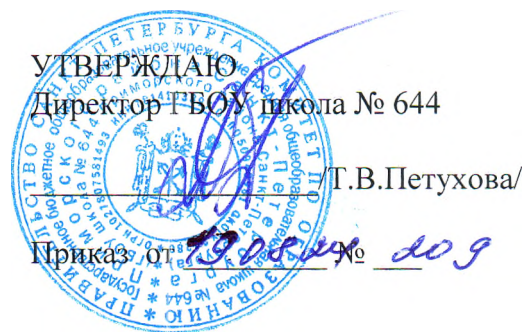


Государственное бюджетное общеобразовательное учреждение средняя общеобразовательная
школа № 644
Приморского района Санкт-Петербурга

УТВЕРЖДАЮ
Директор ГБОУ школа № 644
Т.В.Петухова/
Приказ от 29.08.2024 № 209



Рабочая программа
социального педагога
«Безопасность в сети Интернет»

5 классы

Составитель:
Социальный педагог
ГБОУ школы № 644
Вильгельм И.В.

Санкт-Петербург
2024 год.

1. Пояснительная записка

1.1. Актуальность программы

За последние годы сеть Интернет вошла в нашу жизнь и стала важным современным источником информации и средством общения. Сегодняшние дети уже не представляют себе мир без смартфона и планшета, браузера и онлайн-игр. И так же, как мы учим малышей чистить зубы и правильно переходить дорогу, мы стараемся рассказывать им об основных правилах безопасного использования сети Интернет.

Сегодня, по данным Института развития Интернета, им пользуются 76% россиян. Растет и число школьников, ежедневно использующих социальные сети. Результаты мониторинга Фонда «Национальные ресурсы образования», проведенного среди 2 500 школьников от 13 до 18 лет в 84 регионах России, показывают, что 50% ребят заходят в социальные сети более девяти раз в день. Чаще всего школьники используют социальные сети для переписки с друзьями — 83%, для чтения постов и просмотра новостной ленты — 74%, для прослушивания музыки — 70%, для размещения фотографий — 26%. Технический прогресс делает информацию все более доступной.

И если раньше основными угрозами, которые таит в себе увлечение компьютером и Интернетом, взрослые считали нарушение зрения, осанки, развитие зависимости и нежелательный контент, то сегодня все чаще называются такие явления, как потеря конфиденциальности, кибербуллинг, фейкньюз, финансовое мошенничество.

В соответствии со «Стратегией развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года», утвержденной распоряжением Правительства Российской Федерации от 1 ноября 2013 г. № 2036-р, «Стратегией развития информационного общества в Российской Федерации», утвержденной Президентом Российской Федерации 7 февраля 2008 г. № Пр-212 и рядом других документов в числе многих других задач выделяются:

- обеспечение различных сфер экономики качественными информационными технологиями;
- обеспечение высокого уровня информационной безопасности государства, индустрии и граждан.

Безопасность в информационном обществе является одним из основных направлений фундаментальных исследований в области информационных технологий.

Число ИТ-преступлений в России за 2023 год выросло на 29,7% в сравнении с 2022-м. Таковую статистику официальный представитель Министерства внутренних дел (МВД) РФ Ирина Волк привела 8 февраля 2024 года.

По ее словам, каждое третье преступление в России по итогам 2023 года совершено с использованием информационно-телекоммуникационных технологий.

В МВД считают, что в связи с этим наиболее эффективным методом противодействия с киберпреступлениями остается профилактическая работа с населением, его информирование о новых способах и схемах совершения высокотехнологичных преступлений и методах защиты граждан от них.

Полный запрет доступа детей к технологиям не решает проблему безопасности.

Современные технологии – важная часть повседневной жизни, необходимая для развития подрастающего поколения, в связи с этим необходимо говорить и обсуждать с детьми о кибербезопасности.

1.2 Анализ условий для реализации в ГБОУ школа № 644 Приморского района СПб

Безусловно, проведение комплексной работы с детьми остается в первую очередь за родителями. При этом сложно переоценить и тот вклад, который может внести школа.

Для современных школьников именно учитель, а не интернет и компьютер, остается центральной фигурой в учебной и внеучебной деятельности — только 1,5% подростков считают, что учеба стала бы интересней, если бы преподавателя полностью заменили компьютерные технологии.

