

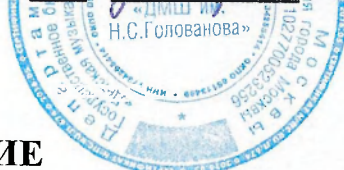
УТВЕРЖДЕНО

Приказом ГБУДО г. Москвы

"Детская музыкальная школа

имени Н.С.Голованова"

от 15 декабря 20 11 г. №51/1-08



ПОЛОЖЕНИЕ

**об обеспечении безопасности персональных данных в ГБУДО
города Москвы "Детская музыкальная школа имени Н.С.Голованова"
при их обработке в информационных системах персональных данных**

1.1. Положение об обеспечении безопасности персональных данных при их автоматизированной обработке в информационных системах персональных данных в Государственном бюджетном учреждении дополнительного образования города Москвы "Детская музыкальная школа имени Н.С.Голованова" (далее – Положение) разработано в соответствии со статьями 18, 19 Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных", постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", постановлением Правительства Российской Федерации от 21 марта 2012 г. № 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами".

1.2. Положение разработано в целях защиты персональных данных при их обработке в информационных системах персональных данных (далее – ИСПДн) в Государственном бюджетном учреждении дополнительного образования города Москвы "Детская музыкальная школа имени Н.С.Голованова" (далее – Оператор).

1.3. Положение определяет порядок работы в ИСПДн в части обеспечения безопасности персональных данных при их обработке; порядок приостановки предоставления персональных данных в случае обнаружения нарушений порядка их предоставления; правила обновления общесистемного и прикладного программного обеспечения; правила организации антивирусной защиты и парольной защиты ИСПДн; порядок охраны и допуска посторонних лиц в помещения ограниченного доступа; порядок разбирательства и составления заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, разработку и принятие мер по предотвращению возможных опасных последствий таких нарушений.

2. Основные понятия и определения

2.1. Безопасность персональных данных при их обработке в ИСПДн обеспечивается с помощью системы защиты персональных данных, нейтрализующей актуальные угрозы. **Система защиты** персональных данных включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности персональных данных и информационных технологий, используемых в информационных системах.

2.2. **Информационная система является информационной системой, обрабатывающей специальные категории персональных данных**, если в ней обрабатываются персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов персональных данных.

Информационная система является информационной системой, обрабатывающей биометрические персональные данные, если в ней обрабатываются сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, и не обрабатываются сведения, относящиеся к специальным категориям персональных данных.

Информационная система является информационной системой, обрабатывающей общедоступные персональные данные, если в ней обрабатываются персональные данные субъектов персональных данных, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона "О персональных данных".

Информационная система является информационной системой, обрабатывающей иные категории персональных данных, если в ней не обрабатываются персональные данные, указанные в абзацах первом – третьем настоящего пункта.

Информационная система является информационной системой, обрабатывающей персональные данные сотрудников оператора, если в ней обрабатываются персональные данные только указанных сотрудников. В остальных случаях информационная система персональных данных является информационной системой, обрабатывающей персональные данные субъектов персональных данных, не являющихся сотрудниками оператора.

2.3. **Под актуальными угрозами безопасности персональных данных** понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

2.3.1. Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится Оператором с учетом оценки возможного вреда, проведенной во исполнение пункта 5 части 1 статьи 18¹ Федерального закона "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение части 5 статьи 19 Федерального закона "О персональных данных".

2.3.2. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных, согласно Требованиям к защите персональных данных при их обработке в информационных системах персональных данных, утвержденным постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119.

3. Порядок обеспечения безопасности персональных данных при их обработке в ИСПДн

3.1. Перед началом работы в ИСПДн пользователи должны ознакомиться с инструкциями по использованию средств защиты информации.

3.2. Допуск пользователей для работы на компьютерах ИСПДн осуществляется в соответствии со списком лиц, допущенных к работе в ИСПДн, назначенных приказом директора школы. С целью обеспечения нормального функционирования и контроля работы средств защиты информации в ИСПДн назначается ответственный за выполнение работ по обеспечению безопасности персональных данных при их обработке в ИСПДн (далее – ответственный за защиту информации).

