверки;
- обнаружение изменений системных файлов со времени проведения последней проверки (контроль целостности системных файлов);
- проверку прав доступа и других атрибутов системных файлов (команд, утилит и таблиц);
- проверку правильности настройки механизмов аутентификации и авторизации сетевых сервисов;
- проверку корректности конфигурации системных и активных сетевых устройств (мостов, маршрутизаторов, концентраторов и сетевых экранов).

6.3. Активное тестирование надежности механизмов контроля доступа производится путем осуществления попыток проникновения в систему (с помощью автоматического инструментария или вручную).

6.4. Пассивное тестирование механизмов контроля доступа осуществляется путем анализа конфигурационных файлов системы.

Информация об известных уязвимостях извлекается из документации и внешних источников. Затем осуществляется проверка конфигурации системы с целью выявления опасных состояний системы, т.е. таких состояний, в которых могут проявлять себя известные уязвимости. Если система находится в опасном состоянии, то, с целью нейтрализации уязвимостей, необходимо, либо изменить конфигурацию системы (для ликвидации условий проявления уязвимости), либо установить программные коррекции, либо установить другие версии программ, в которых данная уязвимость отсутствует, либо отказаться от использования системного сервиса, содержащего данную уязвимость.

6.5. Внесение изменений в системное программное обеспечение осуществляется администраторами систем с обязательным документированием изменений в соответствующем журнале; уведомлением каждого сотрудника, которого касается изменение; рассмотрением претензий в случае, если внесение изменений повлекло причинение вреда; разработкой планов действий в аварийных ситуациях для восстановления работоспособности системы, если внесенное в нее изменение вывело ее из строя.

7. АНТИВИРУСНЫЙ КОНТРОЛЬ

7.1. Для защиты объектов вычислительной техники необходимо использовать антивирусные программы:

- резидентные антивирусные мониторы, контролирующие подозрительные действия программ;

-утилиты для обнаружения и анализа новых вирусов.

7.2. К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

7.3. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать Live CD с другими антивирусными средствами.

7.4. Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

7.5. Антивирусный контроль объектов вычислительной техники должен проводиться в соответствии с «Инструкцией по организации антивирусной защиты на объектах вычислительной техники МАОУ «Средняя общеобразовательная школа №10».

7.6. Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

7.7. На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

- осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;
- проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

7.8. На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае, если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна блокироваться. При этом осуществляется автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

7.9. Администраторы систем еженедельно должны проводить проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которых распространяются вирусы. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

- отключить от компьютерной сети объекты вычислительной техники, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;
- немедленно сообщить о факте обнаружения вирусов своему непосредственному руководителю с указанием предположительного источника (отправителя, владельца и т.д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

8. АНАЛИЗ ИНЦИДЕНТОВ

8.1. Если администратор системы подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

- факт попытки несанкционированного доступа (далее - НСД);
- продолжается ли НСД в настоящий момент;
- кто является источником НСД;
- что является объектом НСД;
- когда происходила попытка НСД;
- как и при каких обстоятельствах была предпринята попытка НСД;
- точка входа нарушителя в систему;
- была ли попытка НСД успешной;
- определить системные ресурсы, безопасность которых была нарушена;
- какова мотивация попытки НСД.

8.2. Для выявления попытки НСД необходимо установить, какие пользователи в настоящее время работают в системе, на каких объектах вычислительной техники. Выявить подозрительную активность пользователей, проверить, что все пользователи вошли в систему со своих

рабочих мест, и никто из них не работает в системе необычно долго. Кроме того, необходимо проверить, что никто из пользователей не выполняет подозрительных программ и программ, не относящихся к его области деятельности.

8.3. При анализе системных журналов администратору необходимо произвести следующие действия:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;
- проверить наличие исходящих сообщений электронной почты, адресованные подозрительным хостам;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки получения полномочий суперпользователя или другого привилегированного пользователя;
- выявить наличие неудачных попыток входа в систему.

8.4. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

- проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;
- проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;
- проверить наличие мест в журналах, которые выглядят необычно;
- выявить попытки изменения таблиц маршрутизации и адресных таблиц;
- проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

8.5. Для обнаружения в системе следов НСД в виде файлов, вирусов, троянских программ, изменений системной конфигурации необходимо:

- составить базовую схему того, как обычно выглядит система;
- провести поиск подозрительных файлов, скрытых файлов, имен файлов и каталогов, которые обычно используются при НСД;
- проверить содержимое системных файлов, которые обычно изменяются при НСД;
- проверить целостность системных программ;
- проверить систему аутентификации и авторизации.