Социальным педагогом проведено анкетирование среди обучающихся 6 классов школы, были опрошены учащиеся в количестве 81 человек.

Подростки, как отмечалось выше, являются крайне подверженной психологическому воздействию возрастной группой, так как их эмоциональные потребности и потребности в самоутверждении в значительной степени влияют на мотивы их поступков, а также на способность критически воспринимать получаемую информацию и имеют потребность в копировании действий, не всегда правомерных и безопасных, людей, которые для них являются авторитетом. Что включает представителей этой возрастной категории в группу риска.

Рассматривая ответы учащихся на вопросы анкеты, выяснено, что подростки осведомлены о существующих в интернете угрозах, о сетевом этикете.

Вместе с тем выявлены риски по следующим вопросам: какое действие предпринять, если на экране компьютера непонятное сообщение, что нужно сделать при получении подозрительного сообщения по э/почте), что нужно сделать, если стал известен пароль чужого человека и др. вопросы.

Таким образом, следует проводить профилактическую работу среди подростков, начиная с 5 класса.

Планируемые результаты работы

1.Предметные:

1.1. Сформированы знания о безопасном поведении при работе с компьютерными программами, информацией в сети интернет;

1.2. Сформированы умения соблюдать нормы информационной этики;

1.3. Сформированы умения безопасно работать с информацией, анализировать и обобщать полученную информацию.

2. Метапредметные:

2.1. Развиваются компьютерная грамотность и информационная культура личности в использовании информационных и коммуникационных технологий;

2.2. Развиваются умения анализировать и систематизировать имеющуюся информацию;

2.3. Развиваются познавательная и творческая активность в безопасном использовании информационных и коммуникационных технологий.

3.Личностные:

3.1. Вырабатывается сознательное и бережное отношение к вопросам собственной информационной безопасности;

3.2. Формируются и развиваются нравственные, этические, патриотические качества личности;

3.3. Стимулируется поведение и деятельность, направленные на соблюдение информационной безопасности.

1.3 Законодательная база.

- Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон от 29.12.2012 г. № 273-ФЗ «Об образовании в Российской Федерации».

2.Концептуальные подходы

2.1. Раскрытие понятийного аппарата

К ключевым понятиям относятся термины «киберпространство» и «кибербезопасность».

Киберпространство - сфера деятельности в информационном пространстве, образованная совокупностью коммуникационных каналов Интернета и других телекоммуникационных сетей, технологической инфраструктуры, обеспечивающей их функционирование, и любых форм осуществляемой посредством их использования человеческой активности (личности, организации, государства)». **«Кибербезопасность»** - совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями. Детям и подросткам интернет необходим для выполнения школьных заданий, общения с учителями и другими учениками, интерактивных игр и выполнения других задач. Это прекрасное место для обучения и общения. Но родители должны быть в курсе того, что их дети видят и слышат в Интернете, с кем общаются и что рассказывают о себе. **Блогер** — человек, который ведет собственный электронный дневник в сети Интернет и администрирует его, в том числе на одной из популярных платформ. **Вредоносный код** — компьютерный код или веб-скрипт, разработанный для создания уязвимостей в системе, с помощью которых выполняются несанкционированные вредоносные действия, такие как кража информации и данных и другие потенциальные повреждения файлов и вычислительных систем. **Контент-фильтр** — устройство или программное обеспечение для фильтрации сайтов по их содержанию, не позволяющее получить доступ к определенным сайтам или услугам сети Интернет. Система позволяет блокировать веб-сайты с содержанием, не предназначенным для просмотра. **Персональные данные** — любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных). **Фишинг** — один из видов интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей: логинам, паролям, лицевым счетам и банковским картам. В основном используется метод проведения массовых рассылок от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих. **Цифровой след** — совокупность информации о посещениях и вкладе пользователя в цифровое пространство. Может включать в себя информацию, полученную из мобильного Интернета, веб-пространства и телевидения. Это могут быть личные профили и учетные записи в социальных сетях, информация о посещаемых веб-сайтах, открытые и созданные файлы, личные сообщения и комментарии, видео, фотографии и другая виртуальная активность, в том числе ввод персональных данных пользователя. Некоторые из этих материалов являются общедоступными, другие — конфиденциальными

2.2. Научно-методические основания.

