

КЪЭБОРДЕЙ-БАЛЪКЪОР РЕСПУБЛИКЭМ
И ШЭДЖЭМ КУЕЙМ
И АДМИНИСТРАЦЭМ ПЦЭНЫГЪЭ
ІУЭХУХЭМКІЭ МУНИЦИПАЛЬНЭ
КІЭЗОНЭ ІУЭХУЩІАПІЭ

КЪАБАРТЫ-МАЛЪАР РЕСПУБЛИКАНЫ
МУНИЦИПАЛ КАЗНА УЧРЕЖДЕНИЯСЫ
«ЧЕГЕМ РАЙОННУ ЖЕР ЖЕРЛИ
АДМИНИСТРАЦИЯСЫНЫ ИЛМУ БИЛИМ
БЕРІУ УПРАВЛЕНИЯСЫ»

Министерство образования и науки КБР
Управление образования Чегемского муниципального района
Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа №2 им. Инала Пшибиева» с. п.Нартан

Адрес: с.п. Нартан ул. им. Али Тухужева,1 тел./факс (86630) 9-74-98, email: elbrusnartan@yandex.ru

Принят
на педагогическом совете
Протокол № 1
от 30.08.2018 г.

Утверждаю
Директор
А.А.Кунижев
Приказ № 314/1
от 31.08.2018 г.



ПРОГРАММА

ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ
СРЕДЫ В МКОУ «СОШ №2 ИМЕНИ ИНАЛА ПШИБИЕВА»
с.п.НАРТАН «БЕЗОПАСНЫЙ ИНТЕРНЕТ В ШКОЛЕ»

Содержание программы

1	ПАСПОРТ ПРОГРАММЫ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СРЕДЫ В МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан «Безопасный интернет в школе»	3-5
2	Пояснительная записка	5-6
3	Программа по обеспечению безопасной информационной среды в школе «Безопасный интернет в школе»	6-11
4	Перечень приложений .	12
5	Приложение 1. План мероприятий по обеспечению информационной безопасности обучающихся МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан	13-15
6	Приложение 2. Документы школы, связанные с работой в сети Интернет	16
7	Приложение 3.РЕГЛАМЕНТ работы МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан в сети Интернет	17-19
8	ПОЛОЖЕНИЕ об использовании сети Интернет в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан	20-23
9	Приложение 5.ПОЛОЖЕНИЕ об информационной доступности МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан»	24-26
10	Приложение 6.ПОЛОЖЕНИЕ о сайте муниципального общеобразовательного учреждения «СОШ №2 имени Инала Пшибиева» с.п.Нартан	27-30
11	Приложение 7. ИНСТРУКЦИЯ для педагогических сотрудников о порядке действий при осуществлении контроля за использованием учащимися муниципального общеобразовательного учреждения «СОШ №2 имени Инала Пшибиева» с.п.Нартан сети Интернет;	31-32
12	Приложение 8.Порядок доступа педагогических работников к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности	33-35
13	Приложение 9.КЛАССИФИКАТОР информации, не имеющей отношения к образовательному процессу	36-42
14	Приложение 10. Регламент работы с электронной почтой в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан	43-45
15	Инструкция по организации антивирусной защиты в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан	46-48
16	Приложение 11.ПОЛОЖЕНИЕ об электронном журнале успеваемости/электронном дневнике учащегося в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан	49-50
17	Приложение 12. Методические рекомендации «Безопасный Интернет»	51
18	Приложение 13. Памятка родителям по управлению безопасностью детей в интернете	52-56
19	Приложение 14. Памятка для детей по безопасному поведению в интернете	56-63

ПАСПОРТ ПРОГРАММЫ

<p>Наименование программы</p>	<p>ПРОГРАММА ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОЙ ИНФОРМАЦИОННОЙ СРЕДЫ В МКОУ «СОШ №2 ИМЕНИ ИНАЛА ПШИБИЕВА» с.п.НАРТАН «БЕЗОПАСНЫЙ ИНТЕРНЕТ В ШКОЛЕ»</p>
<p>Нормативно-правовая база программы</p>	<ul style="list-style-type: none"> • Федеральный закон «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ; • Федеральный закон Российской Федерации от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»; • Федеральный закон Российской Федерации от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»; • Федеральный закон от 27.07.2006 №152 «О персональных данных»; • «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» СанПин 2.4.2.2821-10 с изменениями и дополнениями от 29 июня 2011 г., 25 декабря 2013 г., 24 ноября 2015 г. • Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р»
<p>Материально-техническое обеспечение учебной деятельности</p>	<p>В школе созданы условия для всех участников образовательной деятельности:</p> <ul style="list-style-type: none"> • компьютерный класс (24 посадочных места): 12 компьютеров • 15 учебных кабинетов оборудованы мультимедийными комплектами; • из них 13 кабинетов оборудованы интерактивными досками в комплекте; • имеется выход в Интернет; • все компьютеры, используемые в учебном процессе, подключены к Интернету; • 4 компьютера, используемые в работе администрации, подключены к Интернету; • функционируют 9 МФУ; • создан и функционирует официальный сайт школы; • создан и функционирует электронный журнал школы.
<p>Цели и задачи программы</p>	<p>Цели программы:</p> <ul style="list-style-type: none"> • Обеспечение гармоничного развития молодого поколения при условии минимизации всех негативных факторов, связанных с формированием гипер информационного общества в России. • Формирование безопасной информационной

	<p>образовательной среды в школе, обеспечение информационной безопасности учащихся, использующих Интернет в образовании и пропаганда безопасного поведения в сети Интернет.</p> <p>Задачи программы:</p> <ul style="list-style-type: none"> • формирование у детей навыков самостоятельного и ответственного потребления информационной продукции; • повышение уровня медиаграмотности детей; • формирование у детей позитивной картины мира и адекватных базисных представлений об окружающем мире и человеке; • ценностное, моральное и нравственно-этическое развитие детей; <p>формирование и расширение компетентностей работников образования в области медиабезопасного поведения детей и подростков;</p> <ul style="list-style-type: none"> • формирование информационной культуры как фактора обеспечения информационной безопасности; • изучение нормативно-правовых документов по вопросам защиты детей от информации, причиняющей вред их здоровью и развитию; • формирование знаний в области безопасности детей, использующих Интернет; • организация просветительской работы с родителями и общественностью; • организация технического контроля безопасности.
<p>Основные направления программы</p>	<ul style="list-style-type: none"> • Разработка и внедрение эффективной модели организации процесса информатизации, включающей информационно-методическое, кадровое и материально-техническое обеспечение. • Формирование и апробация инновационных подходов к информатизации школы. • Оснащение школы современными электронными учебными материалами. • Подготовка педагогических кадров к освоению и эффективному внедрению информационных и коммуникационных технологий в образовательный процесс. • Обеспечение школы средствами информационных и коммуникационных технологий.
<p>Планируемые результаты реализации программы</p>	<p>Системный подход в решении задач построения в школе безопасной среды для доступа к сети Интернет:</p> <ul style="list-style-type: none"> • обеспечит потребность учителя в постоянном повышении уровня своей квалификации и профессионализма по данному вопросу; • поможет родителям грамотно организовать информационное пространство ребенка в семье; • совместные усилия педагогов и родителей создадут рабочую среду ребенка и в школе, и дома с учетом

	<p>его интересов, сообразно возрастным особенностям и духовным потребностям в рамках общечеловеческих ценностей. Будет создана новая медиасреда, соответствующая следующим характеристикам:</p> <ul style="list-style-type: none"> • наличие развитых информационно-коммуникационных механизмов, направленных на социализацию молодого поколения и раскрытие его творческого потенциала; • свободный доступ детей к историко-культурному наследию предшествующих поколений; • качественный рост уровня медиаграмотности детей; • увеличение числа детей, разделяющих ценности патриотизма; • гармонизация меж- и внутрипоколенческих отношений; • популяризация здорового образа жизни среди молодого поколения; • формирование среди детей устойчивого спроса на получение высококачественных информационных продуктов; • снижение уровня противоправного и преступного поведения среди детей; • формирование у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования "пиратского" контента. (Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р»)
Возможные риски	<ul style="list-style-type: none"> • Запрет доступа к негативной информации формирует у ребенка желание получить эту информацию.

1. Пояснительная записка

Проблема обеспечения информационной безопасности детей в информационно-телекоммуникационных сетях становится все более актуальной в связи с существенным возрастанием численности несовершеннолетних пользователей. В современных условиях развития общества компьютер стал для ребенка и «другом» и «помощником» и даже «воспитателем», «учителем».

Всеобщая информатизация и доступный, высокоскоростной Интернет уравнил жителей больших городов и малых деревень в возможности получить качественное образование и стал неотъемлемой частью нашей повседневной жизни.

Использование Интернета в образовательных учреждениях и дома расширяет информационное образовательное пространство обучающего и позволяет повысить эффективность обучения. Доступ обучающихся к информационным ресурсам сети Интернет дает возможность школьникам пользоваться основным и дополнительным учебным материалом, необходимым для обучения в школе, выполнять домашние задания, самостоятельного обучаться. Благодаря таким ресурсам у школьников появляется возможность узнавать о проводимых олимпиадах, конкурсах, и принимать в них активное участие. Использование Интернета в работе с детьми и в работе школы достаточно обширно:

- это использование электронной почты;
- поиск в сети нужной информации; - создание собственных школьных веб-страниц;
- рассылка и/или съем материалов (нормативных документов, информации о семинарах и конкурсах и т.п.);
- обмен опытом;
- ответы на типичные вопросы;
- получение ("скачивание") небольших обучающих программ по разным предметам;
- участие в различных интернет-проектах, конкурсах, акциях.

Однако использование Интернета в образовательной деятельности таит в себе много опасностей, существует ряд аспектов, негативно влияющих на физическое, моральное, духовное здоровье подрастающего поколения, порождающих проблемы в поведении у психически неустойчивых школьников, представляющих для детей угрозу. Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие опасности подстерегают их в сети и как их избежать. Важно, чтобы во всех школах был безопасный Интернет. По статистическим данным на сегодняшний день в России насчитывается от 8 до 10 млн. интернет-пользователей в возрасте до 14 лет. Две трети детей выходят в глобальную сеть самостоятельно, без присмотра родителей и педагогов. Примерно 40% школьников посещают веб-страницы нежелательного и запрещенного содержания. У многих развивается интернет-зависимость и игромания.

Обеспечение государством информационной безопасности детей, защита их физического, умственного и нравственного развития во всех аудиовизуальных медиа-услугах и

электронных СМИ – требование международного права (Рекомендации Европейского Парламента и Совета ЕС от 20.12.2006 о защите несовершеннолетних и человеческого достоинства в Интернете, Решение Европейского парламента и Совета № 276/1999/ЕС о принятии долгосрочного плана действий Сообщества по содействию безопасному использованию Интернета посредством борьбы с незаконным и вредоносного содержимого в рамках глобальных сетей).

2. Программа по обеспечению безопасной информационной среды «Безопасный Интернет в школе»

Согласно российскому законодательству информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию (Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"). Преодолеть нежелательное воздействие компьютера возможно только совместными усилиями учителей, родителей и самих школьников. Согласно Концепции информационной безопасности детей, утвержденной распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р», обеспечение информационной безопасности должно строиться на следующих принципах:

- признание детей равноправными участниками процесса формирования информационного общества в Российской Федерации;
- ответственность государства за соблюдение законных интересов детей в информационной сфере;
- необходимость формирования у детей умения ориентироваться в современной информационной среде;
- воспитание у детей навыков самостоятельного и критического мышления;
- развитие государственно-частного партнерства в целях обеспечения законных интересов детей в информационной среде;
- повышение эффективности сотрудничества представителей средств массовой информации и массовых коммуникаций и государственных органов в интересах защиты детей от информации, способной причинить вред их здоровью и развитию;
- обучение детей медиаграмотности;
- поддержка творческой деятельности детей в целях их самореализации в информационной среде;
- создание условий для формирования в информационной среде благоприятной атмосферы для детей вне зависимости от их социального положения, религиозной и этнической принадлежности;
- взаимодействие различных ведомств при реализации стратегий и программ в части, касающейся обеспечения информационной безопасности детей;
- обеспечение широкого доступа детей к историческому и культурному наследию России через использование современных средств массовых коммуникаций;
- открытость и взаимодействие с другой информационной культурой и традициями, формирование у детей объективного представления о российской культуре как неотъемлемой части мировой цивилизации.

Работа с обучающимися должна вестись в зависимости от возрастных особенностей: начальное звено (1-4 классы), среднее (5-9 классы), старшее звено(10-11 классы).

На каждом этапе необходимы специальные формы и методы обучения в соответствии с возрастными особенностями. Для организации безопасного доступа к сети Интернет в МКОУ «Сош №2 имени Инала Пшибиева»с.п.Нартан созданы следующие условия:

1. В образовательном учреждении разработаны и утверждены:
 - РЕГЛАМЕНТ работы в сети Интернет в МКОУ «Сош №2 имени Инала Пшибиева»с.п.Нартан ;
 - ПОЛОЖЕНИЕ об использовании сети Интернет в МКОУ «Сош №2 имени Инала Пшибиева»с.п.Нартан ;
 - ПОЛОЖЕНИЕ об информационной открытости «Сош №2 имени Инала Пшибиева»с.п.Нартан ;
 - ПОЛОЖЕНИЕ о сайте муниципального казенного общеобразовательного учреждения «Сош №2 имени Инала Пшибиева»с.п.Нартан;
 - ИНСТРУКЦИЯ для педагогических сотрудников о порядке действий при осуществлении контроля за использованием учащимися муниципального казенного общеобразовательного учреждения «Сош №2 имени Инала Пшибиева»с.п.Нартан в сети Интернет;
 - Порядок доступа педагогических работников к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности;
 - КЛАССИФИКАТОР информации, не имеющей отношения к образовательному процессу;
 - Регламент работы с электронной почтой в МКОУ «Сош №2 имени Инала Пшибиева»с.п.Нартан ;
 - Инструкция по организации антивирусной защиты в МКОУ «Сош №2 имени Инала Пшибиева»с.п.Нартан ;
 - ПОЛОЖЕНИЕ об электронном журнале успеваемости/электронном дневнике учащегося в МКОУ «Сош №2 имени Инала Пшибиева»с.п.Нартан .