3.3. Пользователь имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИСПДн. При этом для хранения информации, содержащей ПДн, разрешается использовать только машинные носители информации, учтенные в Журнале учета машинных носителей согласно приложению № 2 к настоящему Положению.

3.4. Пользователь несет ответственность за правильность включения и выключения средств вычислительной техники, входа в систему и все действия при работе в ИСПДн.

3.5. Вход пользователя в систему может осуществляться по персональному паролю.

3.6. При работе со съемными машинными носителями информации в случае обнаружения вирусов пользователь обязан немедленно прекратить их использование и действовать в соответствии с требованиями данного Положения.

3.7. Каждый сотрудник, участвующий в рамках своих трудовых обязанностей в процессах автоматизированной обработки персональных данных и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

- строго соблюдать установленные правила обеспечения безопасности информации при работе с программными и техническими средствами ИСПДн;
- хранить в тайне и регулярно менять свой пароль (пароли);
- хранить свое индивидуальное устройство идентификации (ключ) и другие реквизиты в недоступном для посторонних лиц месте;
- выполнять требования по использованию антивирусной защиты в полном объеме.

Немедленно известить ответственного за защиту информации в случае утери индивидуального устройства идентификации (ключа) или при подозрении компрометации личных ключей и паролей, а также при обнаружении:

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ИСПДн;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию средств вычислительной техники, выхода из строя или неустойчивого функционирования узлов средств вычислительной техники или периферийных устройств (сканера, принтера и т.п.), а также перебоев в системе электроснабжения;
- некорректного функционирования установленных на компьютеры технических средств защиты;
- непредусмотренных отводов кабелей и подключенных устройств.

Пользователю категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения средств вычислительной техники в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ИСПДн или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить конфиденциальную информацию (содержащую сведения ограниченного распространения) на неучтенных машинных носителях информации;
- оставлять включенным без присмотра компьютер, не активизировав средства защиты от несанкционированного доступа к персональным данным (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, машинные носители и распечатки, содержащие конфиденциальную информацию;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации;
- размещать средства ИСПДн так, чтобы существовала возможность визуального считывания с них информации.

3.8. Ответственный за защиту персональных данных при их обработке в ИСПДн обязан:

- знать состав основных и вспомогательных технических систем и средств, установленных и смонтированных в ИСПДн, перечень используемого программного обеспечения в ИСПДн;
- контролировать целостность печатей (пломб, защитных наклеек) на периферийном оборудовании, защищенных средств вычислительной техники и других устройствах;
- вести соответствующие журналы согласно приложениям №№ 1-7 к настоящему Положению;
- контролировать своевременное проведение смены паролей для доступа пользователей к компьютерам и ресурсам ИСПДн;
- контролировать выполнения сотрудниками установленного комплекса мероприятий по обеспечению безопасности информации в ИСПДн;
- соблюдать порядок создания, учета, хранения и использования резервных и архивных копий массивов данных;
- настраивать и сопровождать подсистемы регистрации и учета действий пользователей при работе в ИСПДн;
- вводить в базу данных СЗИ от несанкционированного доступа описания событий, подлежащих регистрации в системном журнале согласно приложению № 5 к настоящему Положению;
- периодически тестировать функции средства защиты информации от несанкционированного доступа, особенно при изменении программной среды и полномочий исполнителей;
- восстанавливать программную среду, программные средства и настройки средств защиты информации при сбоях;
- проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления несанкционированного доступа к информации и техническим средствам вычислительной техники;
- обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации технического обслуживания ИСПДн и отправке его в ремонт (затирать конфиденциальную информацию);
- присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн;
- вести Журнал учета нештатных ситуаций, фактов вскрытия и опечатывания средств вычислительной техники согласно приложению № 5 к настоящему Положению, выполнения профилактических работ, установки и модификации аппаратных и программных средств вычислительной техники;
- поддерживать установленный порядок проведения антивирусного контроля согласно требованиям настоящего Положения, в случае отказа средств и систем защиты информации принимать меры по их восстановлению;
- вести документацию на ИСПДн в соответствии с требованиями нормативных документов.

