Государственное бюджетное учреждение дополнительного образования
Центр психолого-педагогической, медицинской и социальной помощи
Красносельского района Санкт-Петербурга
(ЦПМСС Красносельского района)

Принято
Педагогическим советом
Протокол от 29.08.2022 № 1

Седунова Ирина Сергеевна
Подписано цифровой подписью: Седунова Ирина Сергеевна
Дата: 2022.10.03 16:22:20 +03'00'

Утверждаю
Директор
_____ И.С. Седунова
Приказ от 29.08.2022 № 123-од

Дополнительная общеобразовательная общеразвивающая
программа социально-педагогической направленности

Безопасность в сети Интернет

Возраст обучающихся: 11-15 лет

Срок реализации 2022-2023 учебный год

Разработчик: социальный педагог Куцоконь Н.И.

Санкт-Петербург
2022 год

Пояснительная записка

Дополнительная общеобразовательная общеразвивающая программа «Безопасность в сети Интернет» имеет социально-педагогическую направленность, уровень освоения - общекультурный.

Актуальность

Последние десятилетия инновационные коммуникационные технологии многое изменили в нашей жизни. Компьютер, интернет воспринимаются как ее неотъемлемая часть. Большинство современных детей вообще не представляют себе без компьютера ни учебу, ни досуг и проводят с ним много времени.

При этом несовершеннолетние меньше, чем взрослые, подготовлены к проблемам, с которыми могут столкнуться в сети, и нередко остаются беззащитными перед ними. Именно дети и подростки сегодня менее всего защищены от потока негативной информации, встречающейся в компьютере. В связи с существенным возрастанием численности несовершеннолетних пользователей все более актуальной становится проблема обеспечения информационной безопасности детей в сети Интернет.

Даже при неглубоком поиске во «всемирной паутине» легко обнаружить сайты, где положительно оцениваются такие социально опасные явления, как сатанизм, сектантство, расовая и национальная нетерпимость, педофилия, различные виды сексуальных извращений, наркомания, призывы к экстремизму, терроризму и т.п. Появляются сайты, группы в социальных сетях, принадлежащие организованным преступным группировкам и террористическим организациям, через которые они обмениваются информацией, пропагандируют свои идеи и образ жизни. Значительное большинство подобных сайтов, групп в социальных сетях остаются скрытыми от родителей, правоохранительных органов и общества.

Чаще всего несовершеннолетние пользователи попадают на опасные странички случайно. Многочисленные всплывающие окна, неверно истолкованные поисковиком запросы, ссылки в социальных сетях – все это приводит ребенка на сайты небезопасного содержания, связанные с негативной информацией.

Просвещение подрастающего поколения в части использования различных информационных ресурсов, знание элементарных правил отбора и использования информации способствует развитию системы защиты прав детей в информационной среде, сохранению здоровья и нормальному развитию.

Обеспечение государством информационной безопасности детей, защита их физического, умственного и нравственного развития во всех аудиовизуальных медиа-услугах и электронных СМИ – важная задача современности. Реализация данной программы может способствовать развитию морально-этических норм несовершеннолетних пользователей Интернета, обеспечению информационной безопасности и защиты несовершеннолетних.

Нормативно-правовая база программы

Необходимость профилактики безопасного поведения в интернете среди детей в образовательной среде закреплена в следующих нормативно-правовых документах:

- Федеральный закон от 29.12.2012 №273-ФЗ «Об образовании в Российской Федерации» (п. 9, 22, 25, ст. 2, п. 5 ст.12, п.1, п 4 ст.75);
- Федеральный закон от 24.06.1999 № 120-ФЗ «Об основах системы профилактики безнадзорности и правонарушений несовершеннолетних»;
- Федеральный Закон от 29.12.2010 №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» в ред. Федерального закона от 28.07.2012 №139-ФЗ;
- Федеральный закон от 28.07.2012 №139-ФЗ «О внесении изменений в Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации»;

- Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации»;
- Стратегия развития воспитания в Российской Федерации на период до 2025 года», утвержденная распоряжением Правительства Российской Федерации от 29.05.2015 № 996-р;
- «Основы государственной молодежной политики Российской Федерации на период до 2025 года», утвержденные распоряжением Правительства Российской Федерации от 29.11.2014 № 2403-р;
- Концепция развития дополнительного образования детей до 2030 года, утверждена распоряжением Правительства Российской Федерации от 31.03. 2022 № 678-р;
- Федеральный государственный образовательный стандарт основного общего образования (утвержден приказом Министерства просвещения РФ от 31.05.2021 №287);
- Приказ Минпросвещения России от 09.11.2018 №196 «Об утверждении порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
- Распоряжение Комитета по образованию Санкт-Петербурга от 01.03.2017 г. № 617-р «Об утверждении Методических рекомендаций по проектированию дополнительных общеразвивающих программ в государственных образовательных организациях Санкт-Петербурга, находящихся в ведении Комитета по образованию»
- Распоряжение Комитета по образованию от 15.07.2019 № 2081-р «Положение об организации работы по оказанию психолого-педагогической помощи и психолого-педагогического сопровождения»;
- Санитарные правила СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи», утвержденные Постановлением Главного государственного санитарного врача Российской Федерации от 28 сентября 2020 года № 28.