2. Контроль использования учащимися сети Интернет осуществляется с помощью программно-технических средств и визуального контроля.

3. На официальном сайте школы создана страница «Безопасность в Интернете», на которой размещены материалы, посвященные безопасному поведению в сети Интернет и его использованию. А также на сайте размещены полезные ссылки для обучающихся и родителей.

4. Ведется журнал учета работы в сети Интернет.

5. Ежегодно проводится Неделя безопасности в сети Интернет.

Механизм реализации программы.

Безопасность детей одна из главных задач цивилизованного общества, поэтому обеспечивать безопасность детей в Интернете должны все, кто причастен к этому обществу. Контроль использования учащимися сети Интернет осуществляется с помощью программно-технических средств и визуального контроля. Ведется журнал учета работы в сети Интернет. Контроль за учащимися в сети Интернет осуществляют:

- 1) во время проведения занятий – преподаватель, проводящий занятие;
- 2) во время использования сети Интернет для свободной работы учащихся - лицо, назначенное приказом директора школы по вопросам регламентации доступа к информации в Интернете.

Данные лица обладают необходимой квалификацией и знаниями в области информационных технологий. Для решения вопросов безопасности Интернета в школе организован технический контроль, ведется профилактическая работа с обучающимися и их родителями, доступны информационные ресурсы для всех участников образовательного процесса.

Технический контроль.

Чтобы ограничить доступ учащихся к информации, которая может оказать на них негативное воздействие, в школе установлена специальная система фильтрации интернет-цензор и NetPolice, исключающая доступ к такой информации. Программой блокируется доступ к сайтам, содержащим материалы, которые определены как опасные. С помощью технологии фильтров и блокировки можно ограничить список собеседников, с которыми дети общаются через Интернет. Тем не менее, нет компьютерных программ, способных полностью защитить ребенка от доступа к нежелательной информации.

Антивирусный пакет компании «Касперский», установленный на все компьютеры, также позволяет ограничить доступ юных пользователей Интернета к нежелательному контенту и обеспечить безопасность школьной компьютерной сети.

Обе программы позволяют организовать доступ в Интернет по «черным» и «белым» спискам.

Профилактическая работа с обучающимися

Для преодоления негативного воздействия сети Интернет школа должна проводить целенаправленную воспитательную работу с педагогическим коллективом, учащимися, родителями.

Необходимо научить детей извлекать из ресурсов только лучшее и безопасное, делать осознанный и грамотный выбор.

Необходимо обсуждать с детьми все вопросы, которые возникают у них при использовании Интернет. Чем больше взрослые будут знать о том, как дети используют Интернет, тем проще определить и объяснить, что является приемлемым и безопасным.

Работа с учащимися проводится с учетом их возрастных особенностей. В начальной школе – в виде сказок, игр. В среднем звене – в виде бесед, ролевых игр, диспутов, тренингов, проектов, участия в акциях, конкурсах.

Ежегодно в нашей школе проходит традиционная неделя безопасности в сети Интернет. Программа, посвященная этой неделе, включает в себя ряд мероприятий, направленных на обучение учителей, родителей и детей правилам безопасного

пользования Интернетом. Это классные часы по теме «Безопасность в сети Интернет»; выпускаются листовки с памятками для учащихся «Безопасность в Интернете», проводится онлайнтестирование по интернет-безопасности.

Ежегодно учащиеся нашей школы принимают участие во всероссийской акции «Час кода», а также являются активными участниками «Единого урока по безопасности в сети и квеста «Сетевичок».

Профилактическая работа с родителями

Формы работы с родителями различны – родительские собрания, индивидуальные беседы, лекции. Родители должны понимать, что никто так сильно не отвечает за безопасность детей в Интернете, как сами родители. Только они могут полностью контролировать своих детей.

Выдержка из аннотации к книге Заряны и Нины Некрасовых «Как оттащить ребенка от компьютера и что с ним делать», вышедшей в издательстве «София»:

«Дети и подростки прирастают к розетке тогда, когда реальный мир не может предложить им других полноценных занятий. Не надо бороться с компьютером, борьба не укрепляет семьи. Надо просто понять истинные потребности своих детей - и найти в себе силы и время общаться, играть, слушать их. Просто посмотреть на все (в том числе и на компьютеры, ТВ, мобильник, плеер и прочие розеточные изобретения) глазами детей и подростков. И тогда виртуальный мир станет помощником вашей семье, для чего он, собственно, и предназначен».

Для разъяснения родителям опасностей Интернета проводятся родительские собрания «Безопасный Интернет - детям».

Информационный ресурс

Для достижения положительных результатов необходимо проводить комплексную работу семьи школы. Именно преподаватели и родители смогут предостеречь детей от возможных опасностей и ошибок. Существует ряд сайтов, посвященных безопасности детей в Интернете: <http://персональныеданные.дети/>, <http://rkn.gov.ru/personal-data/>, <http://сетевичок.пф/>, www.detionline.org, www.interneshka.ru, ресурсы которых оказывают огромную помощь, как взрослым, так и детям. Также информация для родителей и детей по безопасной работе в Интернет размещена на официальном сайте школы и в классных уголках.

Таким образом, в школе необходимо регулярно вести работу по формированию безопасной информационной образовательной среды школы, обеспечению информационной безопасности учащихся, использующих Интернет в образовании, и пропаганде безопасного поведения в сети Интернет.

Прогноз возможных негативных последствий и способы коррекции, компенсации негативных последствий

Запрет доступа к негативной информации формирует у ребенка желание получить эту информацию во что бы то ни стало. И эту информацию он может получить вне школы и дома у друзей или знакомых. Поэтому очень важно формировать информационную культуру и создать индивидуальную рабочую среду ребенку и в школе и дома с учетом его интересов, сообразно возрастным особенностям и духовным потребностям в рамках общечеловеческих ценностей.

Планируемые результаты.

Системный подход в решении задач построения в школе безопасной среды для доступа к сети Интернет:

- обеспечит потребность учителя в постоянном повышении уровня своей квалификации и профессионализма по данному вопросу;
- поможет родителям грамотно организовать информационное пространство ребенка в семье;
- совместные усилия педагогов и родителей создадут рабочую среду ребенка и в школе, и дома с учетом его интересов, сообразно возрастным особенностям и духовным потребностям в рамках общечеловеческих ценностей. Будет создана новая медиасреда, соответствующая следующим характеристикам:
 - наличие развитых информационно-коммуникационных механизмов, направленных на социализацию молодого поколения и раскрытие его творческого потенциала;
 - свободный доступ детей к историко-культурному наследию предшествующих поколений;
 - качественный рост уровня медиаграмотности детей;
 - увеличение числа детей, разделяющих ценности патриотизма;
 - гармонизация меж- и внутрипоколенческих отношений;
 - популяризация здорового образа жизни среди молодого поколения;
 - формирование среди детей устойчивого спроса на получение высококачественных информационных продуктов;
 - снижение уровня противоправного и преступного поведения среди детей;
 - формирование у детей уважительного отношения к интеллектуальной собственности и авторскому праву, сознательный отказ от использования "пиратского" контента». (Концепция информационной безопасности детей, утвержденная распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р).

Перспективы дальнейшей работы школы по созданию Интернет-пространства для участников образовательной деятельности

Формирование информационной культуры и безопасности - процесс длительный и сложный, но важный и необходимый. Интернет может быть и всемирной энциклопедией, объединяющей информационные ресурсы во всем мире. Задача взрослых (педагогов, родителей) - формирование разносторонней интеллектуальной личности, высокий нравственный уровень которой будет гарантией ее информационной безопасности. А для этого необходимо повышать квалификацию педагогов по вопросам информационной безопасности, чтобы уметь оперативно ориентироваться и ориентировать детей по безопасному поведению в Интернете. Регулярно проводить родительский всеобуч по вопросам кибербезопасности и работать не вдогонку, а на опережение.

Приложения:

1. План мероприятий по обеспечению информационной безопасности обучающихся МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан.

2. Документы школы, связанные с работой в сети Интернет:

— РЕГЛАМЕНТ работы в сети Интернет в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;

— ПОЛОЖЕНИЕ об использовании сети Интернет в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;

— ПОЛОЖЕНИЕ об информационной открытости МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;

— ПОЛОЖЕНИЕ о сайте муниципального общеобразовательного учреждения МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;

— ИНСТРУКЦИЯ для педагогических сотрудников о порядке действий при осуществлении контроля за использованием учащимися МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан в сети Интернет;

— Порядок доступа педагогических работников к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности;

— КЛАССИФИКАТОР информации, не имеющей отношения к образовательному процессу;

— Регламент работы с электронной почтой в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;

— Инструкция по организации антивирусной защиты в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;

— ПОЛОЖЕНИЕ об электронном журнале успеваемости/электронном дневнике учащегося в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;

3. Методические рекомендации «Безопасный Интернет».

4. Памятка родителям по управлению безопасностью детей в интернете.

5. Памятка для детей по безопасному поведению в интернете.

КЪЭБЭРДЕЙ-БАЛТЬКЪЭР РЕСПУБЛИКЭМ
И ШЭДЖЭМ КУЕЙМ
И АДМИНИСТРАЦЭМ ЦЦЭНЬГЪЭ
ГУУХУХЭМКЦЭ МУНИЦИПАЛЬНЭ
КЦЭЗОНЭ ГУУХУХЦАПЦЭ

КЪАБАРТЫ-МАЛКЪАР РЕСПУБЛИКАНЫ
МУНИЦИПАЛ КАЗНА УЧРЕЖДЕНИЯСЫ
«ЧЕГЕМ РАЙОННУ ЖЕР ЖЕРЛИ
АДМИНИСТРАЦИЯСЫНЫ ИЛМУ БИЛИМ
БЕРИУ УПРАВЛЕНИЯСЫ»

Министерство образования и науки КБР
Управление образования Чегемского муниципального района
Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа №2 им. Инала Пшибиева» с. п.Нартан

Адрес: с.п. Нартан ул. им. Али Тухужева,1

тел./факс (86630) 9-74-98, email: elbrusnartan@vandex.r



Утверждаю
Директор
А.А.Кунижев

План мероприятий по обеспечению информационной безопасности обучающихся МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан на 2018-2019 уч.год

№	Наименование мероприятия	Срок исполнения	Исполнители, ответственные за реализацию мероприятия	Ожидаемые результаты (количественные и качественные показатели)
I. Создание организационно-правовых механизмов защиты детей от распространения информации, причиняющей вред их здоровью и развитию				
1.1	Проведение внеурочных занятий с учащимися по теме «Приемы безопасной работы в Интернете»	Ежегодно сентябрь	Классные руководители	100% охват учащихся школы
1.2	Ознакомление родителей с Положением о защите детей от информации, причиняющей вред их здоровью и развитию	Январь-февраль 2018	Классные руководители	100% ознакомление родителей с информацией по медиабезопасности
1.3	Ознакомление родителей с программой информационной безопасности	Март 2018	Классные руководители	100% ознакомление родителей
1.4	Функционирование контент-фильтра в образовательном учреждении	В течение образовательного процесса	Зам. директора ответственный администратор	Обеспечение контентфилтрации трафика
1.5	Функционирование антивирусных программ в образовательном	В течение образовательного процесса	Зам. директора ответственный администратор	Обеспечение антивирусной защиты всех ПК

II. Внедрение систем исключения доступа к информации, несовместимой с задачами гражданского становления детей, а также средств фильтрации и иных аппаратно-программных и техникотехнологических устройств				
2.1	Мониторинг функционирования и использования в школе программного продукта, обеспечивающего контент-фильтрацию Интернет-трафика.	Ежеквартально	Рабочая комиссия	Обеспечение контент-фильтрации трафика. Акты проверок.
2.2	Мониторинг функционирования и использования в школе программного продукта, обеспечивающего антивирусную защиту всех ПК	Ежеквартально	Рабочая комиссия	Обеспечение антивирусной защиты всех ПК. Акты проверок.
2.3	Мониторинг качества предоставления провайдером услуги доступа к сети Интернет образовательным учреждениям с обеспечением контент-фильтрации Интернет - трафика	Ежеквартально	Рабочая комиссия	100% обеспечение услуги доступа в сеть Интернет школе с обеспечением контент-фильтрации Интернет-трафика
III. Профилактика у обучающихся интернет-зависимости, игровой зависимости и правонарушений с использованием информационно-телекоммуникационных технологий, формирование навыков ответственного и безопасного поведения в современной информационно-телекоммуникационной среде через обучение их способам защиты от вредной информации				
3.1	Проведение медиауроков по теме «Информационная безопасность»	По рабочим программам Обеспечение	Классные руководители, учитель информатики	100% охвата учащихся школы Повышение грамотности обучающихся по проблемам информационной безопасности.
3.2	Проведение недели (месячника) «Интернетбезопасность» для учащихся 1-4 классов, 5-9 классов и их родителей	По планам ведомственных организаций	Классные руководители, учитель информатики, библиотекарь.	Повышение грамотности обучающихся, родителей (законных представителей) по проблемам информационной безопасности
3.3	Ведение раздела	В течение	Администратор	Актуальность

