

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ  
ДОПОЛНИТЕЛЬНОГО ОБРАЗОВАНИЯ ВОЛГОГРАДА  
«Детская музыкальная школа № 1»  
(МБУ ДО ДМШ №1)**

---

СОГЛАСОВАНО

На заседании И.О.

МБУ ДО ДМШ №1

Протокол от «17»

Председатель И.О.

МБУ ДО ДМШ №1



2025 г. № 44

А.А.Левшина.

УТВЕРЖДАЮ

Директор МБУ ДО ДМШ №1



Д.В.Шарапудинова

ДМШ № 1

«17»

2025 г.

**Положение  
об информационной безопасности**

**муниципального бюджетного учреждения дополнительного образования  
Волгограда «Детская музыкальная школа № 1»  
(МБУ ДО ДМШ №1)**

**1. Общие положения**

1.1. Положение об информационной безопасности муниципального бюджетного учреждения дополнительного образования Волгограда «Детская музыкальная школа № 1» (далее – МБУ ДО ДМШ № 1) разработано в соответствии с Федеральным законом № 273-ФЗ от 29.12.2012 г. «Об образовании в Российской Федерации», Федеральным законом № 152-ФЗ от 27.07.2006 г. «О персональных данных», Федеральным законом Российской Федерации от 27.07.2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Письмом Федерального агентства по образованию от 29.07.2009 г. № 17-110 «Об обеспечении защиты персональных данных»..

1.2. В понятие информационной безопасности МБУ ДО ДМШ № 1 входит система мер, направленная на защиту информационного пространства и персональных данных от случайного или намеренного проникновения с целью хищения каких-либо данных или внесения изменений в конфигурацию системы, защита образовательного процесса от любых сведений, носящих характер запрещенной законом пропаганды, или любых видов рекламы.

1.3. В составе массивов охраняемой законом информации, находящейся в распоряжении МБУ ДО ДМШ № 1, можно выделить три группы:

– персональные сведения, касающиеся обучающихся, в том числе фамилия, имя, отчество, год, месяц, дата и место рождения, адрес;

- персональные сведения, касающиеся работников, в том числе фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- другая информация для служебного пользования, не относящаяся ни к одному из указанных выше видов и носящая характер интеллектуальной собственности МБУ ДО ДМШ № 1 в том числе библиотека, база данных, образовательные программы и др.

Обязанностями лиц, ответственных за защиту информации, должно стать сохранение данных в целостности и неприкосновенности и обеспечение их:

- доступности в любое время для любого авторизированного пользователя;
- защиты от любой утраты или внесения несанкционированных изменений;
- конфиденциальности, недоступности для третьих лиц.

## **2. Цель и задачи информационной безопасности**

2.1. Основными целями информационной безопасности являются:

- сохранение конфиденциальности информационных ресурсов;
- обеспечение непрерывности доступа к информационным ресурсам МБУ ДО ДМШ № 1;
- защита целостности информации с целью поддержания возможности МБУ ДО ДМШ № 1 по оказанию услуг высокого качества и принятию эффективных управленческих решений;
- повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами МБУ ДО ДМШ № 1;
- определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности;
- повышение уровня эффективности, непрерывности, контролируемости мер по защите от реальных угроз информационной безопасности;
- предотвращение и/или снижение ущерба от инцидентов информационной безопасности.

2.2. Основными задачами информационной безопасности являются:

- разработка требований по обеспечению информационной безопасности;
- контроль выполнения установленных требований по обеспечению информационной безопасности;
- повышение эффективности, непрерывности, контролируемости мероприятий по обеспечению и поддержанию информационной безопасности;
- разработка нормативных документов для обеспечения информационной безопасности МБУ ДО ДМШ № 1;
- выявление, оценка, прогнозирование и предотвращение реализации угроз информационной безопасности МБУ ДО ДМШ № 1;
- организация антивирусной защиты информационных ресурсов школы;
- защита информации школы от несанкционированного доступа (далее-НСД) и утечки по техническим каналам связи.