3.9. Ответственный по обеспечению безопасности персональных данных при их обработке в ИСПДн имеет право:

- требовать от пользователей ИСПДн соблюдения установленных правил обработки информации и выполнения требований по обеспечению безопасности и защите информации в ИСПДн;

- инициировать проведение проверок по фактам нарушения установленных требований обеспечения защиты, несанкционированного доступа, утраты, модификации, порчи защищаемой информации и технических компонентов ИСПДн;
- требовать прекращения обработки информации в случае нарушения установленного порядка работ или нарушения функционирования средств и систем защиты информации;
- участвовать в анализе ситуаций, касающихся функционирования средств защиты информации и расследования фактов несанкционированного доступа.

4. Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных, защищаемой информации и средств защиты информации

4.1. К использованию для создания резервной копии в ИСПДн допускаются только зарегистрированные в журнале учета носители.

4.2. Ответственный за защиту информации в ИСПДн осуществляет резервное копирование конфиденциальной информации.

4.3. Перед резервным копированием ответственный по обеспечению безопасности конфиденциальной информации обязан проверить электронный носитель (ЖМД, CD, USB-накопитель) на отсутствие вирусов.

4.4. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

4.5. Запрещается запись посторонней информации на электронные носители (ЖМД, CD, USB-накопитель и другие) резервной копии.

4.6. Порядок создания резервной копии:

- вставить в компьютер зарегистрированный электронный носитель (ЖМД, CD, USB-накопитель, другие) для резервного копирования;
- выбрать необходимый каталог (файл) для создания резервного архива;
- при использовании систем управления базами данных необходимо создать файл с резервной копией защищаемой информации с помощью встроенных средств системы;
- выполнить процедуру создания резервной копии;
- произвести копирование на отчуждаемый носитель;
- произвести отключение отчуждаемого носителя и, создав необходимые записи в журналах, убрать носитель в специальное хранилище. Хранить совместно с ключевой и аутентифицирующей информацией.

4.7. При восстановлении работоспособности программного обеспечения сначала осуществляется резервное копирование защищаемой информации, затем производится полная деинсталляция некорректно работающего программного обеспечения.

4.8. Ответственный за защиту информации в ИСПДн отвечает за восстановление программного обеспечения.

4.9. Восстановление программного обеспечения производится путем его инсталляции с использованием эталонных дистрибутивов.

4.10. При необходимости ремонта технических средств оборудование передается в сервисный центр производителя. Ремонт носителей защищаемой информации не допускается. Неисправные носители с защищаемой информацией подлежат уничтожению в соответствии с порядком уничтожения носителей защищаемой информации. Работа с использованием неисправных технических средств запрещается.

4.11. При работе на компьютерах ИСПДн рекомендуется использовать источники бесперебойного питания с целью предотвращения повреждения технических средств и (или) защищаемой информации в результате сбоев в сети электропитания.

4.12. При восстановлении работоспособности средств защиты информации следует выполнить их настройку в соответствии с требованиями безопасности информации, изложенными в техническом задании на создание системы защиты персональных данных

4.13. Восстановление средств защиты информации производится с использованием эталонных сертифицированных дистрибутивов, которые хранятся в хранилище. После успешной настройки средств защиты информации необходимо выполнить резервное копирование настроек данных средств с помощью встроенных в них функций на зарегистрированный носитель.

5. Порядок контроля защиты информации в ИСПДн и о принятии мер по предотвращению возможных опасных последствий

5.1. Контроль защиты информации в ИСПДн – комплекс организационных и технических мероприятий, которые организуются и осуществляются в целях предупреждения и пресечения возможности получения посторонними лицами охраняемых сведений, выявления и предотвращения утечки конфиденциальной информации по техническим каналам, исключения или существенного затруднения несанкционированного доступа к информации, хищения технических средств и носителей информации, предотвращения специальных программно-технических воздействий, вызывающих нарушение характеристик безопасности информации или работоспособности систем информатизации.