	«Информационная безопасность» на школьном сайте	образовательного процесса	сайта	раздела.
3.4	Организация и проведение обучающих семинаров для учителей по созданию надежной системы защиты детей от противоправного контента в образовательной среде школы и дома.	Два раза в год	Зам. директора по УВР	Повышение грамотности по проблемам информационной безопасности всех участников образовательного процесса
3.5	Организация свободного доступа обучающихся и учителей к высококачественным и сетевым образовательным ресурсам, в том числе к системе современных учебных материалов по всем предметам.	В течение образовательного процесса	Ответственный администратор	100% обеспечение доступа обучающихся и учителей к электронным образовательным ресурсам через сеть Интернет
3.6	Внедрение и использование программно-технических средств, обеспечивающих исключение доступа обучающихся школы к ресурсам сети Интернет, содержащим информацию, несовместимую с задачами образования и воспитания	В течение образовательного процесса	Ответственный администратор	Отслеживание созданных, обновленных программно-технических средств, обеспечивающих исключение доступа обучающихся школы к ресурсам сети Интернет и установка их на компьютеры

Документы школы, связанные с работой в сети Интернет:

- РЕГЛАМЕНТ работы в сети Интернет в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;
- ПОЛОЖЕНИЕ об использовании сети Интернет в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;
- ПОЛОЖЕНИЕ об информационной открытости МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;
- ПОЛОЖЕНИЕ о сайте муниципального общеобразовательного учреждения МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;
- ИНСТРУКЦИЯ для педагогических сотрудников о порядке действий при осуществлении контроля за использованием учащимися муниципального общеобразовательного учреждения МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан сети Интернет;
- Порядок доступа педагогических работников к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности;
- КЛАССИФИКАТОР информации, не имеющей отношения к образовательному процессу;
- Регламент работы с электронной почтой в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;

- Инструкция по организации антивирусной защиты в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;

- ПОЛОЖЕНИЕ об электронном журнале успеваемости/электронном дневнике учащегося в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан;

КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ
И ШЭДЖЭМ КУЕЙМ
И АДМИНИСТРАЦЭМ ШЦІЭНЫГЪЭ
ІУЭХУХЭМКІЭ МУНИЦИПАЛЬНЭ
КІЭЗОНЭ ІУЭХУЦІАПІЭ

КЪАБАРТЫ-МАЛЪАР РЕСПУБЛИКАНЫ
МУНИЦИПАЛ КАЗНА УЧРЕЖДЕНИЯСЫ
«ЧЕГЕМ РАЙОННУ ЖЕР ЖЕРЛИ
АДМИНИСТРАЦИЯСЫНЫ ІЛМУ БИЛИМ
БЕРІУ УПРАВЛЕНИЯСЫ»

Министерство образования и науки КБР
Управление образования Чегемского муниципального района
Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа №2 им. Инала Пшибиева» с.п.Нартан

Адрес: с.п. Нартан ул. им. Али Тухужева,1 тел./факс (86630) 9-74-98, email: elbrusnartan@vandex.r

РЕГЛАМЕНТ РАБОТЫ УЧИТЕЛЕЙ И ОБУЧАЮЩИХСЯ МКОУ «СОШ №2 ИМЕНИ ИНАЛА ПШИБИЕВА» с.п.НАРТАН В СЕТИ ИНТЕРНЕТ

I. Общие положения

1.1. Настоящий Регламент разработан в соответствии с положением об использовании сети Интернет в муниципальном казенном общеобразовательном учреждении «СОШ №2 имени Инала Пшибиева» с.п.Нартан и является локальным нормативным актом образовательного учреждения.

1.2. «Точка доступа» (все учебные кабинеты) к сети Интернет предназначена для обслуживания обучающихся, педагогов и административного персонала образовательного учреждения, которые допускаются к работе в сети Интернет на бесплатной основе.

1.3. Организацию работы «Точек доступа» осуществляют назначенные приказом по школе ответственные за обеспечение доступа к ресурсам сети Интернет и контроль безопасности работы в сети, а также администраторы «Точек доступа». Пользователями в настоящем документе называются обучающиеся и сотрудники школы, ознакомленные с положением об использовании сети Интернет и прошедшие предварительную регистрацию у администратора «точки доступа». В исключительном случае разрешается допуск к работе других лиц по разрешению директора школы. Предоставление сеанса работы в Интернет осуществляется пользователям, как правило, на основании предварительной записи в журнале администратора в зависимости от категории пользователя:

- учащимся предоставляется доступ в компьютерном классе согласно расписанию занятий, график работы компьютерного класса составляется (на учебную четверть) на основании общешкольного расписания;

- для проведения внеурочных мероприятий доступ предоставляется в соответствии с планом работы и корректируется еженедельно;

- для свободного доступа учащихся к сети Интернет предоставляется не менее 2 часов в неделю, сеансами не более 30 минут при предварительной записи у администратора «точки доступа»;

-учителям, административному, вспомогательному персоналу предоставляется доступ по графику согласно ежемесячно подаваемым служебным запискам на имя ответственного лица, но не менее 2 часов в неделю, сеансами не менее 30 минут.

II. Правила работы

Для проведения сеанса работы, необходимо обратиться к администратору «точки доступа» за разрешением для работы. При наличии свободных мест и после регистрации в журнале учета, пользователю предоставляется рабочая станция в «точке доступа».

1. В начале работы пользователь обязан зарегистрироваться в журнале учета.

2. Пользователю разрешается записывать полученную информацию на личные носители информации (диски, флэш-карты) с предварительной проверкой на наличие вирусов. Копирование с носителей на жесткие диски производится только с разрешения администратора «точки доступа».

3. Разрешается использовать оборудование только для работы с информационными ресурсами и электронной почтой и только в образовательных целях или для осуществления научных изысканий, выполнения гуманитарных и культурных проектов. Любое использование оборудования в коммерческих целях запрещено.

4. Запрещена передача информации, представляющую коммерческую или государственную тайну, распространение информации, порочащей честь и достоинство граждан.

5. Запрещается работать с объемными ресурсами (video, audio, игры и др.) без согласования с администратором.

6. Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.

7. Пользователь обязан сохранять оборудование в целостности и сохранности.

8. Пользователю запрещено вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на серверах без прямого разрешения администратора. За административное нарушение, не влекущее за собой порчу имущества и вывод оборудования из рабочего состояния пользователь может быть лишен права выхода в Интернет сроком на месяц. При повторном административном нарушении – пользователь лишается доступа в Интернет. При возникновении технических проблем пользователь обязан поставить в известность администратора.

III. Памятка пользователя по использованию ресурсов сети Интернет

1. В начале работы пользователь обязан зарегистрироваться в журнале учёта работы в сети Интернет.

2. Каждый пользователь при наличии технической возможности может иметь персональный каталог, предназначенный для хранения личных файлов общим объемом не более 200 Мб. Аналогично может быть предоставлена возможность работы с почтовым ящиком. При возникновении проблем необходимо обратиться к дежурному администратору.

3. Пользователю разрешается переписывать полученную информацию на личные носители информации, которые предварительно проверяются на наличие вирусов

4. Разрешается использовать оборудование классов только для работы с информационными ресурсами и электронной почтой и только в образовательных целях

или для осуществления научных изысканий, выполнения проектов. Любое использование оборудования в коммерческих целях запрещено.

5. Запрещена передача внешним пользователям информации, представляющую коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан. Правовые отношения регулируются Законом «Об информации, информатизации и защите информации», Законом «О государственной тайне», Законом «Об авторском праве и смежных правах», статьями Конституции об охране личной тайне, статьями Гражданского кодекса и статьями Уголовного кодекса о преступлениях в сфере компьютерной информации.

6. Запрещается работать с объемными ресурсами (video, audio, chat, игры) без согласования с администратором.

7. Запрещается доступ к сайтам, содержащим информацию сомнительного содержания и противоречащую общепринятой этике.

8. При случайном обнаружении ресурса, содержание которого противоречит законодательству Российской Федерации, противоречит целям обучения и воспитания, или имеет провокационный или оскорбительный характер, пользователь обязан незамедлительно сообщить об этом администратору “точки доступа”.

9. Пользователю запрещено вносить какие-либо изменения в программное обеспечение, установленное как на рабочей станции, так и на серверах без прямого разрешения администратора. Запрещается перегружать компьютер без согласования с администратором.

10. Пользователь обязан сохранять оборудование в целостности и сохранности.

11. Пользователь обязан соблюдать общественный порядок и чистоту в помещении и способствовать соблюдению порядка другими пользователями; проявлять корректность по отношению к пользователям.

12. При возникновении технических проблем пользователь обязан поставить в известность администратора. При нанесении любого ущерба (порча имущества, вывод оборудования из рабочего состояния) пользователь несет материальную ответственность. За административное нарушение, не влекущее за собой порчу имущества и вывод оборудования из рабочего состояния пользователь может быть лишен права выхода в Интернет сроком на месяц. При повторном административном нарушении – пользователь лишается доступа в Интернет.

КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКОМ
И ШЭДЖЭМ КУЕЙМ
И АДМИНИСТРАЦЭМ ЦЦЭНЫГЪЭ
ІУЭХУХЭМКІЭ МУНИЦИПАЛЬНЭ
КІЭЗОНЭ ІУЭХУЦАПІЭ

КЪАБАРТЫ-МАЛКЪАР РЕСПУБЛИКАНЫ
МУНИЦИПАЛ КАЗНА УЧРЕЖДЕНИЯСЫ
«ЧЕГЕМ РАЙОННУ ЖЕР ЖЕРЛИ
АДМИНИСТРАЦИЯСЫНЫ ИЛМУ БИЛИМ
БЕРІУ УПРАВЛЕНИЯСЫ»

Министерство образования и науки КБР
Управление образования Чегемского муниципального района
Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа №2 им. Инала Пшибиева» с.п.Нартан

Адрес: с.п. Нартан ул. им. Али Тухужева,1 тел./факс (86630) 9-74-98, email: elbrusnartan@yandex.r

Принят
на педагогическом совете
Протокол № 1
от « 30 » 08. 2018 г.



ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ СЕТИ ИНТЕРНЕТ В МКОУ «СОШ №2 ИМЕНИ ИНАЛА ПШИБИЕВА» с.п.НАРТАН

1. Общие положения

1.1. Использование сети Интернет в школе направлено на решение задач учебно-воспитательного процесса.

1.2. Настоящее Положение регулируют условия и порядок использования сети Интернет в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан

1.3. Настоящее Положение имеет статус локального нормативного акта МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан

2. Организация использования сети Интернет в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан

2.1. Вопросы использования возможностей сети Интернет в учебно-образовательной деятельности рассматриваются на педагогическом совете школы. Положение вводится в действие приказом директора школы.

2.2. Положение об использовании сети Интернет разрабатывается педагогическим советом на основе примерного регламента самостоятельно, либо с привлечением внешних экспертов, в качестве которых могут выступать:

- преподаватели других образовательных учреждений, имеющие опыт использования Интернета в образовательной деятельности;
- специалисты в области информационных технологий;
- представители органов управления образованием;
- родители обучающихся.

2.3. При разработке Положения об использовании сети Интернет педагогический совет руководствуется:

- законодательством Российской Федерации;
- опытом целесообразной и эффективной организации учебного процесса с использованием информационных технологий и возможностей Интернета;
- интересами обучающихся;
- целями образовательного процесса;
- рекомендациями профильных органов и организаций в сфере классификации ресурсов Сети.

2.4. Директор школы отвечает за обеспечение эффективного и безопасного доступа к сети Интернет в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан, а также за выполнение установленных правил.

Для обеспечения доступа участников образовательной деятельности к сети Интернет в соответствии с установленным в школе Положением директор назначает своим приказом ответственного за организацию работы с Интернетом и ограничение доступа.

2.5. Заместитель директора школы по УВР:

- принимает решение о разрешении/блокировании доступа к определенным ресурсам и (или) категориям ресурсов сети Интернет;
- определяет характер и объем информации, публикуемой на интернет-ресурсах школы; – дает руководителю школы рекомендации о назначении и освобождении от исполнения своих функций лиц, ответственных за обеспечение доступа к ресурсам сети Интернет и контроль безопасности работы в Сети;

2.6. Во время уроков и других занятий в рамках учебного плана контроль использования обучающимися сети Интернет осуществляет преподаватель, ведущий занятие. При этом преподаватель:

- наблюдает за использованием компьютера и сети Интернет обучающимися;
- принимает меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

2.7. Во время свободного доступа обучающихся к сети Интернет вне учебных занятий, контроль использования ресурсов Интернета осуществляют ответственный за организацию доступа к ресурсам сети Интернет, определенные приказом его руководителя.

2.8. При использовании сети Интернет в школе обучающимся предоставляется доступ только к тем ресурсам, содержание которых не противоречит законодательству Российской Федерации и которые имеют прямое отношение к образовательному процессу. Проверка выполнения такого требования осуществляется с помощью специальных технических средств и программного обеспечения контентной фильтрации, установленного в школе или предоставленного оператором услуг связи.

2.10. Отнесение определенных ресурсов и (или) категорий ресурсов в соответствующие группы, доступ к которым регулируется техническими средствами и программным обеспечением контентной фильтрации, в соответствии с принятыми в школе Положением обеспечивается работником школы, назначенным его руководителем.

2.11. Принципы размещения информации на интернет-ресурсах школы призваны обеспечивать:

- соблюдение действующего законодательства Российской Федерации, интересов и прав граждан;
- защиту персональных данных обучающихся, преподавателей и сотрудников;
- достоверность и корректность информации.

2.12. Персональные данные обучающихся (включая фамилию и имя, класс/год обучения, возраст, фотографию, данные о месте жительства, телефонах и пр., иные сведения личного характера) могут размещаться на интернет-ресурсах, создаваемых школой, только с письменного согласия родителей или иных законных представителей обучающихся. Персональные данные преподавателей и сотрудников школы размещаются на его интернет-ресурсах только с письменного согласия лица, чьи персональные данные размещаются.

