

СОГЛАСОВАНО



Председатель ПК МАДОУ МО Динской
район «Детский сад № 10»

И.А. Логвиненко

УТВЕРЖДЕНО



Заведующий МАДОУ МО
Динской район «Детский сад № 10»

Л.А. Анпилова

Приказ № 13-ОД
от «01» 12 2020 г.

Положение об обеспечении информационной безопасности

1. Общие положения

- 1.1. Настоящее Положение об обеспечении информационной безопасности в **МАДОУ МО Динской район «Детский сад № 10»** (далее – Положение) определяет систему правовых, организационных и технических мероприятий, направленных на обеспечение информационной безопасности обучающихся и работников в **МАДОУ МО Динской район «Детский сад № 10»**
- 1.2. Положение разработано в соответствии с:
 - Федеральным законом от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
 - Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
 - Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных»;
 - Федеральным законом от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
 - Федеральным законом от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности»;
 - Доктриной информационной безопасности Российской Федерации, утв. Указом Президента РФ от 05.12.2016 № 646;
 - Концепцией информационной безопасности детей, утв. Распоряжением Правительства РФ от 02.12.2015 № 2471-р;
 - Приказом Департамента образования и науки Краснодарского края от 24.04.2012 года № 3325 «Об утверждении концепции информационной безопасности образовательных учреждений Краснодарского края»;
 - Порядком организации и осуществления образовательной деятельности по основным общеобразовательным программам – образовательным программам дошкольного образования, утвержденным приказом Минобрнауки от 30.08.2013 № 1014;
 - Порядком организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам, утвержденным приказом Минобрнауки от 29.08.2013 № 1008;
 - Порядком применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ, утв. приказом Минобрнауки от 23.08.2017 № 816;

- Приказом 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»;
- ГОСТ Р 53114-2008. Национальный стандарт Российской Федерации. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения, утв. и введен в действие Приказом Ростехрегулирования от 18.12.2008 № 532-ст;
- ГОСТ Р 52653-2006. Национальный стандарт Российской Федерации. Информационно-коммуникационные технологии в образовании. Термины и определения, утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 № 419-ст;
- ГОСТ Р 53620-2009. Национальный стандарт Российской Федерации. Информационно-коммуникационные технологии в образовании. Электронные образовательные ресурсы. Общие положения, утв. и введен в действие Приказом Ростехрегулирования от 15.12.2009 № 956-ст;
- Методическими материалами для обеспечения информационной безопасности детей при использовании ресурсов сети Интернет, направленными Письмом Минобрнауки России от 28.04.2014 № ДЛ-115/03;
- Методическими рекомендациями о размещении на информационных стендах, официальных интернет-сайтах и других информационных ресурсах общеобразовательных организаций и органов, осуществляющих управление в сфере образования, информации о безопасном поведении и использовании сети Интернет, направленными Письмом Минобрнауки России от 14.05.2018 № 08-1184;
- **Уставом МАДОУ МО Динской район «Детский сад № 10»**

1.1. В Положении используются следующие термины и определения:

- информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;
- доступ детей к информации - возможность получения и использования детьми свободно распространяемой информации;
- знак информационной продукции - графическое и (или) текстовое обозначение информационной продукции в соответствии с классификацией информационной продукции, предусмотренной частью 3 статьи 6 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- места, доступные для детей, - общественные места, доступ ребенка в которые и (или) нахождение ребенка в которых не запрещены, в том числе общественные места, в которых ребенок имеет доступ к продукции средств массовой информации и (или) размещаемой в информационно-телекоммуникационных сетях информационной продукции;
- информационная продукция - предназначенные для оборота на территории Российской Федерации продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, программы для электронных вычислительных машин (программы для ЭВМ) и базы данных, а также информация, распространяемая посредством зрелищных мероприятий, посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, и сетей подвижной радиотелефонной связи;

- информационная продукция для детей - информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей;
- информация, причиняющая вред здоровью и (или) развитию детей, - информация (в том числе содержащаяся в информационной продукции для детей), распространение которой среди детей запрещено или ограничено в соответствии с настоящим Федеральным законом;
- персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);
- оператор персональных данных (оператор) – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными;
- обработка персональных данных – действие (операция) или совокупность действий (операций) с персональными данными с использованием и без использования средств автоматизации, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение.

1.2. Система информационной безопасности является неотъемлемой частью системы комплексной безопасности **МАДОУ МО Динской район «Детский сад № 10»** (далее - Учреждение).