Методологические принципы

Технология подготовки и реализации программы опирается на следующие принципы.

1. *Принцип информационной безопасности.*

Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» определяет информационную безопасность детей как состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию. Информацией, причиняющей вред здоровью и (или) развитию детей, признаётся информация, распространение которой среди детей запрещено или ограничено в соответствии с Федеральным законом № 436-ФЗ. Согласно статье 5 данного закона к запрещённой для распространения среди детей относится информация:

- побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству;

- способная 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.

2. *Принцип ситуационной адекватности.*

Определяет соответствие содержания и организации профилактических мероприятий и программ реалиям экономической и социальной жизни и ситуации, связанной с проявлениями девиантного поведения, социокультурной среде конкретной образовательной организации.

3. *Принцип научной достоверности.*

В соответствии с этим принципом, вся предлагаемая учащимся информация научно

достоверна и излагается с использованием научной терминологии.

Занятия по программе проводятся преимущественно в активной форме, позволяющей учащимся участвовать в рефлексивной деятельности, используя свой творческий потенциал.

Особенностью программы является возможность ее применения в сочетании с другими программами ЦПМСС Красносельского района и использование ее результатов другими специалистами для групповой и индивидуальной работы.

Адресат программы: учащиеся образовательных организаций 11-15 лет.

Цель:

Формирование культуры здорового и безопасного образа жизни в информационной среде, личностное развитие учащихся.

Достижение цели раскрывается через следующие **задачи**:

- ***обучающие*** – включение в познавательную деятельность, приобретение знаний, умений, навыков безопасного поведения в сети интернет;
- ***развивающие*** – развитие потребности в саморазвитии, самостоятельности, ответственности, компетенции сопротивления социальному давлению;
- ***воспитательные*** – формирование культуры общения и поведения в Интернет-пространстве.

Условия реализации программы

Условия набора в группы: групповые интерактивные занятия с учащимися проводятся по Соглашениям на учебный год с администрацией образовательного учреждения и на базе ОУ.

Условия формирования групп*:* одновозрастные, разновозрастные.

Количество детей в группе: класс делится на 2 группы, работа ведется в группах не более 15 человек.

Особенности организации образовательного процесса: сферы ответственности, основные права и обязанности специалистов ЦПМСС Красносельского района и образовательной организации, на базе которого реализуется программа, определяются договором между ЦПМСС Красносельского района и образовательной организацией. Перед началом реализации программы рекомендуется беседа с классным руководителем и социальным педагогом, с целью выявления особенностей уже сложившегося классного коллектива.

Формы проведения занятий: лекция, диспут, игра, элементы тренинга, творческие задания.

Формы организации деятельности учащихся на занятии:

- фронтальная: работа педагога со всеми учащимися одновременно (беседа, объяснение демонстрация презентаций, видеороликов);
- коллективная: организация проблемно-поискового или творческого взаимодействия между всеми детьми одновременно (диспут, проект):
- групповая: организация работы (совместные действия, общение, взаимопомощь) в малых группах, в том числе в парах, для выполнения определенных задач; задание выполняется таким образом, чтобы был виден вклад каждого учащегося (группы могут выполнять одинаковые или разные задания, состав группы может меняться в зависимости от цели деятельности).

Материально-техническое оснащение

Занятия проводятся в просторном, хорошо проветриваемом помещении образовательной организации, оборудованном современной цифровой аппаратурой (мультимедийным оборудованием) для показа видеороликов и презентаций.

Внеурочные занятия для обучающихся с использованием компьютеров рекомендуется проводить не более 60 минут.

Рекомендуемая (онлайн) непрерывная длительность работы, связанная с фиксацией взора непосредственно на экране устройства отображения информации, на занятии не

должна превышать для обучающихся в 5-9х классах 20 минут.

Кадровое обеспечение – специалисты ЦПМСС Красносельского района.

Реализация программы с использованием дистанционных образовательных технологий

В целях обеспечения безопасных условий реализации дополнительных общеобразовательных общеразвивающих программ ЦПМСС Красносельского района в ситуации осложнения эпидемической обстановки возможна реализация программы с использованием дистанционных образовательных технологий и электронного обучения. Использование дистанционных образовательных технологий и электронного обучения регулируется Положением об электронном обучении и использовании дистанционных образовательных технологий при реализации дополнительных общеобразовательных программ в государственном бюджетном учреждении дополнительного образования Центре психолого-педагогической, медицинской и социальной помощи Красносельского района Санкт Петербурга.

Планируемые результаты

Личностные результаты: сформировавшиеся и формирующиеся качества осознанной и ответственной личности по отношению к собственным поступкам на основе распознавания и оценки вредных факторов воздействия информационно-телекоммуникационных сетей и Интернета.

Метапредметные результаты

– освоенные учащимися общие способы коммуникации, потребности в саморазвитии, самостоятельности, ответственности, применимые как в рамках образовательного процесса, так и при решении проблем в реальных жизненных ситуациях;

– умение самостоятельно распознавать попытки вовлечения в противоправную и иную антиобщественную деятельность.

Предметные результаты: освоенный учащимися опыт конструктивного социального взаимодействия в сети Интернет.