8.6. В случае заражения значительного количества объектов вычислительной техники после устранения последствий заражения проводится системный аудит.

9. ПОРЯДОК ПРОВЕДЕНИЯ РЕЗЕРВНОГО КОПИРОВАНИЯ

9.1. Для предотвращения потери данных из-за сбоев оборудования, уничтожения оборудования, программных ошибок, неправильных действий персонала и других возможных причин утери информации предусмотрена система регулярного резервного копирования данных. Такое резервное копирование позволяет в случае возникновения ошибки и потери информации вернуться к ближайшей работоспособной копии.

9.2. Резервное копирование критически важной информации и информации, размещенной на серверах, выполняется на предназначенные для этих целей сервера, ленточные накопители и оптические носители.

9.3. Резервное копирование проводится автоматически в установленные промежутки времени (ночью, 1 раз в сутки).

9.4. На объектах вычислительной техники пользователей не предусматривается резервного копирования системной информации, но в целях сохранности важных документов пользователю желательно проводить архивирование и хранение данных документов на оптических дисках (CD-R).

10. УКАЗАНИЯ ПО ПРОВЕДЕНИЮ ПРОФИЛАКТИЧЕСКИХ РАБОТ

10.1. Профилактические работы проводятся строго в соответствии с установленным графиком. График проведения профилактических работ на серверах на следующий месяц составляется ответственным за данный сервер и утверждается директором Учреждения.

10.2. Системный администратор обязан включить в график все периодические профилактические работы,независимо от необходимости их проведения.

10.3. Проведение профилактических работ должно фиксироваться с описанием перечня действий согласно Приложению № 2, 3 к настоящей Инструкции.

Приложение № 1

Форма журнала по безопасности за _____ 20___г.

Имя/Инвентарный номер компьютера/сервера	Дата	Планируемые работы по системному аудиту	Фактически выполненные работы	Результат	Лицо, проводившее аудит

Приложение № 2

Профилактические работы

Ежедневные работы	Еженедельные работы	Декадные работы	Ежемесячные работы
Анализ Интернет-траффика	Проверка сетевого взаимодействия	Проверка целостности операционной системы	Составление отчета доступа к Интернет-ресурсам
Анализ возможностей доступа пользователей к сетевым ресурсам	Профилактика баз данных	Принудительная проверка отказоустойчивости системы	Удаление временных и устаревших копий файлов
Просмотр отчетов служебных программ	Проверка наличия обновлений операционной системы и серверных приложений	Профилактика дисковой и файловой подсистем на сервере	
Анализ журналов событий серверов	Проверка работы сервисов и служб	Выполнение прочих работ, непосредственно связанных с работоспособностью рабочих станций	
Анализ отчетов системы безопасности	Антивирусная профилактика сервера	Профилактический останов сервера	
Проверка работоспособности почтовых служб и служб Интернета	Проверка времени последнего обновления антивирусных баз на рабочих станциях		
Выявление попыток несанкционированной установки приложений на рабочих станциях	Удаление временных и устаревших копий файлов		

Приложение № 3

Перечень проведенных профилактических работ за_____ 20___г.

Дата	Инвентарный номер компьютера	Планируемые профилактические работы	Фактически выполненные работы	Результат	Лицо, проводившее профилактику

Приложение № 4

Директору
МАОУ «Средняя школа №10»
Верясову В.Н.
_____

Служебная записка

Прошу создать учетную запись для:

№ п/п	Фамилия, имя, отчество работника	Должность	Номер кабинета, телефон	На период времени (постоянно или дата окончания договора)	Доступ к персональным данным (да, нет)
1					
2					
3					
4					
5					
6					
7					
8					
9					

Контактное лицо_____ Телефон_____

Руководитель подразделения _____

Приложение № 5

Директору
МАОУ «Средняя школа №10»
Верясову В.Н.
_____

Служебная записка

Прошу изменить, восстановить пароль или заблокировать, разблокировать учетную запись (нужное подчеркнуть) для:

Фамилия, имя, отчество работника	Должность	На период времени (для блокировки)	Номер кабинета, телефон

Руководитель подразделения _____