**Методические рекомендации**

**для проведения мероприятий по основам информационной безопасности детей.**

Стремительное развитие информационных технологий заставило современное поколение детей и подростков столкнуться с принципиально новыми вызовами. Взросление, обучение и социализация детей проходят в условиях гиперинформационного общества.

Процесс социализации через традиционные институты (семьи, школы) все активнее дополняется средствами массовой информации и массовых коммуникаций, особенно информационно телекоммуникационной сетью "Интернет" (далее - сеть "Интернет"), которые становятся важнейшими институтами социализации, образования и просвещения нового поколения, в определенной мере замещая традиционно сложившиеся формы. В современных условиях развития общества компьютер стал для ребенка и «другом» и «помощником» и даже «воспитателем», «учителем». Всеобщая информатизация и доступный, высокоскоростной Интернет уравнял жителей больших городов и малых деревень в возможности получить качественное образование. В тоже время количество угроз информационной безопасности растет сегодня с каждым днем.

Деятельность по обеспечению информационной безопасности регулируется следующими нормативно-правовыми актами:

- 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 вредоносным содержимым в рамках глобальных сетей;

- Доктрина информационной безопасности Российской Федерации, утверждена Президентом Российской Федерации 09.09.2000 № ПР-1895, в которой закреплены общие принципы обеспечения информационной безопасности граждан и государства;

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

- Федеральный закон от 29.12. 2010 N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (закон закладывает правовые основы для кардинального преобразования информационного пространства российского общества с учетом потребности формирования социальной среды, благоприятной для полноценного психического и нравственно–духовного развития детей);

- Концепция информационной безопасности детей, утверждена распоряжением Правительства Российской Федерации от 02.12. 2015 № 2471-р (результатом реализации Концепции должно стать формирование к 2020 году поколения молодых граждан, которые смогут свободно и самостоятельно ориентироваться в современном информационном пространстве);

- Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации» определяет ответственность образовательной организации по вопросу обеспечения информационной безопасности детей;

- Рекомендации Российской библиотечной ассоциации по реализации норм Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в общедоступных библиотеках России, осуществляющих обслуживание пользователей  до 18-летнего возраста;

- Приказ Генерального прокурора Российской Федерации от 26.11.2007 № 188 «Об организации прокурорского надзора за исполнением законов о несовершеннолетних и молодежи» (п. 3.2) – предусмотрено проведение систематических проверок соблюдения законодательства о защите детей от информации, наносящей вред их здоровью, репутации, нравственному и духовному развитию, в деятельности средств массовой информации, органов и учреждений образования и культуры.

В компетенции образовательной организации входит создание необходимых условий для охраны и укрепления здоровья обучающихся, на основании которых мы выделили задачи педагогического характера для организации мероприятий по информационной безопасности: 1. формирование у учащихся устойчивого убеждения в использовании информационных ресурсов; 2. формирования устойчивых поведенческих навыков в сфере информационной безопасности; 3. развитие у учащихся способности распознать и противостоять негативной информации в Интернет-пространстве и СМИ, через обучение способам защиты от вредной информации.

В Концепции информационной безопасности детей утверждается, что обеспечение информационной безопасности детей возможно исключительно при условии эффективного сочетания государственных и общественных усилий при определяющей роли семьи. В связи с этим важнейшей задачей является налаживание согласованного взаимодействия семьи, главного института социализации и воспитания детей, с государством и всеми элементами современного медиарынка - производителями и распространителями контента, психолого-педагогическими экспертными сообществами и экспертными сообществами в области художественного образования. Комплексное решение поставленной задачи со стороны семьи и школы позволит значительно сократить риски причинения различного рода ущерба ребенку со стороны сети Интернет. Обеспечение информационной безопасности и воспитание информационной культуры должно стать одним из приоритетных направлений работы современного образовательного учреждения.

Организация безопасной информационной среды в образовательных организациях включает в себя 4 основных направления:

1. Технический контроль:

- антивирусные программы;

- контентная фильтрация.