2.13. В информационных сообщениях о мероприятиях, размещенных на сайте школы без уведомления и получения согласия упомянутых лиц или их законных представителей, могут быть указаны лишь фамилия и имя обучающегося либо фамилия, имя и отчество преподавателя, сотрудника или родителя.

2.14. При получении согласия на размещение персональных данных представитель школы обязан разъяснить возможные риски и последствия их опубликования. Школа не несет ответственности за такие последствия, если предварительно было получено письменное согласие лица (его законного представителя) на опубликование персональных данных.

3. Использование сети Интернет в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан

3.1. Использование сети Интернет в школе осуществляется, как правило, в целях образовательного процесса.

3.2. По разрешению лица, ответственного за организацию в школе работы сети Интернет и ограничение доступа, преподаватели, сотрудники и обучающиеся вправе:

- размещать собственную информацию в сети Интернет на интернет-ресурсах школы;
- иметь учетную запись электронной почты на интернет-ресурсах школы.

3.3. Обучающемуся запрещается:

- 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 Интернет;
- осуществлять загрузки файлов на компьютер школы без специального разрешения;
- распространять оскорбительную, не соответствующую действительности, порочащую других лиц информацию, угрозы.

3.4. При случайном обнаружении ресурса, содержание которого не имеет отношения к образовательному процессу, обучающийся обязан незамедлительно сообщить об этом преподавателю, проводящему занятие. Преподаватель обязан зафиксировать доменный адрес ресурса и время его обнаружения и сообщить об этом лицу, ответственному за организацию доступа к ресурсам сети Интернет.

Ответственный обязан:

- принять информацию от преподавателя;
- направить информацию о некатегоризированном ресурсе оператору технических средств и программного обеспечения технического ограничения доступа к информации (в течение суток); – в случае явного нарушения обнаруженным ресурсом законодательства Российской Федерации сообщить о нем по специальной «горячей линии» для принятия мер в соответствии с законодательством Российской Федерации (в течение суток).

Передаваемая информация должна содержать:

- доменный адрес ресурса;
- сообщение о тематике ресурса, предположения о нарушении ресурсом законодательства Российской Федерации либо его несовместимости с задачами образовательного процесса;
- дату и время обнаружения;
- информацию об установленных в школе технических средствах технического ограничения доступа к информации.

КЪБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ
И ШЭДЖЭМ КУЕЙМ
И АДМИНСТРАЦЭМ ШЦЭНЬГЭЭ
ГУХУХЭМКІЭ МУНИЦИПАЛЬНЭ
КІЭЗОНЭ ГУЭХУЦІАПІЭ

КЪАБАРТЫ-МАЛЪБАР РЕСПУБЛИКАНЫ
МУНИЦИПАЛ КАЗНА УЧРЕЖДЕНИЯСЫ
«ЧЕГЕМ РАЙОННУ ЖЕР ЖЕРЛИ
АДМИНИСТРАЦИЯСЫНЫ ИЛМУ БИЛИМ
БЕРИУ УПРАВЛЕНИЯСЫ»

Министерство образования и науки КБР
Управление образования Чегемского муниципального района
Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа №2 им. Инала Пшибиева» с.п.Нартан

Адрес: с.п. Нартан ул.им.Али Тухужева,1 тел./факс (86630) 9-74-98, email: elbrusnartan@yandex.r

Принят
на педагогическом совете
Протокол № 1
от « 30» 08. 2018 г.



Утверждаю
Директор
А.А.Кунижев
Пр. № _____ от 31.08.2018 г.

ПОЛОЖЕНИЕ ОБ ИНФОРМАЦИОННОЙ ДОСТУПНОСТИ В МКОУ «СОШ №2 ИМЕНИ ИНАЛА ПШИБИЕВА» с.п.НАРТАН

Настоящее положение включает в себя ч 1. 29 статью Федерального закона № 273 «Об образовании в Российской Федерации» от 20.12.2012г и является нормой, которой руководствуется МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан (далее – ОО).

1. ОО формирует открытые и общедоступные информационные ресурсы, содержащие информацию об его деятельности, и обеспечивают доступ к таким ресурсам посредством размещения их в информационно-телекоммуникационных сетях, в том числе на официальном сайте ОО в сети "Интернет".
2. ОО обеспечивает открытость и доступность:
 - 1) информации:
 - а) о дате создания ОО, об учредителе, о месте нахождения ОО и ее филиалов (при наличии), режиме, графике работы, контактных телефонах и об адресах электронной почты;
 - б) о структуре и об органах управления ОО;
 - в) о реализуемых образовательных программах с указанием учебных предметов, курсов, дисциплин (модулей), практики, предусмотренных соответствующей образовательной программой;
 - г) о численности обучающихся по реализуемым образовательным программам за счет бюджетных ассигнований федерального бюджета, бюджетов субъектов Российской Федерации, местных бюджетов и по договорам об образовании за счет средств физических и (или) юридических лиц;

д) о языках образования;

е) о федеральных государственных образовательных стандартах, об образовательных стандартах (при их наличии);

ж) о руководителе ОО, его заместителях, руководителях филиалов образовательной организации (при их наличии);

з) о персональном составе педагогических работников с указанием уровня образования, квалификации и опыта работы;

и) о материально-техническом обеспечении образовательной деятельности (в том числе о наличии оборудованных учебных кабинетов, объектов для проведения практических занятий, библиотек, объектов спорта, средств обучения и воспитания, об условиях питания и охраны здоровья обучающихся, о доступе к информационным системам и информационно-телекоммуникационным сетям, об электронных образовательных ресурсах, к которым обеспечивается доступ обучающихся);

к) о наличии и об условиях предоставления обучающимся стипендий, мер социальной поддержки;

л) об объеме образовательной деятельности, финансовое обеспечение которой осуществляется за счет бюджетных ассигнований федерального бюджета, бюджетов субъектов Российской Федерации, местных бюджетов, по договорам об образовании за счет средств физических и (или) юридических лиц;

м) о поступлении финансовых и материальных средств и об их расходовании по итогам финансового года;

н) о трудоустройстве выпускников;

2) копий:

а) устава образовательной организации;

б) лицензии на осуществление образовательной деятельности (с приложениями);

в) свидетельства о государственной аккредитации (с приложениями);

г) плана финансово-хозяйственной деятельности образовательной организации, утвержденного в установленном законодательством Российской Федерации порядке, или бюджетной сметы образовательной организации;

д) локальных нормативных актов, предусмотренных частью 2 статьи 30 Федерального закона «Об образовании», правил внутреннего распорядка обучающихся, правил внутреннего трудового распорядка, коллективного договора;

3) отчета о результатах самообследования.

Показатели деятельности ОО, подлежащей самообследованию, и порядок его проведения устанавливаются федеральным органом исполнительной власти, осуществляющим функции по

выработке государственной политики и нормативно-правовому регулированию в сфере образования;

4) документа о порядке оказания платных образовательных услуг, в том числе образца договора об оказании платных образовательных услуг, документа об утверждении стоимости обучения по каждой образовательной программе;

5) предписаний органов, осуществляющих государственный контроль (надзор) в сфере образования, отчетов об исполнении таких предписаний;

6) иной информации, которая размещается, публикуется по решению ОО и (или) размещение, опубликование которой являются обязательными в соответствии с законодательством Российской Федерации.

3. Информация и документы, указанные в п. 2 настоящего Положения, если они в соответствии с законодательством Российской Федерации не отнесены к сведениям, составляющим государственную и иную охраняемую законом тайну, подлежат размещению на официальном сайте образовательной организации в сети "Интернет" и обновлению в течение десяти рабочих дней со дня их создания, получения или внесения в них соответствующих изменений.

Порядок размещения на официальном сайте образовательной организации в сети "Интернет" и обновления информации об образовательной организации, в том числе ее содержание и форма ее предоставления, устанавливается Правительством Российской Федерации.

КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ
И ШЭДЖЭМ КУЕЙМ
И АДМИНИСТРАЦЭМ ШЦЭНЫГЪЭ
ГУЭХУХЭМКІЭ МУНИЦИПАЛЬНЭ
КІЭЗОНЭ ГУЭХУЩАПІЭ

КЪАБАРТЫ-МАЛЪКАР РЕСПУБЛИКАНЫ
МУНИЦИПАЛ КАЗНА УЧРЕЖДЕНИЯСЫ
«ЧЕГЕМ РАЙОННУ ЖЕР ЖЕРЛИ
АДМИНИСТРАЦИЯСЫНЫ ИЛМУ БИЛИМ
БЕРИУ УПРАВЛЕНИЯСЫ»

Министерство образования и науки КБР
Управление образования Чегемского муниципального района
Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа №2 им. Инала Пшибиева» с.п.Нартан

Адрес: с.п. Нартан ул. им. Али Тухужева,1 тел./факс (86630) 9-74-98. email: efbrusnartan@yandex.ru

Принят
на педагогическом совете
Протокол № 1
от « 30» 08. 2018 г.



ПОЛОЖЕНИЕ

О САЙТЕ МКОУ «СОШ №2 ИМЕНИ ИНАЛА ПШИБИЕВА» с.п.НАРТАН

(<https://nartansosh2.edu07.ru>)

1. Общие положения

1.1. Положение о сайте МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан (далее - положение) определяет статус сайта <https://nartansosh2.edu07.ru>, структуру и порядок размещения в сети Интернет информационных материалов, образующих информационные ресурсы МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан (далее - ОУ), а также права, обязанности, ответственность и регламент взаимодействия администратора, осуществляющего программно-техническую поддержку данного сайта, и лиц, осуществляющих предоставление информации для размещения в его разделах.

1.2. Сайт обеспечивает официальное представление информации о ОУ в сети Интернет с целью расширения рынка образовательных услуг ОУ, оперативного ознакомления сотрудников, обучающихся, родителей (законных представителей) обучающихся, деловых партнеров и других заинтересованных пользователей с различными аспектами деятельности ОУ, повышения эффективности взаимодействия ОУ с целевой аудиторией.

1.3. Пользователем сайта может быть любое лицо, имеющее технические возможности выхода в Интернет.

1.4. Функционирование сайта регламентируется действующим законодательством, Уставом ОУ, настоящим положением, а также локальными нормативными актами ОУ, приказами и распоряжениями директора ОУ. 1.5. Положение вступает в силу со дня утверждения директором ОУ и действует до его отмены.

1.6. Изменения в положение могут вноситься по рекомендации администрации ОУ, а также лиц, ответственных за информационное наполнение и поддержание сайта. Изменённая редакция положения вступает в силу после утверждения ее директором ОУ.

2. Информационный ресурс сайта

2.1. Информационный ресурс сайта (контент) формируется в соответствии с деятельностью всех структурных подразделений ОУ, ее сотрудников, обучающихся, родителей и общественных организаций ОУ.

2.2. Права на информационные материалы, размещенные на сайте, принадлежат ОУ при условии, что иное не регламентировано отдельными юридически оформленными документами.

2.3. Информационный ресурс сайта является открытым и общедоступным, если иной статус ресурса не оговорен специальными документами.

2.4. Условия размещения ресурсов ограниченного доступа регулируются отдельными документами; размещение таких ресурсов допустимо только при наличии соответствующих организационных и программно-технических возможностей.

2.5. Основными информационно-ресурсными компонентами сайта являются:

- общая информация о ОУ как муниципальном образовательном учреждении;
- справочные и иные материалы об образовательных программах ОУ;
- материалы по организации учебного процесса;
- подборки тематических материалов;
- материалы о персоналиях - руководителях, сотрудниках ОУ;
- материалы о событиях текущей жизни ОУ, проводимых в ОУ и при ее участии мероприятиях, архивы новостей;
- материалы о ходе реализации в ОУ комплексного проекта модернизации образования;
- адресные информационные материалы.

2.6. Часть информационного ресурса, формируемого по инициативе творческих коллективов и отдельных работников ОУ, может быть размещена на отдельных специализированных сайтах, доступ к которым организуется с сайта ОУ.

3. Организация работ

3.1. Информационное наполнение и актуализация сайта осуществляется совместными усилиями всех структурных подразделений ОУ, ее сотрудников, обучающихся, родителей и общественных организаций ОУ.

3.2. По каждому разделу сайта (виду информационного ресурса) определяются должностные лица, ответственные за подборку и предоставление соответствующей информации.

3.3. Руководство обеспечением функционирования сайта и его программно-технической поддержкой, непосредственное выполнение работ по размещению информации на сайте, обеспечению ее целостности и доступности, реализации правил разграничения доступа

возлагается на администратора сайта (далее — администратор), который назначается директором школы.

3.4. Администратор сайта курирует качественное выполнение всех видов работ, связанных с эксплуатацией сайта: изменение дизайна и структуры, размещение новой и удаление устаревшей информации, публикация информации из баз данных, реализация политики разграничения доступа и обеспечение безопасности информационных ресурсов.

3.5. Администратор сайта осуществляет консультирование лиц, ответственных за предоставление информации, а также других работников, заинтересованных в размещении информации на сайте.

3.6. Информация, готовая для размещения на сайте, предоставляется должностными лицами, ответственными за подборку и предоставление соответствующей информации по разделам школьного сайта, в электронном виде администратору сайта, который обеспечивает ее размещение в соответствующем разделе сайта.

3.7. Текстовая информация предоставляется в формате .doc, графическая - в формате .jpg. В порядке исключения графическая информация может быть предоставлена в виде фотографий, схем, чертежей – в этом случае администратор изыскивает возможность перевода материалов в электронный вид.

3.8. Администратор сайта имеет право направить материалы на пересмотр с целью проведения корректуры и редакторской правки.

