

УТВЕРЖДЕНО
Приказом директора МБУДО
«Детская художественная школа»
от _28.12.2024г. № 101-од

**Правила
организации работы по обеспечению информационной безопасности в
Муниципального бюджетного учреждения дополнительного образования
«Детская художественная школа»**

Оглавление

Раздел 1. Общие сведения об организации работы по обеспечению информационной безопасности в Школе.

Раздел 2. Нормативно-правовые основы обеспечения информационной безопасности Школы

Раздел 3. Деятельность Школы по обеспечению информационной безопасности обучающихся

Раздел 4. Деятельность по обеспечению информационной безопасности Школы. Программные и аппаратные средства защиты Информации

Раздел 1.

Общие сведения об организации работы по обеспечению информационной безопасности в Школе.

Термин «Информационная безопасность» при организации работы Муниципального бюджетного учреждения дополнительного образования «Детская художественная школа» (далее-Школа») используется для обозначения двух понятий:

1. Информационная безопасность – мероприятия Школы, направленные на предотвращение несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации вне зависимости от ее формы (электронная или физическая). (далее – Информационная безопасность Школы).

Основная задача при организации работы данного направления – обеспечение защиты разных видов информации: защита конфиденциальности, целостности и доступности данных с учетом целесообразности применения и без какого-либо ущерба для Школы.

2. Информационная безопасность – мероприятия Школы, направленные на обеспечение защиты детей от информации, причиняющей вред их здоровью и (или) физическому, психическому, духовному, нравственному развитию. (далее – Информационная безопасность обучающихся).

Основная задача при организации работы данного направления – формирование в Школе информационной среды, обеспечивающей целостность личности как активного социального субъекта и возможности развития в условиях информационного взаимодействия с окружающей средой, в том числе в информационно - телекоммуникационной сети Интернет.

Термин «Информационная образовательная среда» в контексте обеспечения информационной безопасности трактуется как «основанная на использовании компьютерной техники программно-телекоммуникационная среда, реализующая едиными технологическими средствами и взаимосвязанным содержательным наполнением качественное информационное обеспечение школьников, педагогов, родителей, сотрудников Школы, общественность».

Термин «Информационная среда» - часть образовательной среды Школы, являющаяся совокупностью следующих компонентов: продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, зрелищные мероприятия.

Информационная безопасность объектов и субъектов информационных отношений Школы, закрепленных в «Политике информационной безопасности Муниципального бюджетного учреждения дополнительного образования «Детская художественная школа», обеспечивается посредством организации мероприятий по следующим направлениям:

- обеспечение информационной защиты обучающихся школы;
- обеспечение информационной защиты данных, обрабатываемых с использованием автоматизированных информационных систем;
- обеспечение информационной защиты данных, обрабатываемых без использования автоматизированных информационных систем;

Локальные нормативные акты, регулирующие организацию работы Школы по каждому из направлений, разрабатываются отдельно.

Делопроизводство по каждому направлений формируется отдельно. В номенклатуре по каждому из направлений формируется отдельное дело.

Раздел 2.

Нормативные документы по обеспечению информационной безопасности

2.1. Нормативные документы по обеспечению информационной безопасности обучающихся

Федеральные законы РФ

Федеральный закон от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации».

Федеральный закон от 13.03.2006 № 38-ФЗ «О рекламе».

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности».

Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

Указы Президента РФ

Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации»

Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»

Постановления и распоряжения Правительства РФ

Концепция информационной безопасности детей. Утверждена распоряжением Правительства Российской Федерации от 2 декабря 2015 г. №2471-р.

Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

Постановление Правительства РФ от 21 марта 2012 г. N 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».

СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения общеобразовательных учреждениях».

Приказы Минкомсвязи России

Приказ Минкомсвязи России от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию».