Учебный план программы
дополнительной общеобразовательной общеразвивающей программы
«Безопасность в сети Интернет»

№ п/п	Название раздела, темы	Количество часов			Формы контроля
		Всего	Теория	Практика	
5-6-е классы					
1.	**Организационно-диагностический этап**	2	1	1	Анкетирование участников образовательного процесса (Приложение 5)
2.	**Профилактический этап** **1. Интернет: риски и защита.** Риски: блокирование компьютера вирусом, интернет-мошенничество, кража личных данных, взлом и создание подставных страниц.	1	0,5	0,5	Наблюдение, рефлексия, анализ работы обучающихся на занятиях. Анкетирование (Приложение7)

	2. Правила личной безопасности. Средства защиты. Потребительские риски (интернет и мобильное мошенничество, потеря денег через интернет или мобильный телефон). «Бесплатный сыр», как не попасться на удочку мошенникам. Защита личных данных: ники, логины, пароли, публикация и приватность личной информации. **3. Компьютер и здоровье.** Зависимость, границы виртуальной реальности	1 1	0,5 0,5	0,5 0,5	
Итого для 5-6-х классов		**5**	**2,5**	**2,5**	
3.	**Консультационный этап участникам образовательного процесса** (по запросу)	3			Отзывы, анализ анкет, презентация результатов на уровне образовательной организации
Всего для 5-6-х классов		**8 часов, включая консультации**			
7-9-е классы					
4.	**Организационно-диагностический этап**	2	1	1	Анкетирование участников образовательного процесса (Приложение 5)
5.	**Профилактический этап** **1. Интернет-этика.** Репутация, поведение в сети. Видеоблоги, авторское право, друзья в сети. **2. Интернет-безопасность.** Тролли, манипуляции, способы противостояния. Правила поведения в сети 3. **Компьютер и здоровье.** Зависимость, границы виртуальной реальности 4. **Интернет и будущее.** Профессии, творчество, обучение	1 1 1 1	0,5 0,5 0,5 0,5	0,5 0,5 0,5 0,5	Наблюдение, рефлексия, анализ работы обучающихся на занятиях. Анкетирование (Приложение7)
Итого для 7-9-х классов		**6**	**3**	**3**	
6.	**Консультационный этап участникам образовательного процесса** (по запросу)	3			Отзывы, анализ анкет, презентация результатов на уровне образовательной организации
Всего для 7-9-х классов		**9 часов, включая консультации**			
Итого для учащихся 11 час. коррекционно-развивающих занятий, 6 час. консультаций					

Оценочные и методические материалы

Система контроля результативности реализации программы

Предусмотрено проведение анкетирования, сбор отзывов обучающихся, включенных в группы по дополнительной общеобразовательной общеразвивающей программе «Безопасность в сети Интернет», их родителей (законных представителей) и педагогов. Результаты анкетирования фиксируются в протоколах обследований. Результативность определяется путем анализа результатов анкетирования и отзывов. Результаты анализа оформляются в аналитической справке по итогам групповой коррекционно-развивающей работы.

Текущий контроль результативности проводится путем наблюдения, рефлексии обучающихся, анализа работы обучающихся на занятиях. Специальные формы фиксации результатов текущего контроля не предусмотрены.

Аналитическая справка по результатам анкетирования детей может использоваться на родительском собрании, на методическом объединении педагогов образовательной организации.

Содержание занятий
по дополнительной общеобразовательной общеразвивающей программе
«Безопасность в сети Интернет»

Блок 5-6-е классы

Тема 1. Интернет и риски интернета

1. Беседа (возможен вариант - комментирование презентации «Лиги безопасного интернета» для учащихся 5-7-х классов, http://www.ligainternet.ru/encyclopedia-of-security/ – Сайт «Лига безопасного интернета»: материалы доля детей, родителей, педагогов).

Три основных направления по обеспечению кибербезопасности:

- защита ваших компьютеров и гаджетов от вирусов и вредоносных программ;
- виртуальное или кибермошенничество;
- нарушение морали и этики в онлайн-общении, троллинг, разрушающий ваше личное пространство.

Интернет-риски:

- Потребительские риски (интернет и мобильное мошенничество).
- Мошенничество в интернете (хакеры, фишинг, скимминг).
- Покупки в интернете. Звонки и выигрыши.
- Вовлечение в преступную деятельность – нарушение закона (экстремизм, продажа наркотиков, половая неприкосновенность)

Защита в интернете: **Линия помощи «Дети онлайн», 8-800-25-000-15** (бесплатно, по рабочим дням)

Основные функции Линии помощи: оказание психологической и практической помощи детям и подросткам, которые столкнулись с опасностью или негативной ситуацией во время пользования интернетом или мобильной связью (виртуальное преследование, домогательство, грубость, шантаж, мошенничество, несанкционированный доступ к ПК, нежелательный контент и т.д.).

Пароли. Использование всегда индивидуальных и сложных паролей, состоящих из букв, цифр и специальных символов.

Вирусы и антивирусы.

Персонализация. Никому не передавать свои конфиденциальные данные (логин, пароль), свидетельство о рождении, адрес и прописку, и даже ваши фотографии. Такие «цифровые следы», если их создать, могут тянуться всю жизнь. Могут навредить на пути к достижению поставленной цели. Игнорируем в сети интернет подобные запросы.

Издевательство (троллинг), травля (буллинг), травля в интернете (кибербуллинг)

2. Практическое упражнение: составление детьми правил онлайн безопасности,

работа в группах по 4-7 человек.