1.3. Функционирование системы информационной безопасности в Учреждении обеспечивается применением комплекса правовых, организационных и технических мер защиты, в результате чего снижается или исключается риск, связанный с причинением информационной продукцией, используемой в образовательном процессе, вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию несовершеннолетних обучающихся.

1.4. Использование сети Интернет в Учреждении в образовательной деятельности допускается только при условии применения административных и организационных мер, технических (программных, программно-аппаратных) средств защиты обучающихся от информации, не совместимой с задачами образования и воспитания, иной информации, распространение которой в Российской Федерации запрещено, информации, причиняющей вред здоровью и (или) развитию детей.

2. Основные цели и задачи функционирования системы информационной безопасности

2.1. Система информационной безопасности направлена на защиту единого информационного образовательного пространства Учреждения от незаконного проникновения, на предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в локальных сетях, а также недопущения доступа обучающихся и работников Учреждения к информации, которая запрещена или ограничена к распространению в Российской Федерации.

2.2. Система информационной безопасности Учреждения направлена на решение следующих задач:

- защита прав и законных интересов обучающихся в образовательной деятельности,

защита обучающихся от информации, причиняющей вред их здоровью и (или) развитию и (или) не соответствующей задачам образования;

- разграничение объемов и содержания информации, которая может быть доступна различным категориям пользователей;
- предотвращение утечки, хищения, утраты, подделки информации Учреждения;
- предотвращение несанкционированных действий по уничтожению модификации, искажению, копированию, блокированию информации Учреждения;
- предотвращение других форм незаконного вмешательства в информационные ресурсы Учреждения и его локальную сеть.

3. Организационно-административные меры, направленные на защиту детей от информации, причиняющей вред их здоровью и (или) развитию.

3.1. Приказом руководителя в Учреждении назначается лицо, ответственное за обеспечение информационной безопасности. В обязанности ответственного за обеспечение информационной безопасности в том числе входит:

- контроль функционирования системы контентной фильтрации;
- контроль функционирования антивирусной защиты, поддержание в актуальном состоянии антивирусных баз автоматической проверке ПК, локальной сети и внешних носителей на наличие вирусов;
- контроль соблюдения требований по обеспечению информационной безопасности при проведении технического обслуживания и ремонтных работ персональных компьютеров;
- оценка рисков информационной безопасности Учреждения;
- выявление угроз безопасности оборудованию и локальной сети Учреждения;
- проведение инструктажа работников Учреждения по правилам работы с используемыми аппаратно-программными средствами и осуществление контроля за действиями пользователей при работе с паролями, соблюдение порядка их смены, хранения и использования;
- информирование обучающихся, родителей несовершеннолетних обучающихся, работников Учреждения о порядке использования сети Интернет в Учреждении и контроль за использованием сети Интернет обучающимися и работниками.

3.1. В Учреждении разрабатываются и утверждаются локальные нормативные акты, регламентирующие:

- политику обработки персональных данных в учреждении, права и обязанности обучающихся и работников учреждения в сфере защиты персональных данных;
- порядок доступа и использования сети Интернет в Учреждении;
- организацию контроля использования сети Интернет в Учреждении;
- организацию контроля за библиотечным фондом Учреждения и предотвращение доступа обучающихся к информации экстремистского характера, к информации, запрещенной для распространения среди детей и (или) не соответствующей возрасту обучающихся.

3.2. В Учреждении оказывается организационная и методическая поддержка работникам в области безопасной работы с информационными ресурсами, информационными образовательными технологиями, в том числе, путем их направления на повышение квалификации по вопросам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, распространяемой посредством сети Интернет.

- 3.3. В Учреждении на регулярной основе осуществляется информирование работников, обучающихся и их родителей (законных представителей) об ответственности за нарушение требований законодательства Российской Федерации, локальных нормативных и организационно-распорядительных актов Учреждения по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети «Интернет».
- 3.4. В Учреждении разрабатывается, реализуется *и совершенствуется* комплекс мероприятий, направленный на правовое просвещение обучающихся и родителей (законных представителей) несовершеннолетних обучающихся в сфере информационной безопасности, на формирование навыков обучающихся безопасной работы в информационно-телекоммуникационных сетях.
- 3.5. Жалобы или претензии о нарушениях законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, включая несоответствие применяемых административных и организационных мер защиты детей от информации, причиняющей вред их здоровью и (или) развитию, установленным законодательством требованиям, а также о наличии доступа детей к информации, запрещенной для распространения среди детей, и направление мотивированного ответа о результатах рассмотрения таких обращений, жалоб или претензий рассматриваются руководством Учреждения в срок, не превышающий 10 (десяти) рабочих дней со дня получения.
- 3.6. В случае получения обращений, жалоб или претензий о наличии доступа детей к информации, запрещенной для распространения среди детей, установление причин и условий возникновения такого доступа и принятие мер по их устранению осуществляется руководством учреждения в срок, не превышающий 10 (десяти) дней.
- 3.7. Мониторинг осуществления организационно-административных мер, направленных на защиту детей от информации, причиняющей вред их здоровью и (или) развитию осуществляется заместителем руководителя по учебно-воспитательной работе в рамках своих полномочий.