## **3. Требования по информационной безопасности**

3.1. В отношении всех собственных информационных активов МБУ ДО ДМШ № 1, активов, находящихся под контролем МБУ ДО ДМШ № 1, а также активов, используемых для получения доступа к инфраструктуре МБУ ДО ДМШ № 1, должна быть определена ответственность соответствующего сотрудника МБУ ДО ДМШ № 1. Информация о смене владельцев активов, их распределении, изменениях в конфигурации и использовании за пределами

школы должна доводиться до сведения директора школы.

3.2. Все работы в пределах МБУ ДО ДМШ № 1 должны выполняться в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию.

3.3. Все конфиденциальные данные, составляющие тайну МБУ ДО ДМШ № 1 и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы.

3.4. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

3.5. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким.

3.6. В процессе своей работы сотрудники обязаны постоянно использовать режим "Экранной заставки" с парольной защитой. Рекомендуется устанавливать максимальное время "простоя" компьютера до появления экранной заставки не дольше 15 минут.

3.7. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

3.8. Рекомендованные правила:

- сотрудникам МБУ ДО ДМШ № 1 разрешается использовать сеть Интернет только в служебных целях;

- запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

- работа сотрудников МБУ ДО ДМШ № 1 с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации МБУ ДО ДМШ № 1 в сеть Интернет;

- сотрудникам, имеющим личные учетные записи, предоставленные публичными провайдерами, не разрешается пользоваться ими на оборудовании, принадлежащем МБУ ДО ДМШ № 1;

- сотрудники МБУ ДО ДМШ № 1 перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

- запрещен доступ в Интернет через сеть МБУ ДО ДМШ № 1 для всех лиц, не являющихся сотрудниками школы, включая членов семьи сотрудников.

3.9. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится информация МБУ ДО ДМШ № 1.

3.10. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения.

3.11. Все компьютерное оборудование (стационарные и портативные компьютеры), периферийное оборудование (принтеры и сканеры), аксессуары (манипуляторы типа "мышь", дисководы для CD-дисков) является собственностью МБУ ДО ДМШ № 1 и предназначено для использования исключительно в производственных целях.

3.12. Каждый сотрудник, получивший в пользование портативный компьютер, обязан принять надлежащие меры по обеспечению его сохранности.

3.13. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима "Экранной заставки". Для установки режимов защиты пользователь должен обратиться к администратору. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

3.14. При записи какой-либо информации на носитель для передачи субъектам, участвующим в информационном обмене, необходимо убедиться в том, что носитель чист, то есть не содержит никаких иных данных. Простое переформатирование носителя не дает гарантии полного удаления записанной на нем информации.

3.15. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено неразрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственно директору МБУ ДО ДМШ №1.

3.16. Сотрудники МБУ ДО ДМШ №1 не должны:

- блокировать антивирусное программное обеспечение;
- устанавливать другое антивирусное программное обеспечение;
- изменять настройки и конфигурацию антивирусного программного обеспечения.

3.17. Электронные сообщения должны строго соответствовать стандартам в области деловой этики. Использование электронной почты в личных целях не допускается. Сотрудникам запрещается направлять конфиденциальную информацию МБУ ДО ДМШ №1 по электронной почте без использования систем шифрования. Строго конфиденциальная информация МБУ ДО ДМШ №1, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

3.18. Использование сотрудниками МБУ ДО ДМШ №1 публичных почтовых ящиков электронной почты осуществляется только при согласовании с ответственным за обеспечение безопасности информации при условии применения механизмов шифрования.

3.19. Сотрудники МБУ ДО ДМШ №1 для обмена документами должны использовать только свой официальный адрес электронной почты.

3.20. Не допускается при использовании электронной почты:

- рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;
- рассылка рекламных материалов;
- подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;
- поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);
- пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско- правовой

ответственности, беспорядков или противоречит стандартам в области этики.