3. Рефлексия.

Тема 2. Средства интернет-защиты

1. Беседа. ***Понятие – личное пространство.*** Пословица: «Мой дом – моя крепость». Личное пространство – это ваша комната, семья, близкие друзья, увлечения и т.д. В реальной жизни вы же не пустите в свой дом чужого, незнакомого человека, не станете рассказывать о себе и своей семье посторонним на улице, так и в интернете нужно оберегать свое личное пространство. Для этого в интерактивном общении (социальные сетях, чатах, форумах) следует использовать псевдонимы – ники – виртуальные имена.

Как правильно выбрать ник и пароль? (правила безопасности)

Никогда не называйся своим настоящим именем и фамилией и правильно выбирай пароли!

У посторонних людей не должно быть возможности добраться до твоей личной информации.

Псевдоним/ник должен быть таким, чтобы нельзя было догадаться о возрасте, адресе, школе и другой личной информации.

Создание надежных паролей

Надежные пароли – это важные элементы защиты, которые позволяют сделать онлайн-действия более безопасными.

Основные элементы надежности пароля: длина и сложность.

Идеальный пароль – это длинный пароль, который включает буквы, знаки пунктуации, символы и цифры.

Если это возможно, следует использовать не менее 14 символов.

Чем больше разнообразных символов включает пароль, тем лучше.

Следует использовать все клавиши клавиатуры, а не только те буквы и символы, которые используются или отображаются чаще всего.

2. Практическое упражнение: создание надежного пароля, который легко запоминается.

Существует множество ***способов создания длинных и сложных паролей***.

1. Придумайте одно-два предложения (всего 10 слов). Придумайте предложение, которое имеет для вас значение. Длинные пароли самые безопасные. (Например, Ехали медведи на велосипеде, а за ними кот задом наперед)

2. Превратите предложение в ряд букв, взяв первую букву каждого слова (емнвазнкзн – 10 символов)

3. Добавьте сложности. Сделайте большими буквы, которые находятся в первой части алфавита (ЕмнВАЗкЗн (10 символов)

4. Добавьте цифры, чтобы пароль стал длиннее. (*ЕмнВ56АЗкЗн* (12 символов)

5. Добавьте знаки пунктуации, чтобы пароль стал длиннее. Поставьте знак пунктуации в начале (?ЕмнВ56АЗкЗн (13 символов)

6. Добавьте символы, чтобы пароль стал длиннее. Поставьте символ в конце ?ЕмнВ56АЗкЗн% (14 символов)

Защита пароля от чужих глаз.

Самый легкий способ запомнить пароли – записать их. Записывать пароли допустимо, если они хранятся в надежном месте.

Компьютерные мошенники используют сложные программы, с помощью которых можно быстро расшифровывать пароли.

Ошибки при создании паролей:

- Слова из словаря на любом языке.
- Слова, написанные в обратном порядке, с распространенными ошибками и аббревиатуры.
- Последовательности повторяемых символов. Например, 12345678, 222222, abcdefg или смежные символы на клавиатуре (qwerty).

- Личная информация. Ваше имя, день рождения, домашний адрес, номер телефона, номер паспорта взрослых или сходные данные.

3. Рефлексия.

Тема 3. Компьютер и здоровье

1. Беседа о кибер-зависимости (возможен вариант - комментирование презентации «Лиги безопасного интернета» для учащихся 5-7-х классов, http://www.ligainternet.ru/encyclopedia-of-security/ – Сайт «Лига безопасного интернета»: материалы доля детей, родителей, педагогов).

Последствия навязчивого вэбсерфинга, игромании и «жизни» в социальных сетях. Границы виртуальной реальности.

Ассоциации на слово «компьютер», «компьютерная зависимость»

2. Практическое упражнение в группах по 4-7 человек. Первая, третья, пятая группа запишут все плюсы компьютеров. А вторая, четвертая и шестая группы запишут минусы компьютеров. Как минимум по 7-10 пунктов.

Далее обучающиеся объединяются в две команды друг напротив друга. По очереди выслушиваем одну (+) и другую (-) команды. Первая группа приводит доводы, что человек может сделать с помощью компьютера, вторая – что компьютер не может дать человеку.

Делаем выводы. Компьютер – необходимость, без него в современном мире невозможно, он облегчает нашу работу, учебу, творчество и т.д. «Уход» в виртуальный мир надолго может обернуться многочисленными проблемами для человека.

3. Упражнение «Я - подарок для человечества». Каждый человек - уникальное существо, единственное в мире! И верить в свою исключительность нужно каждому. В чем ваша исключительность, ваша уникальность. Чем вы нужны, полезны миру? Закончите фразу «Я подарок для человечества, потому что я....».

4. Рефлексия.

Блок 7-9-е классы

Тема 1. Интернет-этика: репутация, поведение в сети

1. Беседа об интернет-безопасности: видеоблоги, авторское право, друзья в сети, тролли, манипуляции, способы противостояния (возможен вариант комментирования презентации «Лиги безопасного интернета» для учащихся средних классов, http://www.ligainternet.ru/encyclopedia-of-security/ – Сайт «Лига безопасного интернета»: материалы доля детей, родителей, педагогов).