5.2. Основными задачами контроля являются:

- выявление демаскирующих признаков объектов ИСПДн;
- уточнение зон перехвата обрабатываемой на объектах информации, возможных каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- проверка выполнения установленных норм и требований по защите информации от утечки по техническим каналам, оценка достаточности и эффективности мероприятий по защите информации;
- проверка выполнения требований по защите ИСПДн от несанкционированного доступа;

- проверка выполнения требований по антивирусной защите автоматизированных систем и автоматизированных рабочих мест;
- проверка знаний работников в области защиты информации и уровня их подготовки для работы с конфиденциальной информацией;
- оперативное принятие мер по пресечению нарушений требований (норм) защиты информации в ИСПДн;
- разработка предложений по устранению (ослаблению) демаскирующих признаков и технических каналов утечки информации.

5.3. Контроль защиты информации проводится с учетом реальных условий по всем физическим полям, по которым возможен перехват информации, циркулирующей в ИСПДн, и осуществляется по объектовому принципу, при котором на объекте одновременно проверяются все вопросы защиты информации. Перечень каналов утечки устанавливается в соответствии с моделью угроз.

5.4. В ходе контроля проверяются:

- соответствие принятых мер по обеспечению безопасности персональных данных;
- своевременность и полнота выполнения требований по обеспечению безопасности персональных данных;
- полнота выявления демаскирующих признаков охраняемых сведений об объектах защиты и возможных технических каналов утечки информации, несанкционированного доступа к ней и программно-технических воздействий на информацию;
- эффективность применения организационных и технических мероприятий по защите информации;
- устранение ранее выявленных недостатков.

Кроме того, могут проводиться необходимые измерения и расчеты приглашенными для этих целей специалистами организации, имеющей соответствующие лицензии Федеральной службы по техническому и экспортному контролю Российской Федерации.

5.5. Основными видами технического контроля являются визуально-оптический контроль, контроль эффективности защиты информации от утечки по техническим каналам, контроль несанкционированного доступа к информации и программно-технических воздействий на информацию.

5.6. Полученные результаты анализируются в целях определения достаточности и эффективности предписанных мер защиты информации и выявления нарушений. При обнаружении нарушений норм и требований по защите информации ответственный за защиту информации докладывает директору для принятия решения о прекращении обработки информации и проведения соответствующих организационных и технических мер по устранению нарушения. Результаты контроля защиты информации оформляются актами либо в соответствующих журналах учета результатов контроля.

5.7. Невыполнение предписанных мероприятий по защите персональных данных считается предпосылкой к утечке информации (далее – предпосылка). По каждой предпосылке для выяснения обстоятельств и причин невыполнения установленных требований проводится расследование.

Для проведения расследования назначается комиссия. Комиссия обязана установить, имела ли место утечка сведений, обстоятельства ей сопутствующие, установить лиц, виновных в нарушении предписанных мероприятий по защите информации, причины и условия, способствовавшие нарушению, и выработать рекомендации по их устранению. После окончания расследования директором школы принимается решение о наказании виновных лиц и необходимых мероприятиях по устранению недостатков.

5.8. Ведение контроля защиты информации осуществляется путем проведения периодических, плановых и внезапных проверок объектов защиты. Периодические, плановые и внезапные проверки объектов организации проводятся, как правило, в соответствии с утвержденным планом или по согласованию с директором.

6. Правила антивирусной защиты

6.1. Настоящие правила определяют требования к организации защиты объекта ИСПДн от разрушающего воздействия вредоносного программного обеспечения, компьютерных вирусов. Настоящие правила распространяются на все объекты ИСПДн.

6.2. К использованию на компьютерах допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

6.3. Установка и начальная настройка средств антивирусного контроля на компьютерах, а также периодическое обновление антивирусных пакетов и контроль их работоспособности осуществляются ответственным за защиту информации.

6.4. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

Настройки средств антивирусной защиты должны быть выполнены в соответствии с требованиями безопасности персональных данных определенного для данной ИСПДн класса. Настройку средств антивирусной защиты выполняет ответственный за защиту информации.