2. Информационный ресурс:

- специализированные сайты в Интернет;

- школьный сайт;

- просветительские стенды;

- печатная продукция (памятки, буклеты).

3. Профилактическая работа с обучающимися:

- на уроках (в том числе на уроках информатики);

- классные часы;

- внеурочные мероприятия;

4. Работа с родителями:

- родительские собрания;

- родительские лектории;

- индивидуальные и групповые консультации.

Информационно-образовательная среда образовательной организации должна обеспечивать возможность осуществлять в электронной (цифровой) форме следующие виды деятельности:

- информационно-методическую поддержку образовательного процесса;

- планирование образовательного процесса и его ресурсного обеспечения;

- размещение и сохранение материалов образовательного процесса, в том числе – работ обучающихся и педагогов, используемых участниками образовательного процесса информационных ресурсов;

- мониторинг и фиксацию хода и результатов образовательного процесса;

- современные процедуры создания, поиска, сбора, анализа, обработки, хранения и представления информации;

- дистанционное взаимодействие всех участников образовательного процесса (обучающихся, их родителей (законных представителей), педагогических работников, органов управления в сфере образования, общественности), в том числе, в рамках дистанционного образования;

- дистанционное взаимодействие образовательной организации с другими организациями социальной сферы: организациями дополнительного образования детей, организациями культуры, здравоохранения, спорта, досуга, службами занятости населения, обеспечения безопасности жизнедеятельности;

При этом надо четко понимать, что все эти виды деятельности требуют жесткий контролируемый доступ участников образовательного процесса к информационным образовательным ресурсам в сети Интернет (ограничение доступа к информации, несовместимой с задачами обучения, развития и воспитания обучающихся). Одним из путей решения вышеобозначенной проблемы, является организация безопасной информационно-образовательной среды в образовательной организации дополненной аппаратными, программными и организационными средствами и способами защиты от негативной информации. Безопасная информационная среда должна  обеспечивать безопасность и защиту личностной информационной среды всех субъектов образовательного процесса в целях создания условий для наиболее полноценного развития и реализации их индивидуальных способностей и возможностей.

Профилактическая работа с учащимися должна быть направлена на решение следующих задач:

- повышение уровня информационной компетентности обучающихся;

- формирование ключевых компетенций: информационную и медиакомпетентность, коммуникативную компетентность, потребительскую и техническую компетентность;

- разработку правила поведения обучающихся в сети Интернет;

- формирование навыков ответственного поведения с целью обеспечения информационной безопасности в сети Интернет;

- формирование и содействие развитию устойчивой направленности у обучающихся на освоение механизмов информационно-психологической самозащиты;

- расширение стратегий поведения у школьников в трудных ситуациях, связанных с коммуникационными технологиями;

- развитие у обучающихся критического мышления.

Данные задачи могут решаться при освоении курсов таких дисциплин как: основы безопасности жизнедеятельности, информатика, обществознание, а также других дисциплин, во внеурочной деятельности, кружковой работе.

Все больше несовершеннолетних предпочитают общение в сетях реальному общению. И здесь возникает очередная проблема: размещение на страницах несовершеннолетних негативного и запрещенного контента. В случае поступления в образовательную организацию информации о размещении на странице несовершеннолетнего негативного контента необходимо:

*Администрации:*

Установить, обучается ли указанный несовершеннолетний в данной образовательной организации. Создать рабочую группу. В нее необходимо включить заместителя директора, курирующего обучение в параллели, педагога – психолога, социального педагога, классного руководителя.

В случае отсутствия выявленного несовершеннолетнего в списочном составе обучающихся (закончил обучение, переведен в другую образовательную организацию, никогда не входил в число обучающихся данной образовательной организации) срочно сообщить об этом в контролирующую организацию, поскольку несовершеннолетнего разыскивают.

*Специалистам:*

Специалисты социально-психологической службы проводят индивидуальную беседу с обучающимся, с целью выяснения причин размещения негативной информации.