Данная рабочая программа составлена на основе курса «Основы кибербезопасности» для общеобразовательных организаций авторов Тонких И.М., Комарова М.М., Ледовского В.И., Михайлова А.В., переработана и модифицирована.

В настоящее время требования ФГОС для уровней начального, общего и полного среднего образования не содержат предметной области «Основы кибербезопасности», но в рамках метапредметных результатов и предметных умений дисциплины «Информатика» вопросы информационной безопасности обозначены:

- требование формирования навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права;
- умения использовать средства информационных и коммуникационных технологий в решении когнитивных, коммуникативных и организационных задач с соблюдением требований

эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;

- понимание основ правовых аспектов использования компьютерных программ и работы в Интернете и т.п.

В рамках данной рабочей программы планируется реализовать в 5 –х классах информацию в количестве 8 тем.

3. Основная часть

3.1 Цели и задачи программы

Цель программы: освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства.

Задачи обучения:

Образовательные:

1. Способствовать формированию знаний о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет;
2. Формировать умения соблюдать нормы информационной этики;
3. Формировать умения безопасной работы с информацией, анализировать и обобщать полученную информацию.

Развивающие:

1. Развивать компьютерную грамотность информационную культуру личности в использовании информационных и коммуникационных технологий;
2. Развивать умение анализировать и систематизировать имеющуюся информацию;
3. Развивать познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий;

Воспитательные:

1. Способствовать выработке сознательного и бережного отношения к вопросам собственной информационной безопасности;
2. Способствовать формированию и развитию нравственных, этических, патриотических качеств личности.
3. Стимулировать поведение и деятельность, направленные на соблюдение информационной безопасности.

3.2. Тематическое планирование занятий

№ п/п	Тема занятий	Количество часов	Планируемые сроки проведения занятий	Дата проведения
1	Информация, компьютер и Интернет	1	сентябрь	17.09.2024
2	Основные правила поведения сетевого взаимодействия	1	октябрь	15.10.2024
3	Гигиена при работе с компьютером. Правила работы с ПК	1	ноябрь	19.11.2024
4	Социальные сети	1	декабрь	17.12.2024
5	Методы безопасной работы в Интернете	1	январь	21.01.2025

6	Что такое интернет-этикет. Как вести себя в гостях у «сетевых» друзей.	1	февраль	18.02.2025
7	Электронная торговля - ее опасности.	1	март	11.03.2025
8	Рисунки на тему безопасности в сети Интернет	1	апрель	15.04.2025

3.3. Условия реализации программы

- Согласие родителей;
- Заинтересованность обучающихся;
- Взаимодействие с классными руководителями.

3.4. Точки риска при ее реализации

- Отсутствие согласия родителей на проведение бесед с учащимися;
- Нежелание самих обучающихся участвовать в занятиях.

3.5 Список литературы

- Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»;
- Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации»;
- Постановление Главного государственного санитарного врача Российской Федерации от 29.12.2010 № 189 (ред. от 25.12.2013 г.) «Об утверждении СанПиН 2.4.2.2821-10 «Санитарно-эпидемиологические требования к условиям и организации обучения в общеобразовательных учреждениях» (Зарегистрировано в Минюсте России 03.03.2011 г. № 19993);
- Бирюков А.А. «Информационная безопасность защита и нападение» 2 издание: Издательство: ДМК-Пресс, 2017, 434 с.
- Колесниченко Денис. «Анонимность и безопасность в интернете. От чайника к пользователю» Самоучитель Издательство: БХВ-Петербург, 2012, 240с. 45
- Мэйволд Э. Безопасность сетей (2-е изд.) Книги» Сетевые Технологии. Название: Безопасность сетей: Издательство: М.: НОУ «Интуит», 2016, 571 с.
- Яковлев В.А. Шпионские и антишпионские штучки: Техническая литература Издательство: Наука и Техника, 2015, 320 с.

Социальный педагог



И.В. Вильгельм

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

**ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 644
ПРИМОРСКОГО РАЙОНА САНКТ-ПЕТЕРБУРГА**, Петухова Тамара Веноровна,
Директор

26.08.24 14:41
(MSK)

Сертификат E2A33D0A7A042B0977978D48211D2F12