6.5. Файлы, помещаемые в электронный архив на магнитных носителях, должны в обязательном порядке проходить антивирусный контроль. Периодически должны проводиться проверки электронных архивов.

6.6. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера

ответственным за защиту информации должна быть выполнена антивирусная проверка ИСПДн.

6.7. На компьютеры запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.

6.8. 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 самостоятельно или вместе с ответственным за защиту информации должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить обработку данных в ИСПДн;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за защиту информации, а также иных работников, допущенных к работе с персональными данными, использующих эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности, дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

6.9. Ответственность за организацию антивирусного контроля в ИСПДн возлагается на ответственного за защиту информации.

6.10. Ответственность за проведение мероприятий антивирусной защиты в конкретной ИСПДн и соблюдение требований настоящего Положения возлагается на всех пользователей данной ИСПДн.

7. Правила парольной защиты

7.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль действий пользователей при работе с паролями возлагается на ответственного за защиту информации.

7.2. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями ИСПДн самостоятельно с учетом следующих требований:

- пароль должен быть не менее 6 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, \$, &, *, % и т.п.);
- символы паролей должны вводиться в режиме латинской раскладки клавиатуры;
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

- при смене пароля новое значение должно отличаться от предыдущих;
- пользователь не имеет права сообщать личный пароль другим лицам.

Владельцы паролей должны быть ознакомлены с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

7.3. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств, технологической необходимости использования имен и паролей пользователей в их отсутствие, работники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение ответственному за защиту информации. Запечатанные конверты с паролями исполнителей должны храниться в недоступном месте.

7.4. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в течение 360 дней.

7.5. Внеплановая смена личного пароля или удаление учетной записи пользователя ИСПДн в случае прекращения его полномочий должна производиться ответственным за защиту информации (либо новым постоянным пользователем) немедленно после окончания последнего сеанса работы данного пользователя с системой.

7.6. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри учреждения и другие обстоятельства) ответственного за защиту информации.

7.7. В случае компрометации личного пароля пользователя ИСПДн должны быть немедленно предприняты меры по восстановлению парольной защиты.

7.8. Контроль действий пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования возлагается на ответственного за защиту информации.

8. Правила обновления общесистемного и прикладного программного обеспечения, технического обслуживания ИСПДн

8.1. Право внесения изменений в конфигурацию аппаратно-программных средств, защищенных ИСПДн предоставляется ответственному за защиту информации в отношении системных и прикладных программных средств и аппаратных средств, а также в отношении программно-аппаратных средств защиты.

8.2. Внесение изменений в конфигурацию системных и прикладных программных средств ИСПДн инициируется ответственным за эксплуатацию ИСПДн с указанием необходимых изменений:

- установка (развертывание) на компьютер(ы) программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи в данной ИСПДн);

- обновление (замена) на компьютере (ах) программных средств, необходимых для решения определенной задачи (обновление версий, используемых для решения определенной задачи программ);

- удаление с компьютера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данном компьютере).

8.3. Установка и обновление программного обеспечения (системного, тестового и т.п.) на компьютерах производится только с оригинальных лицензионных дистрибутивных носителей; прикладного программного обеспечения – с эталонных копий программных средств, полученных из архива дистрибутивов установленного программного обеспечения.

8.4. Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, а также отсутствие опасных функций.

8.5. После установки (обновления) программного обеспечения ответственный за защиту информации должен произвести требуемые настройки средств управления доступом к компонентам компьютера и проверить работоспособность программного обеспечения и правильность их настройки и произвести соответствующую запись в Журнале учета нештатных ситуаций в ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн согласно приложению № 5 к настоящему Положению, делает отметку о выполнении в Техническом паспорте.

8.6. При возникновении ситуаций, требующих передачи технических средств в сервисный центр с целью ремонта, ответственный за защиту информации предпринимает необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера. Делает отметку в Журнале учета нештатных ситуаций ИСПДн, выполнения профилактических работ, установки и модификации программных средств на компьютерах ИСПДн.