Приказ Минкомсвязи России от 07.06.2019 № 261 «Об утверждении требований к подключению и доступу, включая требования к передаче данных, образовательных организаций, избирательных комиссий субъектов Российской Федерации и территориальных избирательных комиссий к единой сети передачи данных».

Документы рекомендательного характера

Письмо департамента государственной политики в сфере оценки качества общего образования, Минпросвещения России № 04-474 от 07.06.2019 «О методических рекомендациях».

Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети «Интернет», причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

Разработаны в рамках реализации пункта 7 приказа № 88 Минкомсвязи России 27 февраля 2018 года «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы» Временной комиссией Совета Федерации по развитию информационного общества, Министерством просвещения России, Министерством цифрового развития, связи и массовых коммуникаций России и Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Письмо Минкомсвязи России от 30.05.2019 № АВ-П17-062-11826 Методические рекомендации по основам информационной безопасности детей, находящихся в организациях отдыха детей и их оздоровления.

Письмо Департамента государственной политики в сфере общего образования Минпросвещения РФ № 03-39 от 29.03.2019 г. «О методических рекомендациях» Методические рекомендации по реализации мер, направленных на обеспечение безопасности и развития детей в сети «Интернет».

Письмо члена Совета Федерации Российской Федерации Боковой Л.Н. №66-02.41/ЛБ от 26.02.2019 г. Материалы в разделе «Проекты» сайта Еди-ный урок. Методические рекомендации по ограничению в образовательных организациях доступа обучающихся к видам информации, распространяемой посредством сети "Интернет", причиняющей вред здоровью и (или) развитию детей, а также не соответствующей задачам образования.

2.2. Нормативно-правовые основы обеспечения информационной безопасности Школы

Защита информации (общие вопросы)

- Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации».
- Положение «О государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», утвержденное Постановлением Совета Министров - Правительства РФ от 15 сентября 1993 года № 912-51.
- «Перечень сведений конфиденциального характера», утвержден указом Президента Российской Федерации № 188 от 6 марта 1997 года.
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждены приказом Гостехкомиссии России № 282 от 30 августа 2002 года.
- Постановление Правительства Российской Федерации от 3 ноября 1994 года № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».
- Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи

с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

Персональные данные

- Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных».
- Постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
- Положение «Об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации», утверждено постановлением Правительства Российской Федерации № 687 от 15 сентября 2008 года.
- Постановление Правительства Российской Федерации от 21 марта 2012 года № 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».
- Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Критически важные объекты

- Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
- Постановление Правительства Российской Федерации от 8 февраля 2018 года № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
- Приказ Федеральной службы по техническому и экспортному контролю от 21 декабря 2017 года № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».
- Приказ Федеральной службы по техническому и экспортному контролю от 22 декабря 2017 года № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

Государственные информационные системы

- Постановление Правительства Российской Федерации от 6 июля 2015 года № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».
- Постановление Правительства Российской Федерации от 7 августа 2019 года № 1026 «О применении пункта 19.1 Требований к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

- Приказ ФСТЭК России 11 февраля 2013 года № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

2.3. Нарушение правил защиты информации. КоАП РФ Статья 13.12.

Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), влечет наложение административного штрафа на граждан в размере от *одной тысячи пятисот до двух тысяч пятисот* рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от *двух тысяч пятисот до трех тысяч* рублей; на юридических лиц - от *двадцати тысяч до двадцати пяти тысяч рублей* с конфискацией несертифицированных средств защиты информации или без таковой.

Раздел 3.

Деятельность Школы по обеспечению информационной безопасности обучающихся

3.1. Информационная безопасность обучающихся – стратегическая задача по созданию в Школе условий для обеспечения защиты от распространения информации, причиняющей вред здоровью и (или) развитию.