3.9. Текущие изменения структуры сайта, изменения, носящие концептуальный характер, согласовываются с директором ОУ.

4. Ответственность

4.1. Ответственность за недостоверное, несвоевременное или некачественное предоставление информации (в том числе с грамматическими и/или синтаксическими ошибками) для размещения на сайте несет соответствующее должностное лицо, ответственное за предоставление данной информации.

4.2. Ответственность за некачественное текущее сопровождение сайта несет администратор.

4.3. Некачественное текущее сопровождение может выражаться:

- в несвоевременном размещении предоставляемой информации;
- в непринятии мер по исключению появления на сайте устаревшей или ошибочной информации;
- в совершении действий, повлекших причинение вреда информационному ресурсу, нарушение работоспособности или возможность несанкционированного доступа к сайту.

4.4. Ответственность за нарушение работоспособности и актуализации сайта вследствие отсутствия четкого порядка во взаимодействии с лицами, ответственными за предоставление

информации, отказ в консультировании сотрудников школы в соответствии с п.3.5 настоящего положения, несет администратор сайта.

5. Контроль

5.1. Контроль над выполнением обязанностей лицами, участвующими в процессах информационного наполнения, актуализации и программно-технического сопровождения сайта, возлагается на директора ОУ.

КЪЭБЪРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ
И ШЭДЖЭМ КУЕЙМ
И АДМИНИСТРАЦЭМ ЦЦЭНЫГЪЭ
ГУЭХУХЭМКІЭ МУНИЦИПАЛЬНЭ
КІЭЗОНЭ ГУЭХУЩІАПІЭ

КЪАБАРТЫ-МАЛЪАР РЕСПУБЛИКАНЫ
МУНИЦИПАЛ КАЗНА УЧРЕЖДЕНИЯСЫ
«ЧЕГЕМ РАЙОННУ ЖЕР ЖЕРЛИ
АДМИНИСТРАЦИЯСЫНЫ ИЛМУ БИЛИМ
БЕРИУ УПРАВЛЕНИЯСЫ»

Министерство образования и науки КБР
Управление образования Чегемского муниципального района
Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа №2 им. Инала Пшибиева» с. п.Нартан

Адрес: с.п. Нартан ул. им. Али Тухужева,1 тел./факс (86630) 9-74-98, email: elbrusnartan@yandex.r



Утверждаю
Директор
А.А.Кунижев

ИНСТРУКЦИЯ

для педагогических работников и сотрудников муниципального казенного общеобразовательного учреждения «СОШ №2 имени Инала Пшибиева» с.п.Нартан о порядке действий при осуществлении контроля использования обучающимися сети Интернет

1. Настоящая инструкция устанавливает порядок действий сотрудников образовательного учреждения при обнаружении:
 - 1) обращения обучающихся к контенту, не имеющему отношения к образовательному процессу;
 - 2) отказа при обращении к контенту, имеющему отношение к образовательному процессу, вызванного техническими причинами.
2. Контроль использования обучающимися сети Интернет осуществляют:
 - 1) во время занятия — проводящий его преподаватель;
 - 2) во время использования сети Интернет для свободной работы обучающихся — дежурный преподаватель.
3. Преподаватель: — определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательном процессе соответствующих технических возможностей, а также длительность сеанса работы одного обучающегося;
 - наблюдает за использованием обучающимися компьютеров и сети Интернет;
 - способствует осуществлению контроля объемов трафика ОУ в сети Интернет;
 - запрещает дальнейшую работу обучающегося в сети Интернет на уроке (занятии) в случае нарушения им порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;

— доводит до классного руководителя информацию о нарушении обучающимся правил работы в сети Интернет;

— принимает необходимые меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

4. При обнаружении ресурса, который, по мнению преподавателя, содержит информацию, запрещенную для распространения в соответствии с законодательством Российской Федерации, или иного потенциально опасного для обучающихся контента, он сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

5. В случае отказа доступа к ресурсу, разрешенному в ОУ, преподаватель также сообщает об этом лицу, ответственному за работу Интернета и ограничение доступа.

КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ
И ШЭДЖЭМ КУЕЙМ
И АДМИНИСТРАЦЭМ ШЦІЭНЫГЪЭ
ІУЭХУХЭМКІЭ МУНИЦИПАЛЬНЭ
КІЭЗОНЭ ІУЭХУЩІАПІЭ

КЪАБАРТЫ-МАЛКЪАР РЕСПУБЛИКАНЫ
МУНИЦИПАЛ КАЗНА УЧРЕЖДЕНИЯСЫ
«ЧЕГЕМ РАЙОННУ ЖЕР ЖЕРЛИ
АДМИНИСТРАЦИЯСЫНЫ ИЛМУ БИЛИМ
БЕРІУ УПРАВЛЕНИЯСЫ»

Министерство образования и науки КБР
Управление образования Чегемского муниципального района
Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа №2 им. Инала Пшибиева» с. п.Нартан

Адрес: с.п. Нартан ул. им. Али Тухужева,1 тел./факс (86630) 9-74-98, email: elbrusnartan@yandex.r

Принят
на педагогическом совете
Протокол № 1
от «30» 08. 2018 г.



ПОРЯДОК

доступа педагогических работников к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности

1. Настоящий Порядок регламентирует доступ педагогических работников МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан (далее – Учреждение) к информационно-телекоммуникационным сетям и базам данных, учебным и методическим материалам, материально-техническим средствам обеспечения образовательной деятельности.
2. Доступ педагогических работников к вышеперечисленным ресурсам обеспечивается в целях качественного осуществления образовательной и иной деятельности, предусмотренной уставом Учреждения.
3. Доступ к информационно-телекоммуникационным сетям
 - 3.1. Доступ педагогических работников к информационно-телекоммуникационной сети Интернет в Учреждении осуществляется с персональных компьютеров (ноутбуков, компьютеров и т.п.), подключенных к сети Интернет, в пределах установленного лимита на входящий трафик, а также возможности Учреждения по оплате трафика /без ограничения времени и потребленного трафика.
 - 3.2. Доступ педагогических работников к локальной сети Учреждения осуществляется с персональных компьютеров (ноутбуков, компьютеров и т.п.), подключенных к локальной сети Учреждения, без ограничения времени и потребленного трафика.
 - 3.3. Для доступа к информационно-телекоммуникационным сетям в Учреждении педагогическому работнику предоставляются идентификационные данные (логин и пароль / учётная запись / электронный ключ и др.). Предоставление доступа осуществляется системным администратором / заместителем заведующего Учреждением.

4. Доступ к базам данных

4.1. Педагогическим работникам обеспечивается доступ к следующим электронным базам данных:

- база данных АСИОУ;
- информационные справочные системы;
- поисковые системы.

4.2. Доступ к электронным базам данных осуществляется на условиях, указанных в договорах, заключенных Учреждением с правообладателем электронных ресурсов (внешние базы данных).

4.3. Информация об образовательных, методических, научных, нормативных и других электронных ресурсах, доступных к пользованию, размещена на сайте Учреждения в разделе «Информационные ресурсы». В данном разделе описаны условия и порядок доступа к каждому отдельному электронному ресурсу.

5. Доступ к учебным и методическим материалам

5.1. Учебные и методические материалы, размещаемые на официальном сайте Учреждения, находятся в открытом доступе.

5.2. Педагогическим работникам по их запросам могут выдаваться во временное пользование учебные и методические материалы, входящие в оснащение групповых комнат.

Выдача педагогическим работникам во временное пользование учебных и методических материалов, входящих в оснащение групповых комнат, осуществляется работником, на которого возложено заведование групповой комнатой.

Срок, на который выдаются учебные и методические материалы, определяется работником, на которого возложено заведование групповой комнатой, с учетом графика использования запрашиваемых материалов в данной групповой комнате.

Выдача педагогическому работнику и сдача им учебных и методических материалов фиксируются в журнале выдачи. При получении учебных и методических материалов на электронных носителях, подлежащих возврату, педагогическим работникам не разрешается стирать или менять на них информацию.

6. Доступ к материально-техническим средствам обеспечения образовательной деятельности

6.1. Доступ педагогических работников к материально-техническим средствам обеспечения образовательной деятельности осуществляется:

- без ограничения к актовому залу, физкультурному залу и другим помещениям во время, определенное в расписании занятий;

– к актовому залу, физкультурному залу и другим помещениям и местам проведения занятий вне времени, определенного расписанием занятий, по согласованию с работником, ответственным за данное помещение.

6.2. Использование движимых (переносных) материально-технических средств обеспечения образовательной деятельности (проекторы и т.п.) осуществляется по письменной заявке, поданной педагогическим работником (не менее чем за 5 рабочих дней до дня использования материально-технических средств) на имя лица, ответственного за сохранность и правильное использование соответствующих средств.

Выдача педагогическому работнику и сдача им движимых (переносных) материально-технических средств обеспечения образовательной деятельности фиксируются в журнале выдачи.

6.3. Для копирования, распечатывания или тиражирования учебных и методических материалов педагогические работники имеют право пользоваться копировальной техникой.

7. Накопители информации (CD-диски, флеш-накопители, карты памяти), используемые педагогическими работниками при работе с компьютерной информацией, предварительно должны быть проверены на отсутствие вредоносных компьютерных программ.

КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ
И ШЭДЖЭМ КУЕЙМ
И АДМИНИСТРАЦЭМ ШЦЭНЫГЪЭ
ГУЭХУХЭМКІЭ МУНИЦИПАЛЬНЭ
КІЭЗОНЭ ГУЭХУЦІАШІЭ

КЪАБАРТЫ-МАЛКЪАР РЕСПУБЛИКАНЫ
МУНИЦИПАЛ КАЗНА УЧРЕЖДЕНИЯСЫ
«ЧЕГЕМ РАЙОННУ ЖЕР ЖЕРЛИ
АДМИНИСТРАЦИЯСЫНЫ ИЛІМУ БИЛИМ
БЕРІУ УПРАВЛЕНИЯСЫ»

Министерство образования и науки КБР
Управление образования Чегемского муниципального района
Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа №2 им. Инала Пшибиева» с.п.Нартан

Адрес: с.п. Нартан ул.им. Али Тухужева,1 тел./факс (86630) 9-74-98, email: elbrusnartan@yandex.r



Утверждаю
Директор
А.А.Кунижев

КЛАССИФИКАТОР

**информации, не имеющей отношения к образовательному процессу в
муниципальном казенном общеобразовательном учреждении «СОШ №2 имени Инала
Пшибиева» с.п.Нартан**

1. Классификацию информации, запрещенной законодательством Российской Федерации к распространению и не имеющей отношения к образовательному процессу, осуществляют специальные экспертно-консультативные органы (советы) при органах управления образованием.
2. Классификатор информации, запрещенной законодательством Российской Федерации к распространению, применяется в единообразном виде на всей территории Российской Федерации.
3. Классификатор информации, не имеющей отношения к образовательному процессу, может содержать как части (разделы), рекомендуемые к применению в единообразном виде на всей территории Российской Федерации, так и части (разделы), рекомендуемые к использованию экспертно-консультативными органами (советами) регионального и (или) муниципального уровня.
4. В соответствии с законодательством Российской Федерации образовательное учреждение свободно в выборе и применении классификаторов информации, не имеющей отношения к образовательному процессу, а также несет ответственность за невыполнение функций, отнесенных к его компетенции.
5. Рекомендации по формированию Классификатора информации, распространение которой запрещено в соответствии с законодательством Российской Федерации, разработаны в соответствии с проведенным анализом законодательства Российской Федерации и международных договоров Российской Федерации.

№№	Тематическая категория	Содержание
1	Пропаганда войны, разжигание ненависти и вражды, пропаганда порнографии и антиобщественного поведения	<ul style="list-style-type: none"> • Информация, направленная на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды; • информация, пропагандирующая порнографию, культ насилия и жестокости, наркоманию, токсикоманию, антиобщественное поведение
2	Злоупотребление свободой СМИ — экстремизм	Информация, содержащая публичные призывы к осуществлению террористической деятельности, оправдывающая терроризм, содержащая другие экстремистские материалы
3	Злоупотребление свободой СМИ — наркотические средства	Сведения о способах, методах разработки, изготовления и использования, местах приобретения наркотических средств, психотропных веществ и их прекурсоров, пропаганда какихлибо преимуществ использования отдельных наркотических средств, психотропных веществ, их аналогов и прекурсоров
4	Злоупотребление свободой СМИ — информация с ограниченным доступом	Сведения о специальных средствах, технических приемах и тактике проведения контртеррористических операций
5	Злоупотребление свободой СМИ — скрытое воздействие	Информация, содержащая скрытые вставки и иные технические способы воздействия на подсознание людей и (или) оказывающая вредное влияние на их здоровье
6	Экстремистские материалы или экстремистская деятельность (экстремизм)	<p>А) Экстремистские материалы, то есть предназначенные для обнародования документы или информация, призывающие к осуществлению экстремистской деятельности либо обосновывающие или оправдывающие необходимость осуществления такой деятельности, в том числе труды руководителей национал-социалистской рабочей партии Германии, фашистской партии Италии; публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство либо оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической, социальной, расовой, национальной или религиозной группы;</p> <p>Б) экстремистская деятельность (экстремизм) включает деятельность по распространению материалов (произведений), содержащих хотя бы один из следующих признаков:</p> <ul style="list-style-type: none"> • насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации; • подрыв безопасности Российской Федерации, захват или присвоение властных полномочий, создание незаконных вооруженных формирований; • осуществление террористической деятельности либо публичное оправдание терроризма; • возбуждение расовой, национальной или религиозной розни, а также социальной розни, связанной с насилием или призывами к насилию;