8.7. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом.

8.8. С целью соблюдения принципа персональной ответственности за свои действия каждому работнику, допущенному к работе на компьютерах конкретной ИСПДн, должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать на данном компьютере.

8.9. Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя ("группового имени") запрещено.

8.10. Работнику, зарегистрированному в качестве нового пользователя ИСПДн, сообщается имя соответствующего ему пользователя и может выдаваться персональный идентификатор (для работы в режиме усиленной аутентификации) и начальное(-ые) значение(-ия) пароля(-ей), которое(-ые) он обязан сменить при первом же входе в систему.

9. Порядок контроля соблюдения условий использования средств защиты информации, в том числе криптографических (СЗИ)

9.1. Технические средства защиты информации являются важным компонентом по обеспечению безопасности персональных данных.

9.2. Порядок работы с техническими СЗИ определен в соответствующих руководствах по настройке и использованию СЗИ обязательных для исполнения всеми работниками, обрабатывающими конфиденциальную информацию, а также ответственным за защиту информации в ИСПДн.

9.3. Пользователю ИСПДн категорически запрещается: обрабатывать конфиденциальную информацию с отключенными СЗИ, менять настройки СЗИ.

9.4. Ответственному за защиту информации запрещается менять настройки программно-аппаратных СЗИ, предустановленные специалистом организации, имеющей лицензию на деятельность по технической защите информации, без согласования с этой организацией.

9.5. Если в ходе периодических, плановых или внезапных проверок ИСПДн выявлено нарушение требования п. 8.4, то проводится расследование согласно пункту 5.7 настоящего Положения.

9.6. Криптографические СЗИ должны использоваться в соответствии с технической и эксплуатационной документацией на них, а также в соответствии с правилами пользования ими.

10. Порядок охраны и допуска посторонних лиц в защищаемые помещения

10.1. В целях защиты конфиденциальной информации вскрытие и закрытие помещений осуществляется работниками, допущенными к персональным данным, обрабатываемым в ИСПДн в данных помещениях.

Список работников, допущенных к персональным данным, обрабатываемым в ИСПДн, имеющих право вскрывать помещения, утверждается приказом директора школы.

10.2. При закрытии помещений работники, допущенных к персональным данным, обрабатываемым в ИСПДн, проверяют закрытие окон, выключают освещение, бытовые приборы, оргтехнику и проверяют противопожарное состояние помещения, а документы и носители информации, на которых содержится конфиденциальная информация, убираются для хранения в сейф (металлический шкаф).

10.3. Если обнаружено вторжение в защищаемое помещение, то необходимо действовать в порядке, указанном в пункте 5.7 настоящего Положения.

10.4. При обработке защищаемой информации в ИСПДн запрещено пребывание посторонних лиц.

11. Порядок стирания защищаемой информации и уничтожения носителей защищаемой информации

11.1. В обязательном порядке уничтожению подлежат поврежденные, выводимые из эксплуатации носители, содержащие защищаемую информацию, использование которых не предполагается в дальнейшем. Стиранию подлежат носители, содержащие защищаемую информацию, которые выводятся из эксплуатации в составе ИСПДн. Не допускаются стирание неисправных носителей и передача их в сервисный центр для ремонта. Такие носители должны уничтожаться.

11.2. Стирание должно производиться по технологии, предусмотренной для данного типа носителя, с применением сертифицированных средств гарантированного уничтожения информации (допускается задействовать механизмы затирания встроенные в сертифицированные средства защиты информации).

11.3. Уничтожение носителей производится путем нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления информации (перед уничтожением, если носитель исправен, должно быть произведено гарантирование стирания информации на носителе). Непосредственные действия по уничтожению конкретного типа носителя должны исключать возможность восстановления информации.

11.4. Бумажные и прочие сгораемые носители (конверты с неиспользуемыми более паролями) уничтожают путем сжигания или с помощью любых бумагорезательных машин.

11.5. По факту уничтожения или стирания носителей составляется акт, в журналах учета делаются соответствующие записи.