Кибер-этика – это неформальный свод правил позитивного поведения, используемый всякий раз, когда кто-либо находится онлайн.

2. Практическое упражнение. Работа в мини-группах по 4-6 чел., чтобы найти решение проблемы в определенной ситуации.

Объяснить, что они будут работать как члены одной команды, для того чтобы найти наилучшие решения и записать их на листок ответов.

Предложить детям распределить роли, объяснив предварительно, функции каждого.

Координатор – отвечает за руководство группой, следит за временем и корректным обсуждением предложенного задания. Он будет читать задание вслух и должен быть уверен, что группа своевременно отвечает на каждый вопрос.

Регистратор – записывает ответы членов группы на лист ответов. Только они заполняют лист ответов. Он должен писать быстро и аккуратно, потому что репортеру необходимо будет зачитывать эту информацию.

Репортер – будет отчитаться за ответы по каждой задаче перед классом. Он должен говорить четко и медленно так, что все в аудитории могли услышать и понять.

Примерные задания:

- Вашему другу необходимо выступить на онлайн-мероприятии, а он переживает, что не справится.
- Виртуальный друг зовет на реальную встречу, как быть.
- Знакомого травят в социальной сети, как помочь.

- Другу пришло сообщение о большом выигрыше.
- Подруги Аня и Лена дружили давно, Ане пришлось уехать в другой город, а Лене однажды приходит сообщение с просьбой добавить в друзья с электронного адреса Ivanovo_girl@mail.ru и она решает, что это друг Ани. Новый друг задает много вопросов личного характера, и девочка чувствует себя некомфортно и не отвечает.
- Друг рассказал о новом альбоме любимого исполнителя, который можно скачать на определенном сайте. Сайт запрашивает личные данные: имя, адрес, дату рождения. 10 новых хитов всего за 1, 99$.

3. Рефлексия.

Тема 2. Интернет-безопасность

1. Беседа. Интернет – уникальная возможность нашего времени, несет в себе как плюсы, так и минусы. Использование презентации «Лиги безопасного интернета» для учащихся средней школы с комментариями, http://www.ligainternet.ru/encyclopedia-of-security/ – Сайт «Лига безопасного интернета»: материалы доля детей, родителей, педагогов).

Три основных направления по обеспечению кибербезопасности:

- защита ваших компьютеров и гаджетов от вирусов и вредоносных программ;
- виртуальное или кибермошенничество;
- нарушение морали и этики в онлайн-общении, троллинг, разрушающий ваше личное пространство.

Вредоносные программы — различное программное обеспечение (вирусы, черви, «троянские кони», шпионские программы, боты и др.), которое может нанести вред компьютеру и нарушить конфиденциальность хранящейся в нем информации. Подобные программы чаще всего снижают скорость обмена данными с интернетом, а также могут использовать твой компьютер для распространения своих копий на другие компьютеры, рассылать от твоего имени спам с адреса электронной почты или профиля какой-либо социальной сети. Вредоносное программное обеспечение использует множество методов для распространения и проникновения в компьютеры, не только через внешние носители информации (компакт-диски, флэшки и т.д.), но и через электронную почту посредством спама или скачанных из интернета файлов.

Кибермошенничество – один из видов киберпреступлений, целью которого является причинение материального или иного ущерба путем хищения личной информации пользователя (номера банковских счетов, паспортные данные, коды, пароли и др.). Отправка любых СМС на короткие номера сотовых операторов с последующим списанием средств со счета мобильного телефона сверх указанной ранее суммы либо без получения указанной услуги также является видом кибермошенничества.

Похищение аккаунтов, учетных записей. В большинстве случаев они даже не блокируются, и человек может работать на сайте, не замечая никаких изменений, однако в это же время от его имени другим людям будут приходить рекламные сообщения. Особенно актуальна такая угроза для социальных сетей.

Мошенники имеют выгоду уже от факта использования чужого компьютера, поэтому в данном случае не требуют от его владельца денежной компенсации.

Фишинг. Во многих случаях от пользователя требуют перейти по ссылке на подставной сайт и ввести там свои учетные данные, которые затем применяются для рассылки спама. Однако порой у пользователя пытаются украсть не его аккаунт, а сведения о кредитной карте.

Приобретение продуктов при помощи мобильного телефона, оплата кредитной картой, электронной валютой или, в случае с мобильным телефоном, при помощи платной SMS.

Одним из основных различий между онлайновой и традиционной торговлей является сложность идентификации того, кто находится на другом конце обменной цепочки, и риск мошенничества, который может всегда присутствовать. Одним из наиболее широко

распространенных рисков является риск «фишинга» (*от англ.* fish – рыба, рыбачить), поскольку они «выуживают» информацию.

Фишинг происходит, когда люди отвечают на ложные электронные письма, спам, которые обычно кажутся пришедшими из надежного источника, например, банка или кредитной компании. Мошенники просят ввести большой объем личной информации, например, детали банковского счета, пароли, дату рождения и так далее, которую они впоследствии могут использовать в своих целях.

Если покупка производится при помощи мобильного телефона для чего не нужна кредитная карта, проверяйте реальную стоимость услуг, условия предоставления услуги и как от нее можно отказаться.

Сейчас можно встретить онлайн-услуги, для получения которых нужно отправить СМС. Нередко результаты теста (например, на IQ), гороскопа, какие-нибудь «индивидуальные системы похудения», даются тебе только после отправки смс.