		<ul style="list-style-type: none"> • унижение национального достоинства; • осуществление массовых беспорядков, хулиганских действий и актов вандализма по мотивам идеологической, политической, расовой, национальной или религиозной ненависти либо вражды, а равно по мотивам ненависти либо вражды в отношении какой-либо социальной группы; • пропаганда исключительности, превосходства либо неполноценности граждан по признаку их отношения к религии, социальной, расовой, национальной, религиозной или языковой принадлежности; • воспрепятствование законной деятельности органов государственной власти, избирательных комиссий, а также законной деятельности должностных лиц указанных органов, комиссий, сопровождаемое насилием или угрозой его применения; • публичная клевета в отношении лица, замещающего государственную должность Российской Федерации или государственную должность субъекта Российской Федерации, при исполнении им своих должностных обязанностей или в связи с их исполнением, сопровождаемая обвинением указанного лица в совершении деяний, указанных в настоящей статье, при условии, что факт клеветы установлен в судебном порядке; • применение насилия в отношении представителя государственной власти либо угроза применения насилия в отношении представителя государственной власти или его близких в связи с исполнением им своих должностных обязанностей; • посягательство на жизнь государственного или общественного деятеля, совершенное в целях прекращения его государственной или иной политической деятельности либо из мести за такую деятельность; • нарушение прав и свобод человека и гражданина, причинение вреда здоровью и имуществу граждан в связи с их убеждениями, расовой или национальной принадлежностью, вероисповеданием, социальной принадлежностью или социальным происхождением
7	Вредоносные программы	Программы для ЭВМ, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети
8	Преступления	<ul style="list-style-type: none"> • Клевета (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию); • оскорбление (унижение чести и достоинства другого лица, выраженное в неприличной форме); • публичные призывы к осуществлению террористической деятельности или публичное

		оправдание терроризма; <ul style="list-style-type: none"> • склонение к потреблению наркотических средств и психотропных веществ; • незаконное распространение или рекламирование порнографических материалов; • публичные призывы к осуществлению экстремистской деятельности; • информация, направленная на пропаганду национальной, классовой, социальной нетерпимости, а также социального, расового, национального и религиозного неравенства; • публичные призывы к развязыванию агрессивной войны
9	Ненадлежащая реклама	Информация, содержащая рекламу алкогольной продукции и табачных изделий
10	Информация с ограниченным доступом	Информация, составляющая государственную, коммерческую, служебную или иную охраняемую законом тайну

6. Приводимый далее перечень категорий Классификатора информации, не имеющей отношения к образовательному процессу, носит рекомендательный характер и может быть дополнен, расширен или иным образом изменен в установленном порядке, в том числе с учетом специфики образовательного учреждения, социокультурных особенностей автономного округа и иных обстоятельств.

№№	Тематическая категория	Содержание
1	Алкоголь	Реклама алкоголя, пропаганда потребления алкоголя. Сайты компаний, производящих алкогольную продукцию
2	Баннеры и рекламные программы	Баннерные сети, всплывающая реклама, рекламные программы
3	Вождение и автомобили (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация об автомобилях и других транспортных средствах, вождении, автозапчастях, автомобильных журналах, техническом обслуживании, аксессуарах к автомобилям
4	Досуг и развлечения (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация: <ul style="list-style-type: none"> • ТВ-программы; • прогнозы погоды; • тесты, конкурсы онлайн; • туризм, путешествия; • тосты, поздравления; • кроссворды, сканворды, ответы к ним; • фантастика; • кулинария, рецепты, диеты; • мода, одежда, обувь, модные аксессуары, показы мод; • тексты песен, кино, киноактеры, расписания концертов, спектаклей, кинофильмов, заказ билетов в театры, кино и т.п.; • о дачах, участках, огородах, садах, цветоводстве,

		<p>животных, питомцах, уходе за ними;</p> <ul style="list-style-type: none"> • о рукоделии, студенческой жизни, музыке и музыкальных направлениях, группах, увлечениях, хобби, коллекционировании; • о службах знакомств, размещении объявлений онлайн; • анекдоты, «приколы», слухи; • о сайтах и журналах для женщин и для мужчин; • желтая пресса, онлайн-ТВ, онлайн-радио; • о знаменитостях; • о косметике, парфюмерии, прическах, ювелирных украшениях. • фотоальбомы и фотоконкурсы; • рейтинги открыток, гороскопов, сонников; • гадания, магия и астрология;
5	Здоровье и медицина (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющая отношения к образовательному процессу информация о шейпинге, фигуре, похудении, медицине, медицинских учреждениях, лекарствах, оборудовании, а также иные материалы на тему «Здоровье и медицина», которые, являясь академическими, по сути, могут быть также отнесены к другим категориям (порнография, трупы и т.п.)
6	Компьютерные игры (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющие отношения к образовательному процессу компьютерные онлайн-овые и оффлайн-овые игры, советы для игроков и ключи для прохождения игр, игровые форумы и чаты
7	Корпоративные сайты, интернетпредставительства негосударственных учреждений (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, сайты коммерческих фирм, компаний, предприятий, организаций
8	Личная и немодерируемая информация	Немодерируемые форумы, доски объявлений и конференции, гостевые книги, базы данных, содержащие личную информация информацию (адреса, телефоны и т. п.), личные странички, дневники, блоги
9	Отправка SMS с использованием интернет-ресурсов	Сайты, предлагающие услуги по отправке SMS-сообщений
10	Модерируемые доски объявлений (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, модерируемые доски сообщений/объявлений, а также модерируемые чаты
11	Нелегальная помощь школьникам	Банки готовых рефератов, эссе, проектных работ и пр.

12	Неприличный и грубый юмор	Неэтичные анекдоты и шутки, в частности обыгрывающие особенности физиологии человека
13	Нижнее белье, купальники	Сайты, на которых рекламируется и изображается нижнее белье и купальники
14	Обеспечение анонимности пользователя, обход контентных фильтров	Сайты, предлагающие инструкции по обходу прокси и доступу к запрещенным страницам; Peer-to-Peer программы, сервисы бесплатных прокси-серверов, сервисы, дающие пользователю анонимность
15	Онлайн-казино и тотализаторы	Электронные казино, тотализаторы, игры на деньги, конкурсы и пр.
16	Платные сайты	Сайты, на которых вывешено объявление о платности посещения веб-страниц
17	Поиск работы, резюме, вакансии (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-представительства кадровых агентств, банки вакансий и резюме
18	Поисковые системы (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Содержащие информацию, не имеющую отношения к образовательному процессу, интернет-каталоги, системы поиска и навигации в Интернете
19	Религии и атеизм (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Сайты, содержащие, не имеющую отношения к образовательному процессу, информацию религиозной и антирелигиозной направленности.
20	Системы поиска изображений	Системы для поиска изображений в Интернете по ключевому слову или словосочетанию
21	СМИ (ресурсы СМИ, содержащие новостные ресурсы и сайты данной категории, не имеющие отношения к образовательному процессу)	СМИ, содержащие новостные ресурсы и сайты СМИ (радио, телевидения, печати), не имеющие отношения к образовательному процессу.
22	Табак, реклама табака, пропаганда потребления табака	Сайты, пропагандирующие потребление табака; реклама табака и изделий из него
23	Торговля и реклама (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Сайты, не имеющие отношения к образовательному процессу, сайты следующих категорий: аукционы, распродажи онлайн, интернет-магазины, каталоги товаров и цен, электронная коммерция, модели мобильных телефонов, юридические услуги, полиграфия, типографии и их услуги, таможенные услуги, охранные услуги, иммиграционные услуги, услуги по переводу текста на иностранные языки, канцелярские товары, налоги, аудит, консалтинг, деловая литература, дом, ремонт, строительство, недвижимость, аренда недвижимости,

		покупка недвижимости, продажа услуг мобильной связи (например, картинки и мелодии для сотовых телефонов), заработок в Интернете, е-бизнес
24	Убийства, насилие	Сайты, содержащие описание или изображение убийств, мертвых тел, насилия и т.п.
25	Чаты (ресурсы данной категории, не имеющие отношения к образовательному процессу)	Не имеющие отношения к образовательному процессу сайты для анонимного общения в режиме онлайн.

КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ
И ШЭДЖЭМ КУЕЙМ
И АДМИНИСТРАЦЭМ ШЦІЭНЫГЪЭ
ІУЭХУХЭМКІЭ МУНИЦИПАЛЬНЭ
КІЭЗОНЭ ІУЭХУЦІАПІЭ

КЪАБАРТЫ-МАЛЪАР РЕСПУБЛИКАНЫ
МУНИЦИПАЛ КАЗНА УЧРЕЖДЕНИЯСЫ
«ЧЕГЕМ РАЙОННУ ЖЕР ЖЕРЛИ
АДМИНИСТРАЦИЯСЫНЫ ІЛМУ БИЛИМ
БЕРІУ УПРАВЛЕНИЯСЫ»

Министерство образования и науки КБР
Управление образования Чегемского муниципального района
Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа №2 им. Инала Пшибиева» с. п.Нартан

Адрес: с.п. Нартан ул. им. Али Тухужева,1 тел./факс (86630) 9-74-98, email: elbrusnartan@yandex.r

Утверждаю
Директор
А.А.Кунижев

РЕГЛАМЕНТ

работы с электронной почтой в МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан

1. Общие положения

1.1. Муниципальное казенное общеобразовательное учреждение «СОШ №2 имени Инала Пшибиева» с.п.Нартан (далее – ОУ) имеет свой адрес электронной почты: elbrusnartan@yandex.ru

1.2. Электронная почта в ОУ может использоваться только в административных и образовательных целях.

1.3. Пользователи и владельцы электронных почтовых ящиков должны соблюдать правила и инструкции по работе с электронной почтой, этические нормы общения.

1.4. Перед отправлением сообщения или отчета необходимо проверить правописание и грамматику текста.

1.5. Пользователям данного сервиса запрещено:

– участвовать в рассылке посланий, не связанных с образовательной или административной деятельностью ОУ;

– пересылать по произвольным адресам не затребованную потребителями информацию (спам); – отправлять сообщения противозаконного или неэтического содержания;

– использовать массовую рассылку электронной почты, за исключением необходимых случаев; – электронное послание не должно использоваться для пересылки секретной и конфиденциальной информации, регламент обмена которыми утверждается иными нормативно-правовыми актами.

2. Порядок обработки, передачи и приёма документов по электронной почте

2.1. По электронной почте производится получение и отправка информации законодательного, нормативно-правового, учебного, учебно-методического характера, а также любой другой информации, совместимой с процессом образования

2.2. Для обработки, передачи и приема информации по электронной почте в ОУ приказом директора назначается ответственное лицо – оператор электронной почты.

2.3. При создании электронного почтового ящика (ЭПЯ), сайта ОУ ответственное лицо направляет в муниципальный орган управления образованием свои электронные реквизиты для формирования базы данных образовательных учреждений муниципалитета.

2.4. Администрация ОУ должна обеспечить бесперебойное функционирование сервиса электронной почты и регулярное получение и отpravку информации в течение всего рабочего дня.

2.5. Ответственность за ненадлежащую подготовку информации к передаче по электронной почте несет автор информации, предполагаемой к отправке.

2.6. Ответственность за отправку адресату и получение электронной почты несет оператор электронной почты

2.7. Передаваемые с помощью электронной почты официальные документы должны иметь исходящий регистрационный номер.

2.8. Все передаваемые учебно-методические и справочно-информационные материалы должны передаваться с сопроводительным письмом.

Для отправки электронного сообщения пользователь оформляет документ в соответствии с требованиями по делопроизводству, утвержденными в ОУ.

2.9. При получении электронного сообщения оператор: – передает документ на рассмотрение администрации ОУ или в случае именного сообщения - непосредственно адресату; – в случае невозможности прочтения электронного сообщения уведомляет об этом отправителя.

2.10. Отправка и получение электронных документов осуществляется с использованием программных продуктов, предназначенных для работы с электронной почтой в ОУ.

2.11. Учет электронных документов осуществляется путем регистрации в журнале регистрации входящих / исходящих документов.

2.12. Электронные документы дублируются в виде копий на бумажных носителях с присвоением номера входящего или исходящего документа. Сроки их хранения регламентируются иными нормативными актами.

3. Ответственность

3.1. Изменение наименования официального ЭПЯ ОУ согласовывает со специалистами Управления образования Чегемского муниципального района, ведущими электронный документооборот и отвечающими за информатизацию системы муниципального образования.

3.2. По факту изменения официального ЭПЯ ОУ обязано уведомить информационным письмом Управление образования Администрации Гаврилов-Ямского района Ярославской области за 3 рабочих дня до смены ЭПЯ с указанием даты, с которой изменения вступают в силу.

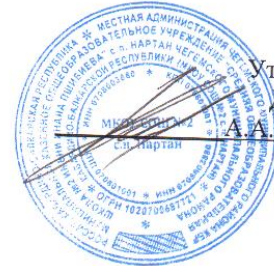
3.3. Ответственность за функционирование электронного документооборота в учреждении несет директор ОУ.

КЪЭБОРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ
И ШЭДЖЭМ КУЕЙМ
И АДМИНИСТРАЦЭМ ЦЦЭНЬГЪЭ
ГУЭХУХЭМКІЭ МУНИЦИПАЛЪНЭ
КІЭЗОНЭ ГУЭХУЦІАПІЭ

КЪАБАРТЫ-МАЛЪБАР РЕСПУБЛИКАНЫ
МУНИЦИПАЛ КАЗНА УЧРЕЖДЕНИЯСЫ
«ЧЕГЕМ РАЙОННУ ЖЕР ЖЕРЛИ
АДМИНИСТРАЦИЯСЫНЫ ИЛМУ БИЛИМ
БЕРНУ УПРАВЛЕНИЯСЫ»

Министерство образования и науки КБР
Управление образования Чегемского муниципального района
Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа №2 им. Инала Пшибиева» с.п.Нартан

Адрес: с.п. Нартан ул. им. Али Тухужева.1 тел./факс (86630) 9-74-98, email: elbrusnartan@yandex.r



Утверждаю
Директор
А.А.Кунижев

ИНСТРУКЦИЯ

для педагогических работников и сотрудников муниципального казенного общеобразовательного учреждения «СОШ №2 имени Инала Пшибиева» с.п.Нартан о порядке действий при осуществлении контроля использования обучающимися сети Интернет

1. Настоящая инструкция устанавливает порядок действий сотрудников образовательного учреждения при обнаружении:
 - 1) обращения обучающихся к контенту, не имеющему отношения к образовательному процессу;
 - 2) отказа при обращении к контенту, имеющему отношение к образовательному процессу, вызванного техническими причинами.
2. Контроль использования обучающимися сети Интернет осуществляют:
 - 1) во время занятия — проводящий его преподаватель;
 - 2) во время использования сети Интернет для свободной работы обучающихся — дежурный преподаватель.
3. Преподаватель: — определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательном процессе соответствующих технических возможностей, а также длительность сеанса работы одного обучающегося;
 - наблюдает за использованием обучающимися компьютеров и сети Интернет;
 - способствует осуществлению контроля объемов трафика ОУ в сети Интернет;
 - запрещает дальнейшую работу обучающегося в сети Интернет на уроке (занятии) в случае нарушения им порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;

1.6. Контроль информации на съёмных носителях производится непосредственно перед её использованием.

1.7. Файлы, помещаемые в электронный архив или на сервер, должны в обязательном порядке проходить антивирусный контроль.

1.8. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

1.9. Факт выполнения антивирусной проверки должен регистрироваться в специальном журнале за подписью лица, ответственного за организацию антивирусной защиты.

2. Мероприятия, направленные на решение задач по антивирусной защите:

2.1. Установка только лицензированного программного обеспечения либо бесплатного антивирусного программного обеспечения.

2.2. Регулярное обновление и профилактические проверки (обновление ежедневное; профилактические проверки: 1 раз в неделю во вторник с 12.00).

2.3. Непрерывный контроль над всеми возможными путями проникновения вредоносных программ, мониторинг антивирусной безопасности и обнаружение деструктивной активности вредоносных программ на всех объектах информационнокоммуникационной системы (далее ИКС) ОУ.

2.4. Проведение профилактических мероприятий по предотвращению и ограничению вирусных эпидемий, включающих загрузку и развертывание специальных правил нейтрализации (отражению, изоляции и ликвидации) вредоносных программ на основе рекомендаций по контролю атак, подготавливаемых разработчиком средств защиты от вредоносных программ и другими специализированными экспертными антивирусными службами до того, как будут выпущены файлы исправлений, признаков и антивирусных сигнатур.

2.5. Внешние носители информации неизвестного происхождения следует проверять на наличие вирусов до их использования.

2.6. Необходимо строго придерживаться установленных процедур по уведомлению о случаях поражения автоматизированной информационной среды компьютерными вирусами и принятию мер по ликвидации последствий от их проникновения.

2.7. Обеспечение бесперебойной работы ОУ для случаев вирусного заражения, в том числе резервного копирования всех необходимых данных и программ и их восстановления.

3. Требования к проведению мероприятий по антивирусной защите

3.1. Ежедневно в начале работы при загрузке компьютера (для серверов ЛВС – при перезагрузке) в автоматическом режиме должно выполняться обновление антивирусных баз и серверов и проводиться антивирусный контроль всех дисков и файлов персонального компьютера и съёмных носителей.

3.2. Периодические проверки компьютеров должны проводиться не реже одного раза в неделю. 3.3. Внеочередной антивирусный контроль всех дисков и файлов персонального компьютера должен выполняться:

3.3.1. непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети) должна быть выполнена антивирусная проверка на серверах и персональных компьютерах ОУ;

3.3.2. при возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.);

3.3.3. при отправке и получении электронной почты оператор электронной почты обязан проверить электронные письма и их вложения на наличие вирусов.

4. Действия сотрудников при обнаружении компьютерного вируса

4.1. В случае обнаружения зараженных компьютерными вирусами файлов или электронных писем пользователи обязаны:

4.1.1. приостановить работу;

4.1.2. немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ответственного за обеспечение антивирусной защиты в ОУ;

4.1.3. совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

4.1.4. провести лечение или уничтожение зараженных файлов.

4.2. При возникновении подозрения на наличие компьютерного вируса ответственный за организацию антивирусной защиты должен провести внеочередной антивирусный контроль.

5. Ответственность

5.1. Ответственность за организацию антивирусной защиты и выполнение положений данной инструкции возлагается на лицо, назначенное директором ОУ.

5.2. Ответственность за проведение мероприятий антивирусного контроля в ОУ возлагается на ответственного за организацию антивирусной защиты.

5.3. Ответственность за соблюдение требований настоящей Инструкции при работе на персональных рабочих станциях возлагается на пользователей данных станций или педагога, отвечающего за работу компьютерного класса.

5.4. Периодический контроль за состоянием антивирусной защиты в ОУ осуществляется директором ОУ и фиксируется Актом проверки (не реже 1 раза в квартал).

КЪЭБЭРДЕЙ-БАЛЪКЪЭР РЕСПУБЛИКЭМ
И ШЭДЖЭМ КУЕЙМ
И АДМИНИСТРАЦЭМ ЦЦЭНЬГЪЭ
ІУЭХУХЭМКІЭ МУНИЦИПАЛНО
КІЭЗОНЭ ІУЭХУЦАПІЭ

КЪАБАРТЫ-МАЛЪБАР РЕСПУБЛИКАНЫ
МУНИЦИПАЛ КАЗНА УЧРЕЖДЕНИЯСЫ
«ЧЕГЕМ РАЙОННУ ЖЕР ЖЕРЛИ
АДМИНИСТРАЦИЯСЫНЫ ИЛМУ БИЛИМ
БЕРІУ УПРАВЛЕНИЯСЫ»

Министерство образования и науки КБР
Управление образования Чегемского муниципального района
Муниципальное казенное общеобразовательное учреждение
«Средняя общеобразовательная школа №2 им. Инала Пшибиева» с.п.Нартан

Адрес: с.п. Нартан ул. им. Али Тухужева,1 тел./факс (86630) 9-74-98, email: elbrusnartan@vandex.r

Принят
на педагогическом совете
Протокол № 1
от «30» 08. 2018 г.



ПОЛОЖЕНИЕ

об электронном классном журнале МКОУ «СОШ №2 имени Инала Пшибиева» с.п.Нартан

1. Общие положения

1.1. Электронным классным журналом называется комплекс программных средств, включающий базу данных и средства доступа к ней (подсистема «электронный журнал» в АИС «Электронный журнал» school.07.edu.o7.com)

1.2. Пользователями электронного журнала являются администрация школы, учителя и классные руководители.

1.3. Электронный классный журнал служит для решения следующих задач:

1.3.1. хранение данных об календарно-тематическом планирование по всем предметам, об успеваемости и посещаемости обучающихся;

1.3.2. оперативный доступ к оценкам за весь период ведения журнала, по всем предметам, в любое время;

1.3.3. автоматизация создания периодических отчетов учителей и администрации;

1.3.4. своевременное информирование родителей по вопросам успеваемости их детей.

1.4. Поддержание информации хранящейся в базе данных электронного классного журнала в актуальном состоянии является обязательным.

1.5. Категорически запрещается допускать учащихся к работе с электронным журналом.

2. Правила и порядок работы с электронным классным журналом

2.1. Заместитель директора по УВР, отвечающий за информатизацию ОУ обеспечивает надлежащее функционирование программно-аппаратной среды.

2.2. Пользователи получают реквизиты (логин и пароль) доступа к электронному журналу в следующем порядке:

2.2.1. Классные руководители, администрация получают реквизиты доступа у ответственного администратора по работе в АИС;

2.2.2. Родители получают реквизиты доступа к электронному дневнику у классного руководителя по заявлению (приложение 1).

2.3. Учителя аккуратно и своевременно заполняют пройденные темы уроков, данные об успеваемости и посещаемости учащихся.

2.4. Заместитель директора по УВР осуществляют периодический контроль за ведением электронного журнала: своевременность выставления отметок учителями, заполнения тем, заинтересованность родителей в данной электронной услуге.

2.5. Родители имеют доступ только к собственным данным и используют электронный дневник для их просмотра.

3. Права и обязанности пользователей

3.1. Права:

3.1.1. Все пользователи имеют право на своевременные консультации по вопросам работы с электронным журналом;

3.2. Обязанности:

3.2.1. Заместитель директора по информатизации несет ответственность за техническое функционирование электронного журнала.

3.2.2. Учителя несут ответственность за ежедневное и достоверное заполнение журнала (тема урока, оценки и отметки о посещаемости учащихся);

3.2.3. Классные руководители несут ответственность за актуальность данных: списки класса, данные об успеваемости и посещаемости и за своевременное оповещение родителей о проблемах, связанных с поведением ребёнка в школе.

3.2.4. Все пользователи несут ответственность за сохранность своих реквизитов доступа;

3.2.5. Все пользователи несут ответственность за сохранность персональных данных обучающихся.

Методические рекомендации «Безопасный Интернет»

В наши дни компьютер становится привычным элементом не только в научных лабораториях, но и дома, в школьных классах. Так, например, в Российской Федерации в настоящее время уже эксплуатируется не менее 5 млн. персональных компьютеров. В Западной Европе компьютер используют свыше 60% взрослого населения. Людей, ежедневно проводящих за компьютером по несколько часов, становится все больше. При этом уже мало кто сомневается, что работа на персональном компьютере влияет на физическое и психологическое здоровье человека не самым лучшим образом. Длительное пребывание у экрана, неподвижность позы пользователя ПК, электромагнитные поля и излучения, мелькание изображения на экране – все это небезвредно для здоровья.

Бурное развитие компьютерных технологий и широкое распространение сети Интернет открывает перед людьми большие возможности для общения и саморазвития. Мы понимаем, что Интернет - это не только кладезь возможностей, но и источник угроз. Сегодня количество пользователей российской сети Интернет составляет десятки миллионов людей, и немалая часть из них - дети, которые могут не знать об опасностях мировой паутины.

Одним из средств решения этой проблемы может стать просвещение общественности и специальная подготовка профессионалов, в первую очередь, педагогов в сфере безопасного поведения человека, специалиста, школьника в мире компьютерных технологий и Интернет. В данном разделе представлены материалы для разработки классных часов для школьников трех возрастных групп, направленные на обеспечение необходимыми знаниями в области психолого-педагогического и здоровьесберегающего сопровождения образовательного процесса, персонала и школьников, использующих персональные компьютеры и Интернет в профессиональной, учебной и внеучебной деятельности. Кроме того, пособие может быть интересно родителям школьников, так как содержит советы и рекомендации, как сделать компьютер и Интернет безопасным для своего ребенка.

Данные рекомендации - практическая информация для родителей и классных руководителей, которая поможет предупредить угрозы и сделать работу детей в Интернете полезной.

Памятка для родителей об информационной безопасности детей

Памятка для родителей об информационной безопасности детей

ОПРЕДЕЛЕНИЕ ТЕРМИНА "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ" СОДЕРЖИТСЯ В ФЕДЕРАЛЬНОМ ЗАКОНЕ N 436-ФЗ "О ЗАЩИТЕ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И РАЗВИТИЮ", РЕГУЛИРУЮЩИМ ОТНОШЕНИЯ, СВЯЗАННЫЕ С ЗАЩИТОЙ ДЕТЕЙ ОТ ИНФОРМАЦИИ, ПРИЧИНЯЮЩЕЙ ВРЕД ИХ ЗДОРОВЬЮ И (ИЛИ) РАЗВИТИЮ. СОГЛАСНО ДАННОМУ ЗАКОНУ "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ДЕТЕЙ" - ЭТО СОСТОЯНИЕ ЗАЩИЩЕННОСТИ, ПРИ КОТОРОМ ОТСУТСТВУЕТ РИСК, СВЯЗАННЫЙ С ПРИЧИНЕНИЕМ ИНФОРМАЦИЕЙ ВРЕДА ИХ ЗДОРОВЬЮ И (ИЛИ) ФИЗИЧЕСКОМУ, ПСИХИЧЕСКОМУ, ДУХОВНОМУ, НРАВСТВЕННОМУ РАЗВИТИЮ.

В СИЛУ ФЕДЕРАЛЬНОГО ЗАКОНА N 436-ФЗ ИНФОРМАЦИЕЙ, ПРИЧИНЯЮЩЕЙ ВРЕД ЗДОРОВЬЮ И (ИЛИ) РАЗВИТИЮ ДЕТЕЙ, ЯВЛЯЕТСЯ:

1. информация, запрещенная для распространения среди детей;
2. информация, распространение которой ограничено среди детей определенных возрастных категорий.
3. К информации, запрещенной для распространения среди детей, относится:
4. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;
5. способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
6. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
7. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
8. оправдывающая противоправное поведение;
9. содержащая нецензурную брань;
10. содержащая информацию порнографического характера.

К ИНФОРМАЦИИ, РАСПРОСТРАНЕНИЕ КОТОРОЙ ОГРАНИЧЕНО СРЕДИ ДЕТЕЙ ОПРЕДЕЛЕННОГО ВОЗРАСТА, ОТНОСИТСЯ:

1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
2. вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
4. содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С УЧЕТОМ ЭТОГО ВАМ ПРЕДЛАГАЮТСЯ ПРАВИЛА РАБОТЫ В СЕТИ ИНТЕРНЕТ ДЛЯ РАЗЛИЧНЫХ ВОЗРАСТНЫХ КАТЕГОРИЙ, СОБЛЮДЕНИЕ КОТОРЫХ ПОЗВОЛИТ ОБЕСПЕЧИТЬ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ВАШИХ ДЕТЕЙ.

