Приложение

к приказу отдела образования

Администрации Пограничного

муниципального округа

от 26.02.2021 № 27

**Положение**

**об обеспечении информационной безопасности в образовательных организациях Пограничного муниципального округа**

1. Общие положения.
   1. Настоящее Положение об обеспечении информационной безопасности в образовательных организациях Пограничного муниципального округа (далее - Положение) определяет систему правовых, организационных и технических мероприятий, направленных на обеспечение информационной безопасности обучающихся и работников образовательных организаций.
   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»;

- Концепцией информационной безопасности детей, утвержденной Распоряжением Правительства РФ от 02.12.2015 №2471-р;

- Порядком применения организациями, осуществляющими образовательную деятельность, электронного обучения, дистанционных образовательных технологий при реализации образовательных программ, утвержденным 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».

1.3. Для целей и задач настоящего Положения используются следующие понятия:

* + 1. информационная безопасность детей - состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию;
    2. доступ детей к информации - возможность получения и использования детьми свободно распространяемой информации;
    3. 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»;
    4. 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;
    5. информационная продукция для детей - информационная продукция, соответствующая по тематике, содержанию и художественному оформлению физическому, психическому, духовному и нравственному развитию детей;
    6. 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;
    7. персональные данные - любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);
    8. 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;
    9. 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.

**2. Система информационной безопасности**

* 1. Система информационной безопасности является неотъемлемой частью системы комплексной безопасности в образовательных организациях (далее ОО).
  2. Функционирование системы информационной безопасности в ОО обеспечивается применением комплекса правовых, организационных и технических мер защиты, в результате чего снижается или исключается риск, связанный с причинением информационной продукцией, используемой в образовательной деятельности, вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию несовершеннолетних обучающихся.
  3. Использование сети Интернет 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.

1. Основные цели и задачи функционирования системы информационной безопасности.
   1. Система информационной безопасности направлена на защиту единого информационного образовательного пространства ОО 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. Система информационной безопасности ОО направлена на решение следующих задач:
      1. 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;
      2. разграничение объемов и содержания информации, которая может быть доступна различным категориям пользователей;
      3. предотвращение утечки, хищения, утраты, подделки информации ОО;
      4. предотвращение несанкционированных действий по уничтожению модификации, искажению, копированию, блокированию информации учреждения;
      5. предотвращение других форм незаконного вмешательства в информационные ресурсы ОО и его локальную сеть.
2. Организационно-административные меры, направленные на защиту детей от информации, причиняющей вред их здоровью и (или) развитию.
   1. Приказом директора образовательной организации назначается лицо, ответственное за обеспечение информационной безопасности. В обязанности ответственного за обеспечение информационной безопасности в том числе входит:

4.1.1. контроль функционирования антивирусной защиты, поддержание в актуальном состоянии антивирусных баз автоматической проверке ПК, локальной сети и внешних носителей на наличие вирусов;

4.1.2. контроль соблюдения требований по обеспечению информационной безопасности при проведении технического обслуживания и ремонтных работ персональных компьютеров;

4.1.3. оценка рисков информационной безопасности учреждения;

4.1.4. выявление угроз безопасности оборудованию и локальной сети ОО;

4.1.5. проведение инструктажа работников ОО 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;

4.1.6. информирование обучающихся, родителей несовершеннолетних обучающихся, работников ОО о порядке использования сети Интернет и контроль за использованием сети Интернет обучающимися и работниками;

4.1.7. разработка и утверждение локальные нормативных актов регламентирующих:

- политику обработки персональных данных,

- права и обязанности обучающихся и работников Школы в сфере защиты персональных данных;

- порядок доступа и использования сети Интернет в Школе;

- организацию контроля использования сети Интернет в Школе;

- организацию контроля за библиотечным фондом и предотвращение доступа обучающихся к информации экстремистского характера, к информации, запрещенной для распространения среди детей и (или) не соответствующей возрасту обучающихся.

* 1. В ОО 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.
  2. В ОО 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 ОО по вопросам обеспечения информационной безопасности обучающихся при организации доступа к сети Интернет.
  3. В ОО 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.
  4. 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 ОО в срок, не превышающий 7 (семи) рабочих дней со дня получения.
  5. 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 ОО незамедлительно.
  6. Мониторинг осуществления организационно-административных мер, направленных на защиту детей от информации, причиняющей вред их здоровью и (или) развитию осуществляется лицом, ответственным за обеспечение информационной безопасности.

1. Информация, используемая в образовательной деятельности и контроль за ее

содержанием.

* 1. Информация и (или) информационная продукция, используемая в образовательной деятельности, осуществляемой в ОО, должна соответствовать требованиям законодательства Российской Федерации к защите детей от информации, причиняющей вред их здоровью и (или) развитию, соответствовать содержанию и задачам образования.
  2. При осуществлении образовательной деятельности в ОО обеспечивается доступ обучающихся и работников к:

- печатной продукции, которая входит в библиотечный фонд ОО;

- электронным образовательным ресурсам, прошедшим педагогическую экспертизу, рекомендованным и (или) сформированным органами государственной власти, осуществляющими управление в сфере образования, подведомственными им организациями; разработанным 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 ОО.

* 1. В ОО осуществляется административный контроль за соблюдением возрастной классификации информационной продукции, приобретаемой и (или) используемой в образовательной и (или) досуговой деятельности.
  2. В процессе осуществления образовательной деятельности с использованием информационно-компьютерных технологий педагогическими работниками осуществляется контроль за использованием обучающимися сети Интернет, в том числе визуальный контроль.
  3. При обнаружении угроз информационной безопасности ОО, несанкционированного доступа к локальной сети, а также обнаружении доступа к ресурсу, содержание которого может нанести вред здоровью и (или) развитию обучающихся, работники ОО обязаны незамедлительно сообщить об этом руководству для принятия соответствующих мер.

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

* 1. В ОО обеспечивается антивирусная защита компьютерной техники, систематически проводится обновление антивирусных программ.
  2. Для приобретения и использования программного обеспечения в образовательной и иной деятельности ОО проводится проверка его подлинности.

1. Обучение и просвещение в сфере информационной безопасности.
   1. В рамках образовательной деятельности в ОО осуществляется обучение безопасным способам работы в информационно-телекоммуникационных сетях, в план воспитательной работы ОО включаются мероприятия, направленные на повышение медиаграмотности обучающихся, формированию навыков безопасного поведения в сети Интернет.
   2. В ОО проводятся образовательные и консультационные мероприятия с родителями обучающихся с целью объяснения правил, рисков предоставления детям средств связи с выходом в сеть Интернет.
   3. На информационных стендах, расположенных в ОО, и в кабинетах, оснащенных персональными устройствами для выхода в сеть Интернет, размещаются информационные памятки, содержащие основные советы по обеспечению информационной безопасности обучающихся.