Такие файлы стоит считать подозрительными:

- Файлы с расширением .exe. Такое расширение имеют запускаемые программы.
- Файлы с именами в виде набора букв.
- Любые файлы, которые не ожидал получить, даже если они присланы со знакомого адреса. Обычно друзья предупреждают заранее, что хотят что-то отправить, или сам просишь прислать, например, фотографии. Если файл приходит без предварительной договорённости, есть шанс того, что кто-то посторонний завладел электронным адресом друга и рассылает вредоносные файлы с него.

2. Практическое упражнение в группах по 4-7 человек. Первая, третья, пятая группа запишут все плюсы компьютеров. А вторая, четвертая и шестая группы запишут минусы компьютеров. Как минимум по 7-10 пунктов.

Далее в две команды друг напротив друга. По очереди выслушиваем одну (+) и другую (-) команды. Первая группа приводит доводы, что человек может сделать с помощью компьютера, вторая – что компьютер не может дать человеку.

Делаем выводы. Компьютер – необходимость, без него в современном мире невозможно, он облегчает нашу работу, учебу, творчество и т.д. «Уход» в виртуальный мир надолго может обернуться многочисленными проблемами для человека.

3. Упражнение «Я - подарок для человечества». Каждый человек - уникальное существо, единственное в мире! И верить в свою исключительность нужно каждому. В чем ваша исключительность, ваша уникальность. Чем вы нужны, полезны миру? Закончите фразу «Я подарок для человечества, потому что я...».

4. Рефлексия.

Тема 3. Компьютер и здоровье: зависимость, границы виртуальной реальности

1. Беседа о кибер-зависимости (возможен вариант комментирования презентации «Лиги безопасного интернета» для учащихся 8-9-х классов, http://www.ligainternet.ru/encyclopedia-of-security/ – Сайт «Лига безопасного интернета»: материалы доля детей, родителей, педагогов). Последствия навязчивого вэбсерфинга, игромании и «жизни» в социальных сетях. Границы виртуальной реальности.

Ассоциации на слово «компьютер», «компьютерная зависимость»

2. Практическое упражнение: визуализация «Я – в реальности, я – в интернете».

Упражнение необходимо начать с *дыхательной подготовки.* Необходимо занять удобное положение, выпрямиться. С выпрямленными спинами легкие больше вдыхают кислорода, следовательно, мозг лучше «дышит». Закрыть глаза, сделать три медленных глубоких вдоха так тихо, чтобы никто их не слышал, и медленно выдохнуть, возможно, музыкальное сопровождение для фона.

«Сегодня мы совершим небольшое путешествие. Мы будем использовать нашу фантазию и, фантазируя, создавать различные картинки в нашем воображении. Мы с вами

отправимся в одно место. Представьте, что вы оказались в зале, из которого ведут две двери – на одной надпись «Реальность», на другой «Виртуальность (интернет)». Реальность – это обычный мир с обычными улицами, домами, людьми, предметами, а Виртуальность – это нереальный (цифровой) мир интернет-пространства, который отличается от реального. Заходите по очереди в каждую из двух дверей, запоминайте всё, что там видите и сравнивайте, чем отличаются эти два мира».

Упражнение позволяет участникам посмотреть на их взаимоотношения с виртуальностью, отметить проблемы в распределении энергии.

Возвращаемся в нашу комнату (класс), чувствуем ноги, руки, спинку стула, открываем глаза, смотрим на всех, осматриваемся вокруг. Мы в реальности. Сейчас посмотрим, что вы видели за теми двумя дверями.

Инструкция: разделить лист пополам. Составить 2 списка определений (как можно больше) «Я – в реальности», «Я – в интернете». Как вариант можно предложить составить списки определений «В реальности я никогда», «В виртуальности я никогда».

Обсуждение:

- есть ли похожие и противоположные черты, одинаковые качества, проявляющиеся в разных сферах,
- наблюдается ли полное отсутствие общих черт,
- какой список было составлять легче, а какой получился объемнее,
- каково отношение участников к тому, что есть заметные различия.

3. Рефлексия.

Тема 4. Интернет и будущее: профессии, творчество, обучение

1. Беседа о безопасных развлекающих и обучающих сайтах.

8-9-е классы. В основной школе (8-9-е классы) происходит формирование представлений о профессиональных навыках, перспективах профессионального роста и мастерства, правилах выбора профессии, умение адекватно оценить свои личностные возможности в соответствии с требованиями избираемой профессии. Начиная с этапа основной школы (8-9 классы, для ребят от 14 лет и старше), государственные бюджетные (бесплатно) и негосударственные (на платной основе) организации Санкт-Петербурга ведут комплекс профориентационных услуг и мероприятий.

10-11-е классы. Следующая ступень школьной профориентации – это старшая школа (10-11-е классы). Формируются профессионально важные качества в избранном виде деятельности, оценки и коррекции профессиональных планов; знакомство со способами достижения результатов в профессиональной деятельности, самоподготовка к избранной профессии.

Далее следует планирование карьеры.

Организации Санкт-Петербурга, оказывающие услуги в профессиональной ориентации молодежи.