ОБЩИЕ ПРАВИЛА ДЛЯ РОДИТЕЛЕЙ

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку - главный метод защиты.
2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)
4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающим и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).
5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

ВОЗРАСТ ОТ 7 ДО 8 ЛЕТ

В ИНТЕРНЕТЕ РЕБЕНОК СТАРАЕТСЯ ПОСЕТИТЬ ТЕ ИЛИ ИНЫЕ САЙТЫ, А ВОЗМОЖНО И ЧАТЫ, РАЗРЕШЕНИЕ НА ПОСЕЩЕНИЕ КОТОРЫХ ОН НЕ ПОЛУЧИЛ БЫ ОТ РОДИТЕЛЕЙ. ПОЭТОМУ РОДИТЕЛЯМ ОСОБЕННО ПОЛЕЗНЫ БУДУТ ТЕ ОТЧЕТЫ, КОТОРЫЕ ПРЕДОСТАВЛЯЮТСЯ ПРОГРАММАМИ ПО ОГРАНИЧЕНИЮ ИСПОЛЬЗОВАНИЯ ИНТЕРНЕТА, Т.Е. РОДИТЕЛЬСКИЙ КОНТРОЛЬ ИЛИ ТО, ЧТО ВЫ СМОЖЕТЕ УВИДЕТЬ ВО ВРЕМЕННЫХ ФАЙЛАХ. В РЕЗУЛЬТАТЕ, У РЕБЕНКА НЕ БУДЕТ ОЩУЩЕНИЯ, ЧТО ЗА НИМ ВЕДЕТСЯ ПОСТОЯННЫЙ КОНТРОЛЬ, ОДНАКО, РОДИТЕЛИ БУДУТ ПО-ПРЕЖНЕМУ ЗНАТЬ, КАКИЕ САЙТЫ ПОСЕЩАЕТ ИХ РЕБЕНОК. ДЕТИ В ДАННОМ ВОЗРАСТЕ ОБЛАДАЮТ СИЛЬНЫМ ЧУВСТВОМ СЕМЬИ, ОНИ ДОВЕРЧИВЫ И НЕ СОМНЕВАЮТСЯ В АВТОРИТЕТАХ. ОНИ ЛЮБЯТ ИГРАТЬ В СЕТЕВЫЕ ИГРЫ И ПУТЕШЕСТВОВАТЬ ПО ИНТЕРНЕТУ, ИСПОЛЬЗУЯ ЭЛЕКТРОННУЮ ПОЧТУ, ЗАХОДИТЬ НА САЙТЫ И ЧАТЫ, НЕ РЕКОМЕНДОВАННЫЕ РОДИТЕЛЯМИ.

СОВЕТЫ ПО БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ ДЛЯ ДЕТЕЙ 7 - 8 ЛЕТ

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь.
3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
4. Используйте специальные детские поисковые машины.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
8. Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
9. Научите детей не загружать файлы, программы или музыку без вашего согласия.
10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.
11. В "белый" список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
13. Не делайте "табу" из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты "для взрослых".
14. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

ВОЗРАСТ ДЕТЕЙ ОТ 9 ДО 12 ЛЕТ

В ДАННОМ ВОЗРАСТЕ ДЕТИ, КАК ПРАВИЛО, УЖЕ НАСЛЫШАНЫ О ТОМ, КАКАЯ ИНФОРМАЦИЯ СУЩЕСТВУЕТ В ИНТЕРНЕТЕ. СОВЕРШЕННО НОРМАЛЬНО, ЧТО ОНИ ХОТЯТ ЭТО УВИДЕТЬ, ПРОЧЕСТЬ, УСЛЫШАТЬ. ПРИ ЭТОМ НУЖНО ПОМНИТЬ, ЧТО ДОСТУП К НЕЖЕЛАТЕЛЬНЫМ МАТЕРИАЛАМ МОЖНО ЛЕГКО ЗАБЛОКИРОВАТЬ ПРИ ПОМОЩИ СРЕДСТВ РОДИТЕЛЬСКОГО КОНТРОЛЯ.

СОВЕТЫ ПО БЕЗОПАСНОСТИ ДЛЯ ДЕТЕЙ ОТ 9 ДО 12 ЛЕТ

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.
3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.
4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.
5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Не забывайте принимать непосредственное участие в жизни ребенка, беседовать с детьми об их друзьях в Интернете.
7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
8. Позволяйте детям заходить только на сайты из "белого" списка, который создайте вместе с ними.
9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.

12. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.
13. Расскажите детям о порнографии в Интернете.
14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

ВОЗРАСТ ДЕТЕЙ ОТ 13 ДО 17 ЛЕТ

В ЭТОМ ВОЗРАСТЕ ПОДРОСТКИ АКТИВНО ИСПОЛЬЗУЮТ ПОИСКОВЫЕ МАШИНЫ, ПОЛЬЗУЮТСЯ ЭЛЕКТРОННОЙ ПОЧТОЙ, СЛУЖБАМИ МГНОВЕННОГО ОБМЕНА СООБЩЕНИЯМИ, СКАЧИВАЮТ МУЗЫКУ И ФИЛЬМЫ. МАЛЬЧИКАМ В ЭТОМ ВОЗРАСТЕ БОЛЬШЕ ПО НРАВУ СМЕТАТЬ ВСЕ ОГРАНИЧЕНИЯ, ОНИ ЖАЖДУТ ГРУБОГО ЮМОРА, АЗАРТНЫХ ИГР, КАРТИНОК "ДЛЯ ВЗРОСЛЫХ". ДЕВОЧКИ ПРЕДПОЧИТАЮТ ОБЩАТЬСЯ В ЧАТАХ, ПРИ ЭТОМ ОНИ ГОРАЗДО БОЛЕЕ ЧУВСТВИТЕЛЬНЫ К СЕКСУАЛЬНЫМ ДОМОГАТЕЛЬСТВАМ В ИНТЕРНЕТЕ.

ЗАЧАСТУЮ В ДАННОМ ВОЗРАСТЕ РОДИТЕЛЯМ УЖЕ ВЕСЬМА СЛОЖНО КОНТРОЛИРОВАТЬ СВОИХ ДЕТЕЙ, ТАК КАК ОБ ИНТЕРНЕТЕ ОНИ УЖЕ ЗНАЮТ ЗНАЧИТЕЛЬНО БОЛЬШЕ СВОИХ РОДИТЕЛЕЙ. ТЕМ НЕ МЕНЕЕ, НЕ ОТПУСКАЙТЕ ДЕТЕЙ В "СВОБОДНОЕ ПЛАВАНИЕ" ПО ИНТЕРНЕТУ. СТАРАЙТЕСЬ АКТИВНО УЧАСТВОВАТЬ В ОБЩЕНИИ РЕБЕНКА В ИНТЕРНЕТЕ.

ВАЖНО ПО-ПРЕЖНЕМУ СТРОГО СОБЛЮДАТЬ ПРАВИЛА ИНТЕРНЕТ-БЕЗОПАСНОСТИ - СОГЛАШЕНИЕ МЕЖДУ РОДИТЕЛЯМИ И ДЕТЬМИ. КРОМЕ ТОГО, НЕОБХОДИМО КАК МОЖНО ЧАЩЕ ПРОСМАТРИВАТЬ ОТЧЕТЫ О ДЕЯТЕЛЬНОСТИ ДЕТЕЙ В ИНТЕРНЕТЕ. СЛЕДУЕТ ОБРАТИТЬ ВНИМАНИЕ НА НЕОБХОДИМОСТЬ СОДЕРЖАНИЯ РОДИТЕЛЬСКИХ ПАРОЛЕЙ (ПАРОЛЕЙ АДМИНИСТРАТОРОВ) В СТРОГОМ СЕКРЕТЕ И ОБРАТИТЬ ВНИМАНИЕ НА СТРОГОСТЬ ЭТИХ ПАРОЛЕЙ.

СОВЕТЫ ПО БЕЗОПАСНОСТИ В ЭТОМ ВОЗРАСТЕ ОТ 13 ДО 17 ЛЕТ

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов ("черный список"), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).
2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.
3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерлируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.

8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
11. Приучите себя знакомиться с сайтами, которые посещают подростки.
12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде - даже в виртуальном мире.
13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.
14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

ПОСТОЯННО КОНТРОЛИРУЙТЕ ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТА ВАШИМ РЕБЕНКОМ! ЭТО НЕ НАРУШЕНИЕ ЕГО ЛИЧНОГО ПРОСТРАНСТВА, А МЕРА ПРЕДОСТОРОЖНОСТИ И ПРОЯВЛЕНИЕ ВАШЕЙ РОДИТЕЛЬСКОЙ ОТВЕТСТВЕННОСТИ И ЗАБОТЫ.

Памятка

для обучающихся по информационной безопасности в сети интернет

Информационная памятка для обучающихся

С каждым годом молодежи в интернете становится больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

Компьютерные вирусы

Компьютерный вирус - это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

1. Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
2. Постоянно устанавливай пачки (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
3. Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ устанавливаться на твоём персональном компьютере;
4. Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
5. Ограничь физический доступ к компьютеру для посторонних лиц;
6. Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;
7. Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Сети WI-FI

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WЕСА», что обозначало словосочетание «Wireless Fidelity», который переводится как «беспроводная точность».

До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высший звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Да, бесплатный интернет-доступ в кафе, отелях и аэропортах является отличной возможностью выхода в интернет. Но многие эксперты считают, что общедоступные WiFi сети не являются безопасными.

Советы по безопасности работе в общедоступных сетях Wi-fi

1. Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
2. Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закладки вируса на твоё устройство;
3. При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
4. Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
5. Используй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
6. В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Социальные сети

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

1. Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
2. Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
3. Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
4. Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
5. Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твоё местоположение;
6. При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
7. Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Электронные деньги

Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах.

В России же они функционируют и о них уже прописано в законе, где их разделяют на несколько видов - анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификация пользователя является обязательной.

Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

1. Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
2. Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
3. Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, StROng!;;
4. Не вводи свои личные данные на сайтах, которым не доверяешь.

Электронная почта

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

1. Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;
2. Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;
3. Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
4. Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
5. Если есть возможность написать самому свой личный вопрос, используй эту возможность;
6. Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
7. Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
8. После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Кибербуллинг или виртуальное издевательство

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

1. Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
2. Управляй своей киберрепутацией;
3. Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
4. Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;
5. Соблюдай свой виртуальную честь смолоду;
6. Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
7. Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
8. Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Мобильный телефон

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений.

Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность.

Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

1. Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
2. Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
3. Необходимо обновлять операционную систему твоего смартфона;
4. Используй антивирусные программы для мобильных телефонов;
5. Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
6. После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;
7. Периодически проверяй какие платные услуги активированы на твоем номере;
8. Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;

- Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Online игры

Современные **онлайн-игры** - это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.

Все эти средства идут на поддержание и развитие игры, а также на самую безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов.

В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

1. Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
2. Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
3. Не указывай личную информацию в профайле игры;
4. Уважай других участников по игре;
5. Не устанавливай неофициальные патчи и моды;
6. Используй сложные и разные пароли;
7. Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Фишинг или кража личных данных

Обычной кражей денег и документов сегодня уже никого не удивишь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься «любимым» делом.

Так появилась новая угроза: интернет-мошенничества или **фишинг**, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль).

Основные советы по борьбе с фишингом:

1. Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
2. Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
3. Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
4. Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзья, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
5. Установи надежный пароль (PIN) на мобильный телефон;
6. Отключи сохранение пароля в браузере;

7. Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Цифровая репутация

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация размещенная в интернете может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете.

Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких - все это накапливается в сети.

Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.

Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающие люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой - как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

1. Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
2. В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
3. Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

Авторское право

Современные школьники- активные пользователи цифрового пространства. Однако далеко не все знают, что пользование многими возможностями цифрового мира требует соблюдения прав на интеллектуальную собственность.

Термин «интеллектуальная собственность» относится к различным творениям человеческого ума, начиная с новых изобретений и знаков, обозначающих собственность на продукты и услуги, и заканчивая книгами, фотографиями, кинофильмами и музыкальными произведениями.

Авторские права - это права на интеллектуальную собственность на произведения науки, литературы и искусства. Авторские права выступают в качестве гарантии того, что интеллектуальный/творческий труд автора не будет напрасным, даст ему справедливые возможности заработать на результатах своего труда, получить известность и признание. Никто без разрешения автора не может воспроизводить его произведение, распространять, публично демонстрировать, продавать, импортировать, пускать в прокат, публично исполнять, показывать/исполнять в эфире или размещать в Интернете.

Использование «пиратского» программного обеспечения может привести к многим рискам: от потери данных к твоим аккаунтам до блокировки твоего устройства, где установленный не легальная программа. Не стоит также забывать, что существует легальные и бесплатные программы, которые можно найти в сети.

О портале

Сетевичок.рф - твой главный советчик в сети. Здесь ты можешь узнать о безопасности в сети понятным и доступным языком, а при возникновении критической ситуации обратиться за советом. А также принять участие в конкурсах и стать самым цифровым гражданином

Памятка для родителей об информационной безопасности детей

Определение термина «информационная безопасность детей» содержится в Федеральном законе № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону «информационная безопасность детей» - это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В силу Федерального закона № 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;
2. информация, распространение которой ограничено среди детей определенных возрастных категорий.

К информации, запрещенной для распространения среди детей, относится:

1. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;
2. способность вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, алкогольную и спиртосодержащую продукцию, пиво и напитки, изготавливаемые на его основе; принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;
3. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
4. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
5. оправдывающая противоправное поведение;
6. содержащая нецензурную брань;
7. содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
2. вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;

3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
4. содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.