Классный руководитель приглашает родителей/законных представителей несовершеннолетнего в образовательную организацию для проведения индивидуальных бесед.

Представителю образовательной организации необходимо провести беседы с несовершеннолетним и его родителями/законными представителями о негативных последствиях размещения данной информации в социальных сетях (административной ответственности и др.).

Показателем эффективно проведенной работы будет удаление негативного контента со страницы несовершеннолетнего.

Взять и просто запретить Интернет невозможно, да собственно, в этом нет такой необходимости. Посредством виртуального пространства, наши дети получили возможность находить большое количество интересной и полезной информации, помогающей в обучении и развитии.

Информации, положительной и отрицательной, очень много и главное – умение правильно и безопасно ее использовать. Задача педагогов и родителей - научить ребенка критически оценивать полученную информацию, а не слепо принимать ее, как руководство к действию.

Достичь высоких результатов в воспитании невозможно без привлечения родителей. Очень часто родители не понимают и недооценивают угрозы, которым подвергается подросток, находящийся в сети Интернет. Некоторые из них считают, что ненормированное «сидение» ребенка в сети лучше, чем прогулки в сомнительных компаниях.

По данным исследования Фонда Развития Интернет и факультета психологии МГУ имени М. В. Ломоносова при поддержке Google, российские подростки обгоняют родителей по частоте использования Интернета. Ежедневно пользуются Интернетом 89 % подростков и 53 % родителей подростков. Причем 17 % всех опрошенных родителей отметили, что не пользуются Интернетом вообще. Исследовался также так называемый «цифровой разрыв» — разница в компетенции пользования Интернетом между родителями и детьми. Выявились следующие факты:

• менее половины родителей осведомлены о рисках, с которыми сталкивается ребенок. Каждый третий родитель знает, что дети видят изображения сексуального характера в Интернете, потому что видят их сами. В то же время они почти не имеют представления о том, что дети становятся жертвами агрессивного поведения или могут быть агрессорами сами. Хотя самих детей в наибольшей степени волнует именно то, что представляет собой коммуникационные риски. Также родители очень мало знают о том, что их дети встречаются с теми, с кем познакомились в Интернете;

• готовность ребенка увидеть и принять помощь. Треть детей отмечает, что не ощущают со стороны родителей никакой поддержки, хотя сами родители при этом считают, что помогают своему ребенку.

Исходя из вышеизложенного в мероприятия по обучению родителей (законных представителей) несовершеннолетних детей основам информационной безопасности детей приобретают особую актуальность, поэтому необходимо включить тематику по информационной безопасности в родительский всеобуч. Цель данных мероприятий: формирование ответственного родительства в области обеспечения информационной безопасности детей. Задачи:

- информирование родителей о видах информации, способной причинить вред здоровью и развитию несовершеннолетних, запрещенной или ограниченной для распространения на территории Российской Федерации, а также о негативных последствиях распространения такой информации;

- информирование родителей о способах незаконного распространения такой информации в информационно-телекоммуникационных сетях, в частности, в СМИ, сетях Интернет и мобильной (сотовой) связи (в том числе путем рассылки SMS-сообщений незаконного содержания);

- ознакомление родителей с международными принципами и нормами, с нормативными правовыми актами Российской Федерации, регулирующими вопросы информационной безопасности несовершеннолетних;

- обучение родителей техническим способам защиты детей от информационной угрозы;

- обучение родителей способам формирования правил ответственного и безопасного пользования услугами медиа, Интернет и мобильной (сотовой) связи, другими электронными средствами связи и коммуникации, в том числе способам защиты от противоправных и иных общественно опасных посягательств в информационно-телекоммуникационных сетях, в частности, от таких способов разрушительного воздействия на психику детей, как кибербуллинг (жестокое обращение с детьми в виртуальной среде) и буллицид (доведение до самоубийства путем психологического насилия);

- обучение родителей способам профилактика интернет-зависимости и игровой зависимости (игромании, гэмблинга) у детей;

- обучение родителей способам предупреждения совершения детей правонарушений с использованием информационно-телекоммуникационных технологий.