1.1. Санкт-Петербургское государственное бюджетное учреждение «Центр содействия занятости и профессиональной ориентации молодежи «Вектор», подведомственное Комитету по молодежной политике и взаимодействию с общественными организациями, отмечает свой день рождения с 22 марта 1987 года и носит почетное звание первого государственного центра профориентации в России и первой в городе государственной службы психологической поддержки и профессиональной ориентации молодежи.

В Центре «Вектор» работают профессионалы, которые помогают молодежи выбрать профессию по душе, стать высококлассными специалистами и определить варианты развития в карьере. Для школьников, студентов, молодых специалистов проводятся профессиональные консультации, лекционные курсы по профориентации и рынку труда, организуются экскурсии на предприятия нашего города, активно проводятся игры, тренинги, посвящённые практическому применению и закреплению теории и навыков ориентирования в мире профессий, а также адаптации.

Старшеклассники могут посетить районные ярмарки профессий «Образование. Карьера. Досуг», которые проводит Центр «Вектор» совместно с отделами образования и учебными заведения города, студенты учреждений профессионального образования – прослушать лекции, участвовать в семинарах-тренингах, посетить экскурсии на предприятия, узнать о прохождении производственной практики и трудоустройстве.

Услуги Центра «Вектор» БЕСПЛАТНЫЕ для всех горожан в возрасте от 14 до 30 лет. Контакты: 190068, Санкт-Петербург, Вознесенский пр., дом 25/78 (вход под арку, дверь направо, 5 этаж).

190068, Санкт-Петербург, набережная канала Грибоедова, д.105 (для лиц с ограниченными возможностями), info@profvector.spb.ru

Телефоны

запись на профессиональное консультирование	314-72-45, 312-11-12
приемная директора	315-30-27
финансово-бухгалтерский отдел	571-23-57
отдел по организационно-правовой работе и материально-технического обеспечения	571-42-74
отдел профессионального консультирования и дополнительного образования	314-72-45
отдел профессионального консультирования и дополнительного образования (медико-психологические консультации)	312-11-12
отдел информационно-методической работы	314-74-28
отдел развития молодежных инициатив.	571-83-66

https://profvector.spb.ru/

1.2. Академия дополнительного профессионального образования (АДПО) является автономной некомерческой организацией, созданной на базе старейшего государственного ведомственного заведения (Госплан СССР, ЦСУ РСФСР), основанного в 1949 году.

Академия имеет бессрочную лицензию на осуществение образовательной деятельности. Наличие лицензии у образовательного учреждения свидетельствует о его статусе и качестве реализуемых образовательных программ и обучения в целом. А родителям наших учеников наличие лицензии позволит вернуть в семейный бюджет налоговый вычет по расходам на обучение.

В целях более углублённой профориентационной подготовки своих учеников и выпускников, содействуя их успешному поступлению на бюджетное обучение в вузы и колледжи, Академия активно сотрудничает с ведущими петербургскими учебными заведениями.

АДПО имеет статус Microsoft IT Academy, является сертифицированным центром по подготовке к международным Кембриджским экзаменам и имеет статус Cambridge English Exam Preparation Centre, является Региональным представительством "Центра тестирования и развития Гуманитарные технологии" при МГУ им. М.В. Ломоносова. В 2009 году получен Диплом лауреата международной премии «Лучшее предприятие года» и вручена Золотая медаль качества «Европейский гранд» (Люцерн, Швейцария). Руководители АДПО имеют научные степени и учёные звания.

Академия дополнительного профессионального образования – член Союза «Санкт-Петербургская торгово-промышленная палата».

Члены СПб ТПП – это компании, заинтересованные в росте и развитии своего бизнеса, укреплении своих позиций как на российском, так и на зарубежном рынках.

Телефон (812) 612-11-22

https://spbapo.ru/uslugi

В Академии дополнительного профессионального образования может подготовиться к

ОГЭ ученик 9 класса, может подготовиться к ЕГЭ ученик 11 класса, студент колледжа или выпускник прошлых лет, чтобы сдать ЕГЭ впервые или улучшить свой предыдущий результат.

1.3. Образовательный центр THINK - профориентационная консультация бесплатно, 8 (812) 244-71-26 https://center-think.ru/

Санкт-Петербург, Таврическая ул. 35, офис 27

Санкт-Петербург, Московский проспект 183/185

Санкт-Петербург, Таврическая ул. 35, офис

Консультация включает несколько этапов:

- Тестирование по предметам. Тестирование по 3-5 предметам для определения реального уровня знаний. Позволяет получить представление об уровне интереса к различным сферам профессиональной деятельности, а также поможет определиться с выбором ОГЭ, ЕГЭ и дополнительных занятий.
- Консультация специалиста. Проходит личная беседа с преподавателем, в результате которой даём объективную оценку уровня знаний и рекомендации по обучению.
- Диагностика знаний. Учитывая предрасположенность ребенка и резюме преподавателей, консультируем по направлениям и специальностям. Подбираем возможные университеты для обучения.

1.4. Психологический центр «Вторая навигация» – многофункциональный практико-ориентированный центр психологической помощи и поддержки, кризисного консультирования, семейного, личностного, профессионального, делового и организационного развития.

Запись на консультацию в удобное для Вас время/день.

Записаться: +7 953 355-22-52 (WhatsApp), +7 963 321-64-92

Онлайн консультации.