Информационная безопасность обучающихся обеспечивается реализацией в Школе комплекса мер, сформированного в соответствии со следующими группами угроз:

- технологические угрозы, сопряженные с распространением вредоносных, шпионских программ, риском взлома защитных систем персонального компьютера;
- угрозы, связанные вредным или оскорбительным содержанием, с которым индивид сталкивается в сети Интернет;
- угрозы преследования обучающихся, включающие в себя любую форму нежелательных контактов, внимания, издевательства, насилия, связанные с коммуникацией в сети Интернет;
- угрозы, сопряженные с ситуацией раскрытия личной или конфиденциальной информации, персональных данных;
- угрозы, определяющие возникновение рисков социализации и негативных изменений в развитии личности детей и подростков, нанесение вреда их физическому и (или) психическому здоровью информацией, независимо от источника ее получения.

3.2. Комплекс мер по обеспечению информационной безопасности обучающихся:

- **правовая защита обучающихся**, заключающаяся в создании нормативно-правовой базы регулирования общественных отношений в области обеспечения информационной безопасности;
- **технологическая защита**, направленная на создание технических способов блокировки нежелательного контента, ограничения доступа к отрицательной информации, технические возможности осуществления родительского контроля за временем пребывания ребенка в сети и качественный анализ сайтов и интернет-сообществ, посещаемых детьми;
- **психолого-педагогическая защита**, направленная на формирование медиа и компьютерной грамотности обучающихся, стратегий поведения при встрече с нежелательным контентом и опасными знакомыми в сети Интернет, формирование критического мышления по отношению к информации, получаемой в сети и др.

3.3. Направления работы по обеспечению информационной безопасности обучающихся.

- для обучающихся дошкольного образования - меры по защите детей от негативного воздействия информации (формирование предпосылок информационной культуры, культуры безопасности).

- для обучающихся школьного возраста - меры по защите детей от негативного воздействия информации (формирование предпосылок информационной культуры, культуры безопасности); анализ привлекаемых для осуществления образовательной деятельности ресурсов, компонентов информационной среды Школы на предмет соответствия требованиям и критериям безопасности информации.

3.4. Порядок действий в целях реализации комплекса мер по обеспечению информационной безопасности обучающихся:

- Изучение руководителями Школы и преподавателями нормативно-правовых основ обеспечения информационной безопасности обучающихся. (Раздел 2).

- Разработка необходимых локальных актов по вопросам информационной безопасности в Школе.

- Проведение с родителями (законными представителями) обучающихся просветительской работы, нацеленной на повышение культуры информационной безопасности.

Раздел 4.

Деятельность по обеспечению информационной безопасности Школы. Средства защиты информации

В целях обеспечения информационной безопасности Школы применяются следующий группы средств защиты информации:

- физические средства защиты информации;
- организационные средства защиты информации;
- программные (в том числе криптографические).

Подбор технических мер защиты в Школе формируется на основе концепции и принципов информационной безопасности, закреплённой в Политике информационной безопасности Муниципального бюджетного учреждения дополнительного образования «Детская художественная школа»

Физические средства защиты информации (механические, электрические и электронные механизмы, которые функционируют независимо от информационных систем и создают препятствия для доступа к ним):

- замки, в том числе электронные;
- системы контроля и управления доступом;
- системы видеонаблюдения;

Организационные средства защиты информации:

- разработать правила, инструкции, регламентирующие действия по защите информации;
- исключить пребывание посторонних в местах, где обрабатывается конфиденциальная информация;
- располагать мониторы таким образом, чтобы исключить просмотр информации с них посторонними;

- всегда блокировать рабочие станции при оставлении рабочего места.

Программные средства защиты информации (программное обеспечение, предназначенные для решения задач, связанных с обеспечением информационной безопасности):

1. Средства операционных систем (далее – ОС);
2. Антивирусные программы.
3. Программы резервного копирования и восстановления данных.
4. Прикладные программы, в которых существует разграничение прав пользователей.
5. Криптографические средства защиты информации.

Прошито, пронумеровано и скреплено печатью
5 (пять) листов

Директор МБУДО

«Детская художественная школа»

Подпись / Л. В. Бельшева /