При обучении родителей основам информационной безопасности могут быть использованы традиционные формы работы: родительские собрания (классные, общешкольные, городские, районные), тематические классные часы, собрания отцов, родительские конференции, консультирование, так и нетрадиционные формы (активные методы и формы обучения: дискуссии, круглые столы, деловые игры, занятия по отработке практических навыков работы в Интернете, открытые уроки и классные мероприятия, индивидуальные тематические консультации и пр.)

При организации родительского всеобуча следует привлекать как сотрудников образовательного учреждения (специалисты должны иметь базовую подготовку по педагогике, психологии, информационным технологиям), так и узких специалистов в соответствии с потребностями родителей и школы(медицинского работника, социального педагога).

При организации обучения родителей (законных представителей) основам интернет безопасности можно использовать следующую тематику:

1. Компьютеры и Интернет в нашей жизни. Использование ресурсов ПК для обучения.

2. Опасности в Сети. Механизмы защиты.

3. Внимание: персональные данные! Мои персональные данные. Форма допуска. Сим-сим откройся или надёжный пароль.

4. Общение в Интернете. Коммуникативная компетентность. Безопасная коммуникация в Сети.

5. Кибербуллинг. Толерантность в сети.

6. Эффективное время онлайн.

7. Компьютерная, интернет зависимость.

*Перечень методических материалов и ресурсов:*

1. Горбунова Л.Н., Анеликова Л.А., Семибратов А.М., Смирнов Н.К., Сорокина Е.В., Третьяк Т.М. Здоровье и безопасность детей в мире компьютерных технологий и Интернет. – Учебно-методический комплект. - М.: СОЛОНПРЕСС, 2010. - 176 с.

2. Грачев Г. В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г. В. Грачев. – М.: Изд-во РАГС, 1998. – 125 с.

3. Емельянова Е.В. Психологические проблемы современного подростка и их решение в тренинге. Спб.: Речь, 2008. – 336с.

4. Информационная безопасность: учеб. пособие / В.В. Гафнер. – Ростов н/Д : Феникс, 2010. — 324 с.

5. Практическая психология безопасности. Управление персональными данными в интернете: учеб.-метод. пособие для работников системы общего образования / Г.У. Солдатова, А.А. Приезжева, О.И. Олькина, В.Н. Шляпников. — М.: Генезис, 2017. - 224 с.

6. <http://www.microsoft.com/eesti/education/veebivend/koomiksid/rus/html/etusivu.htm>) в разделе «Для учащихся» рассказы для детей 7-10 лет, а также в разделе «Тесты» (можно организовать on-line тестирование школьников 7-10 лет);

7. [http://www.onlandia.org.ua/ru-RU/](http://www.onlandia.org.ua/ru-ru/) On-ляндия. Безопасная веб-страна в разделе «Для детей 7-10 лет» рассказы в картинках, задания и вопросы;

8. <http://content-filtering.ru/aboutus/> Информационно-аналитический ресурс «Ваш личный Интернет» в разделе «Юным пользователям» - «Дошкольники и младшие классы» подсказки и советы по безопасному поведению в сети Интернет;

9. <http://stopfraud.megafon.ru/> федерального проекта по борьбе с мобильным мошенничеством компании МегаФон в разделах «Виды мошенничества» и «Наши рекомендации», а также советы родителям;

10. [http://youtu.be/789j0eDglZQ](http://youtu.be/789j0edglzq) мультфильм «Безопасный интернет», который разработала студия Mozga.ru, принимавшая участие в конкурсе "Безопасный интернет - детям!", проведенном Mail.ru, где заняла первое место.

Составитель: Нагребецкая С.Г., методист центра по воспитательной работе и основам здоровья, ГБОУ ДПО РК «Крымский республиканский институт постдипломного педагогического образования».