4. Информация, используемая в образовательной деятельности и контроль за ее содержанием.

- 4.1. Информация и (или) информационная продукция, используемая в образовательной деятельности, осуществляемой в Учреждении, должна соответствовать требованиям законодательства Российской Федерации к защите детей от информации, причиняющей вред их здоровью и (или) развитию, соответствовать содержанию и задачам образования.
- 4.2. При осуществлении образовательной деятельности в Учреждении обеспечивается доступ обучающихся и работников к:
- печатной продукции, которая входит в библиотечный фонд Учреждения;
 - электронным образовательным ресурсам, прошедшим педагогическую экспертизу, рекомендованным и (или) сформированным органами государственной власти, осуществляющими управление в сфере образования, подведомственными им организациями; разработанными издательствами, выпускающими учебную литературу, учреждениями высшего и среднего образования, российскими библиотеками и иными уполномоченными или допущенными органами и организациями;
 - общедоступным государственным и региональным информационным системам;
 - информационно-телекоммуникационной сети Интернет в порядке, установленном локальным нормативным актом Учреждения.

- 4.3. В работе и (или) общении с обучающимися Учреждения педагогическим работникам или иным работникам Учреждения не допускается использовать информацию:
- которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иную информацию, за распространение которой предусмотрена уголовная или административная ответственность;
 - запрещенную для распространения среди детей в соответствии со ст.5 Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
 - имеющую знак информационной продукции, не соответствующий возрасту обучающегося (обучающихся);
 - полученную с нарушением авторских или смежных прав;
 - имеющую конфиденциальный характер в соответствии с действующим законодательством и (или) локальными нормативными актами Учреждения.
- 4.4. Мониторинг содержания информационной продукции, используемой в образовательной деятельности педагогических работников осуществляется предметными методическими объединениями, а также администрацией Учреждения в рамках внутришкольного контроля.
- 4.5. В образовательной и (или) досуговой деятельности с обучающимися Учреждения, организуемой его работниками, не допускается посещения зрелищных или иных мероприятий, билеты на которые (афиши или иная информация о мероприятии) содержат знак информационной продукции, не соответствующий возрасту обучающегося (обучающихся).
- 4.6. В Учреждении осуществляется административный контроль за соблюдением возрастной классификации информационной продукции, приобретаемой и (или) используемой в образовательной и (или) досуговой деятельности Учреждения.
- 4.7. В процессе осуществления образовательной деятельности с использованием информационно-компьютерных технологий педагогическими работниками осуществляется контроль за использованием обучающимися сети Интернет, в том числе, визуальный контроль.
- 4.8. При обнаружении угроз информационной безопасности Учреждения, несанкционированного доступа к локальной сети Учреждения, а также обнаружении доступа к ресурсу, содержание которого может нанести вред здоровью и (или) развитию обучающихся, работники Учреждения обязаны незамедлительно сообщить об этом руководству Учреждения для принятия соответствующих мер.
- 4.9. Работник, ответственный за обеспечение информационной безопасности, при получении информации, указанной в п. 4.8. настоящего Положения незамедлительно:
- устанавливает обстоятельства получения доступа к ресурсу сети Интернет, содержащему информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей;
 - идентифицирует ресурс сети Интернет;
 - в течение одного рабочего дня с момента получения информации, указанной в п.4.8. настоящего Положения, проводит мероприятия, направленные на ограничение доступа к ресурсу сети Интернет, содержащему информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей (вносит изменения в политики доступа, применяемые в технических средствах

контентной фильтрации, вносит изменения в конфигурацию технических средств контентной фильтрации, в случае необходимости предпринимает другие меры).

- проводит анализ обстоятельств, послуживших причиной доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей.

- вносит руководителю Учреждения на основе проведенного анализа предложения по совершенствованию системы контентной фильтрации в целях минимизации количества инцидентов, связанных с получением доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей.

