Приложение№1 к приказу ГОУ СПО ЛНР «МАК»

от 01.12.2023 №172

**ПОЛОЖЕНИЕ**

**ОБ ОБЩЕСТВЕННОМ КОНТРОЛЕ ОБЕСПЕЧЕНИЯ**

**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ**

**ГОУ СПО ЛНР «МАРКОВСКИЙ АГРАРНЫЙ КОЛЛЕДЖ»**

# Общие положения

* 1. Настоящее Положение разработано на основании следующих документов:
* «Конвенция о правах ребенка» (одобрена Генеральной Ассамблеей ООН 20.11.1989) (вступила в силу для СССР 15.09.1990);
* Федеральный закон от 24.07.1998 № 124 «Об основных гарантиях прав ребенка в Российской Федерации»;
* Федеральный закон от 25.07.2002 N 114 –ФЗ «О противодействии экстремисткой деятельности»;
* Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
* Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» и все его изменения;
* Федеральный закон от 01.05.2019 № 93-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации»;
* концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 02.12.2015 № 2471-p;
* методические рекомендации Совета Федерации Федерального собрания Российской Федерации 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;
* приказ Департамента образования и молодёжной политики XMAO — Югры от 19.08.2013 № 798 «О контроле за Интернет-ресурсами, используемыми в деятельности образовательными учреждениями».
  1. Настоящие положение разработано с целью ограничения доступа в МБОУ СОШ №44 (далее — общеобразовательное учреждения) к информации, причиняющей вред здоровью и (или) развитию обучающихся, а также не соответствующей целям и задачам образования.
  2. Все обязанности по обеспечению эффективного функционирования средств контентной фильтрации (далее — СКФ) регулируются локальными нормативными актами общеобразовательного учреждения (приказами, положением и должностным инструкциями, утвержденными директором общеобразовательного учреждения).
  3. Ознакомление с положением и его соблюдение обязательно для всех сотрудников общеобразовательного учреждения.
  4. Срок действия данного Положения не ограничен. Положение действует до принятия нового.

# Обязанности директора и сотрудников общеобразовательного учреждения по обеспечению информационной безопасности обучающихся

**при работе в сети «Интернет»**

* 1. Директор общеобразовательного учреждения:
     + осуществляет общее управление по организации КФ в общеобразовательном учреждении;
     + устанавливает правила по ограничению физического доступа обучающихся к автоматизированным рабочим местам (далее — APM) педагогов и сотрудников образовательной организации (например: запретить нахождение обучающихся в кабинетах на перемене в отсутствии сотрудника общеобразовательного учреждения, где есть APM с выходом в сеть «Интернет»);
     + назначает заместителя директора, ответственного за организацию и обеспечение информационной безопасности в общеобразовательном учреждении;
     + назначает специалиста, ответственного за техническое сопровождение СКФ ресурсов сети «Интернет»;
     + принимает решение о создании совета по обеспечению информационной безопасности обучающихся (далее — Совет) и утверждает его состав;
     + разрабатывает план мероприятий общеобразовательного учреждения по обеспечению информационной безопасности обучающихся при работе в сети

«Интернет» на 2023-2024 годы (далее — План мероприятий) на основании примерного плана мероприятий по обеспечению информационной безопасности обучающихся пpи работе в сети «Интернет» на 2023-2024 годы;

* + - несет полную ответственность за качественное выполнение Плана мероприятий.
* Ответственный заместитель директора общеобразовательного учреждения:
* исполняет План мероприятий;
* контролирует деятельность сотрудников общеобразовательного учреждения, в том числе технического специалиста по исполнению Плана мероприятий;
* принимает решение о разрешении/блокировании доступа к определённым ресурсам и (или) категориям ресурсов сети «Интернет»;
* осуществляет хранение в сейфе логинов и паролей, установленных па операционную систему и программу, осуществляющую КФ на персональных компьютерах обучающихся, и предоставляет их сотрудникам MAУ «ИМЦ» для выполнения функциональных обязанностей.
  1. Технический специалист:
     + исполняет План мероприятий;
     + принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательной деятельности.
  2. Совет по обеспечению информационной безопасности обучающихся:
     + принимает участие в реализации Плана мероприятий. 2.4. Сотрудники общеобразовательного учреждения:
     + соблюдают в своей профессиональной деятельности законодательство РФ в области информационный безопасности, в том числе КФ при работе с обучающимися в сети «Интернет»;
     + исполняют План мероприятий;
     + принимают меры по пресечению обращений обучающихся к ресурсам, не имеющим отношения к образовательной деятельности.

1. **Сотрудникам общеобразовательного учреждения разрешается:**

- отключать СКФ на своих персональных устройствах или устройствах, предоставленных педагогическому работнику, только после осуществления образовательной деятельности и отсутствия обучающихся на территории общеобразовательного учреждения, а также получения письменного согласия от директора или заместителя директора общеобразовательного учреждения с указанием или пояснением целей отключения СКФ и временных сроках отключения СКФ с занесением информации в журнал работы КФ.

1. **Сотрудникам общеобразовательного учреждения запрещается:**
   1. При работе на автоматизированном рабочем месте:
      * работать в сети «Интернет», без прохождения соответствующего инструктажа;
      * подключать оборудование, проводить настройку сети и СКФ самостоятельно (кроме технического специалиста, отвеивающего за техническое сопровождение СКФ ресурсов сети «Интернет»);
      * отключать СКФ во время нахождения на территории общеобразовательного учреждения обучающихся;
      * использовать поисковые системы Yandex, Google, Rambler, Mail.ru и т.д., кроме поисковых систем сервиса ООО «СкайДНС», http://seareh.skydns.ru;
      * обращаться к ресурсам, содержание и тематика которых не допустимы для несовершеннолетних и/или нарушают законодательство Российской.

Федерации (эротика, порнография, пропаганда насилия, терроризма, политического или религиозного экстремизма, национальной, расовой и т.п. розни, иные ресурсы схожей направленности);

* + - осуществлять любые сделки через сеть «Интернет»;
    - загружать и запускать исполняемые либо иные файлы без предварительной проверки на наличие вирусов установленным антивирусным пакетом;
    - распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы;
    - загружать и распространять:
      * материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности компьютерного или телекоммуникационного оборудования;
        + программы, для осуществления несанкционированного доступа, серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети

«Интернет», а также размещать ссылки на вышеуказанную информацию;

* + - пользоваться чужими учетными данными при использовании сетевых сервисов, предполагающих авторизацию.
  1. Работать на своих персональных (личных) устройствах без СКФ в присутствии обучающихся на территории общеобразовательного учреждения.