11.6. Процедуры стирания и уничтожения осуществляются комиссией, в которую входят: ответственный за эксплуатацию ИСПДн, ответственный за защиту информации.

12. Заключительные положения

12.1. Требования настоящего Положения обязательны для всех работников, обрабатывающих конфиденциальную информацию (персональные данные).

12.2. Нарушение требований настоящего Положения влечет за собой ответственность в соответствии с законодательством Российской Федерации.

12.3. Срок действия Порядка неограничен.

12.4. В Порядок могут вноситься уточнения в случае изменения требований законодательства Российской Федерации в области персональных данных, в том числе в случае изменения требований к защите персональных данных при их обработке в ИСПДн. Изменения в документ вносятся путем издания новой версии.

12.5. Порядок действует до принятия нового.

Приложение 1
к Положению по обеспечению безопасности
персональных данных при их автоматизированной
обработке в информационных системах персональных
данных в ГБУДО г. Москвы "Детская музыкальная школа
имени Н.С.Голованова"

**Журнал
поэкземплярного учета криптосредств, эксплуатационной и технической
Документации к ним, ключевых документов**

№ п/п	Наименование криптосредства эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографичес кие номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводи тельного письма	Ф.И.О. пользователя криптосредств	Дата, подпись в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф.И.О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф.И.О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение 2
к Положению по обеспечению безопасности
персональных данных при их автоматизированной
обработке в информационных системах персональных
данных в ГБУДО г. Москвы "Детская музыкальная школа
имени Н.С.Голованова"

**Журнал
учета машинных носителей информации**

[illegible]

Приложение 3
к Положению по обеспечению безопасности
персональных данных при их автоматизированной
обработке в информационных системах персональных
данных в ГБУДО г. Москвы "Детская музыкальная школа
имени Н.С.Голованова"

**Журнал
учета хранилищ**

№ п/п	Регистрационный (учетный) номер хранилища	Вид хранилища	Дата постановки на учет	Фамилия и подпись принявшего (ответственного), дата	Место расположения (номер помещения)	Дата и номер акта о выводе из эксплуатации	Примечание
1	2	3	4	5	6	7	8

Приложение 4
к Положению по обеспечению безопасности
персональных данных при их автоматизированной
обработке в информационных системах персональных
данных в ГБУДО г. Москвы "Детская музыкальная школа
имени Н.С.Голованова"

**Журнал
периодического тестирования средств защиты информации**

№ п/п	Наименование средства защиты информации от НСД или криптосредства	Регистрационные номера СЗИ от НСД или криптосредства	Дата тестирования	Фамилия и подпись ответственного пользователя, проводившего тестирование	Наименование теста, используемые средства для проведения теста	Результат тестирования (успешный/ неуспешный), комментарий	Дата очередного тестирования
1	2	3	4	5	6	7	8

Приложение 5
к Положению по обеспечению безопасности
персональных данных при их автоматизированной
обработке в информационных системах персональных
данных в ГБУДО г. Москвы "Детская музыкальная школа
имени Н.С.Голованова"

Журнал
учета нештатных ситуаций ИСПДн, выполнения профилактических работ,
установки и модификации программных средств на компьютерах ИСПДн

№ п/п	Дата	Краткое описание выполненной работы (нештатной ситуации)	Ф.И.О. исполнителей и их подписи	Ф.И.О. ответственного за эксплуатацию ПЭВМ, подпись	Подпись специалиста по защите информации	Примечание (ссылка на заявку)
1	2	3	4	5	6	7

Приложение 6
к Положению по обеспечению безопасности
персональных данных при их автоматизированной
обработке в информационных системах персональных
данных в ГБУДО г. Москвы "Детская музыкальная школа
имени Н.С.Голованова"

Журнал регистрации письменных запросов

[illegible]

Приложение 7
к Положению по обеспечению безопасности
персональных данных при их автоматизированной
обработке в информационных системах персональных
данных в ГБУДО г. Москвы "Детская музыкальная школа
имени Н.С.Голованова"

**Журнал
регистрации персональных данных (ПДн)**

[illegible]