4.10. В порядке реагирования на инцидент, угрожающий информационной безопасности учреждения и (или) обучающихся и работников Учреждения, руководством может быть направлено соответствующее сообщение о наличии на страницах сайтов в сети Интернет информации, распространение которой в Российской Федерации запрещено в Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций, а также в органы внутренних дел.

5. Организационно-технические мероприятия по формированию безопасных условий доступа обучающихся к ресурсам сети Интернет

5.1. К техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию, применяемым при предоставлении доступа к информации, распространяемой посредством сети Интернет, относятся:

- средства ограничения доступа к техническим средствам доступа к сети Интернет;
- средства ограничения доступа к сети Интернет с технических средств третьих лиц;
- средства ограничения доступа к запрещенной для распространения среди детей информации, размещенной на сайтах в сети Интернет.

5.2. В Учреждении обеспечивается антивирусная защита компьютерной техники, систематически проводится обновление антивирусных программ.

5.3. Для приобретения и использования программного обеспечения в образовательной и иной деятельности Учреждения проводится проверка его подлинности.

5.4. В Учреждении с установленной периодичностью осуществляется контроль:

- эксплуатации технических средств контентной фильтрации – постоянно;
- функционирования технических средств контентной фильтрации и их конфигурации – не реже 2 раз в год;
- организации доступа к сети Интернет в целях исключения возможности несанкционированного использования сети Интернет в Учреждении – постоянно;
- функционирования технических средств, применяемых при организации доступа к сети Интернет, и их конфигурации (компьютерное оборудование, сетевое оборудование, системное и прикладное программное обеспечение) – не реже 2 раз в год;
- изменения конфигурации технических средств, применяемых при организации доступа к сети Интернет, контроль наличия в их составе аппаратных, программных средств, предназначенных для нарушения функционирования технических средств контентной фильтрации – не реже 2 раз в год;
- ведения журналов регистрации посещений ресурсов сети Интернет – не реже 1 раза в месяц;

- функционирования системы антивирусной защиты – не реже 1 раза в месяц;
- наличия доступа к ресурсам сети Интернет, содержащим информацию, не совместимую с задачами образования и воспитания, иную информацию, распространение которой в Российской Федерации запрещено, информацию, причиняющую вред здоровью и (или) развитию детей, путем осуществления попыток получения доступа к таким ресурсам сети Интернет – не реже 1 раза в квартал.

- 5.5. В учреждении не допускается обучающимися и работниками, а также иными лицами самовольная установка программного обеспечения на компьютерную технику Учреждения, либо использование не принадлежащих Учреждению программ и оборудования.
- 5.6. Мониторинг осуществления организационно-технических мер, направленных на обеспечение информационной безопасности учреждения осуществляется заместителем руководителя Учреждения по ресурсам в рамках своих полномочий.

6. Обучение и просвещение в сфере информационной безопасности

- 6.1. В рамках образовательной деятельности в Учреждении осуществляется обучение безопасным способам работы в информационно-телекоммуникационных сетях, в план воспитательной работы Учреждения включаются мероприятия, направленные на повышение медиаграмотности обучающихся, формированию навыков безопасного поведения в сети Интернет.
- 6.2. В учреждении проводятся образовательные и консультационные мероприятия с родителями обучающихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в сеть Интернет.
- 6.3. На информационных стендах, расположенных в Учреждении и в кабинетах, оснащенных персональными устройствами для выхода в сеть Интернет, размещаются информационные памятки, содержащие основные советы по обеспечению информационной безопасности учащихся.
- 6.4. На официальном сайте Учреждения размещается специализированный раздел «*Информационная безопасность*», в рамках которого предусмотрено размещение локальных нормативных актов в сфере обеспечения информационной безопасности обучающихся, нормативно-правовых документов, регламентирующих обеспечение информационной безопасности несовершеннолетних, методические рекомендации, информационные памятки для работников, обучающихся и их родителей, направленные на повышение информационной грамотности и обеспечение информационной безопасности детей.

7. Заключительные положения

- 7.1. Положение вступает в силу с момента его утверждения приказом руководителя Учреждения.
- 7.2. Положение отменяется или изменяется в случае изменения действующего законодательства, а также при наличии иных нормативно-правовых оснований, влекущих изменение, дополнение или отмену закрепленных в нем положений.
- 7.3. Положение размещается на информационных стендах Учреждения и на официальном сайте Учреждения в сети Интернет.