3.21. Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

3.22. В случае кражи переносного компьютера следует незамедлительно сообщить заместителю директора и/или директору МБУ ДО ДМШ №1.

3.23. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

- проинформировать заместителя директора;
- не использовать и не включать зараженный компьютер;
- не подсоединять этот компьютер к компьютерной сети МБУ ДО ДМШ №1 до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование администратором.

3.24. Сотрудникам МБУ ДО ДМШ №1 запрещается:

- нарушать информационную безопасность и работу сети МБУ ДО ДМШ №1;
- сканировать порты или систему безопасности;
- контролировать работу сети с перехватом данных;
- получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;
- передавать информацию о сотрудниках или списки сотрудников МБУ ДО ДМШ №1 посторонним лицам;
- создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

3.25. Ответственность за сохранность данных на стационарных и портативных персональных компьютерах лежит на пользователях.

### **Угрозы информационной безопасности**

3.26. Особенностью угроз становится не только возможность хищения сведений или повреждение массивов какими-либо сознательно действующими хакерскими группировками, но и деятельность лиц, намеренно, по злому умыслу или ошибочно способных повредить компьютерное оборудование или внести вирус.

3.27. Группы объектов, которые могут подвергнуться намеренному или ненамеренному воздействию:

- компьютерная техника и другие аппаратные средства, которые могут быть повреждены в результате механического воздействия, вирусов, по иным причинам;
- программы, используемые для обеспечения работоспособности системы или в образовательном процессе, которые могут пострадать от вирусов или хакерских атак;
- данные, хранимые как на жестких дисках, так и на отдельных носителях;
- сам персонал, отвечающий за работоспособность IT-систем;
- дети, подверженные внешнему агрессивному информационному влиянию и способные создать в МБУ ДО ДМШ №1 криминальную ситуацию.

3.28. Угрозы, направленные на повреждение любого из компонентов системы, не зависящие от намерения персонала, учащихся или третьих лиц:

- любые аварийные ситуации, например, отключение электроэнергии или затопление;

- ошибки персонала;
- сбои в работе программного обеспечения;
- выход техники из строя;
- проблемы в работе систем связи.

#### **4. Способы несанкционированного доступа**

##### **4.1. Человеческий.**

Информация может быть похищена путем копирования на временные носители, переправлена по электронной почте. При наличии доступа к серверу изменения в базы данных могут быть внесены вручную.

##### **4.2. Программный.**

Для хищений сведений используются специальные программы, которые обеспечивают копирование паролей, копирование и перехват информации, перенаправление трафика, дешифровку, внесение изменений в работу иных программ.

##### **4.3. Аппаратный.**

Способ связан или с использованием специальных технических средств, или с перехватом электромагнитного излучения по различным каналам, включая телефонные.

#### **5. Защита по внешним цифровым линиям связи**

5.1. В целях уменьшения риска повреждения программного обеспечения и утери информации, доступ из внутренней сети во внешнюю (Интернет, электронная почта) осуществляется через компьютеры с установленными брандмауэром и антивирусом.

5.2. Запрещено несанкционированное использование модемов или иных средств доступа с ПК, подключенных к внутренней сети, во внешние сети.

5.3. Запрещено подключение различных мобильных устройств (личных телефонов, планшетов и других гаджетов) к сети WiFi.

5.4. Роутеры, точки доступа и прочее активное сетевое оборудование должны располагаться в местах по возможности исключающих свободный доступ.

#### **6. Антивирусная защита**

6.1. Антивирусная защита организуется посредством лицензионного антивирусного программного обеспечения. Работа без организации антивирусной защиты не допускается.

6.2. Обновление базы используемого антивирусного программного обеспечения осуществляется автоматически не реже 1 раза в день.

6.3. За своевременное обновление антивирусного программного обеспечения отвечает ответственный за информационную безопасность.



6.4.