Адрес: г. Санкт-Петербург, ул. Барочная, д. 4, м. Чкаловская.

https://2navigation.ru/

2. Обмен собственными проверенными ресурсами во «всемирной паутине», по возможности просмотр страничек онлайн.

3. Рефлексия.

Глоссарий

1. Вредные привычки — совокупность различных форм социального поведения, регулярно совершаемых человеком и приносящих вред здоровью человека или окружающей его среде в результате неблагоприятного воздействия социально-психологических и индивидуально-биологических факторов.
2. Зависимость - связанность явлений, предопределяющая их существование или сосуществование; обусловленность
3. Кибер – это слово-приставка, означающая «связанный с компьютером, интернетом, показывает отношение чего-либо к кибернетике.
4. Кибернетика – (*др-греч.* - искусство управления) – наука об общих закономерностях получения, хранения, преобразования и передачи информации в сложных управляющих системах, будь то машины, живые организмы или общество.
5. Кибербуллинг (*англ.* bullying – задирать, запугивать, травля) — агрессивное преследование в сети Интернет одного из членов коллектива (особенно это актуально сейчас для коллектива школьников) со стороны остальных членов коллектива или его части. При травле жертва оказывается не в состоянии защитить себя от нападок, таким образом, травля отличается от конфликта, где силы сторон примерно равны. Кибербуллинг – травля в психологической форме. Проявляется во всех возрастных и социальных группах. Буллинг приводит к тому, что жертва теряет уверенность в себе. Также это явление может приводить к разной тяжести психическим отклонениям, а также психосоматическим заболеваниям, и может

явиться причиной самоубийства.

6. Миф (*др.-греч*. μῦθος - «речь, слово; сказание, предание») — повествование, передающее представления людей о мире, месте человека в нём, о происхождении всего сущего, о богах и героях.
7. Наркотик (*от греч*. ναρκωτικός — приводящий в оцепенение, *греч*. νάρκωσις — ступор) – согласно определению ВОЗ, «химический агент, вызывающий ступор, кому или нечувствительность к боли.
8. Неуверенное поведение – это отказ от собственных желаний с целью помочь кому-либо, постоянное игнорирование собственных потребностей, это сочетание зависимого и агрессивного поведения, которая проявляется, когда не сформировано уверенное поведение.
9. Профилактика (превенция) – деятельность, направленная на предупреждение приобщения к чему-либо и преодоление последствий. Профилактика (от *греч.* πρόφύλακτικός «предохранительный») – предварительные меры для недопущения чего-либо. Профилактика – термин, означающий комплекс различного рода мероприятий, направленных на предупреждение какого-либо явления и/или устранение факторов риска.
10. Профилактика (превенция) наркомании – деятельность, направленная на предупреждение приобщения к наркотикам и преодоление последствий наркопотребления.
11. Психическая зависимость — часть синдрома зависимости, включающая навязчивое влечение к психоактивному веществу и способность достижения состояния психического комфорта в предмете влечения.
12. Психологическая манипуляция — тип социального воздействия или социально-психологический феномен, представляющий собой стремление изменить восприятие или поведение других людей при помощи скрытой, обманной и насильственной тактики в интересах манипулятора.
13. Скимминг – считывание данных банковской карты при помощи устанавливаемого на банкомат специального устройства (скиммера). С помощью него злоумышленники копируют информацию с магнитной полосы карты (имя держателя, номер и срок действия карты). Для считывания пинкода преступники устанавливают на банкомат миниатюрную камеру или накладку на клавиатуру. Завладев информацией о карте, мошенник изготавливает ее дубликат и распоряжается денежными средствами держателя оригинальной карты.
14. Троллинг — форма провокации или издевательства в сетевом общении, использующаяся как персонифицированными участниками, заинтересованными в большей узнаваемости, публичности, эпатаже, так и анонимными пользователями без возможности их идентификации. В интернете «троллями» называют лиц, провоцирующих эмоциональную перепалку (чаще всего с переходом на личности), преследующих других пользователей или (реже) выдающих себя за других людей. Это слово изначально происходит не от названия мифологических троллей, а от рыболовного термина «тро́ллинг» (*англ.* trolling — ловля на блесну), но созвучие так прижилось, что отождествление интернет-хулиганов с мифологическими троллями стало общим местом и даже темой для шуток и карикатур.
15. Уверенное поведение - поведение, выражающее внутреннюю силу и спокойствие.
16. Факт (*лат.* factum) — термин, в широком смысле может выступать как синоним истины; событие или результат; реальное, а не вымышленное; конкретное и единичное в противоположность общему и абстрактному.
17. Фишинг - кража любых персональных данных, владение которыми позволяет преступникам получать выгоду. Это серии и номера паспортов, реквизиты банковских карт и счетов, пароли для входа в электронную почту, платежную систему и аккаунты в социальных сетях.

Литературно-методическое обеспечение

1. http://www.saferunet.ru/ – Центр Безопасного Интернета в России
2. http://www.saferunet.ru/post/hot_line.php – Горячая линия безопасного Интернета
3. http://www.saferunet.ru/help/ – Линия Помощи жертвам Интернет-угроз (Центр безопасного интернета в РФ)
4. http://detionline.com/helpline/about - Дети России онлайн
5. https://www.kaspersky.ru/home-security?campaign=kl-ru_yadirectps-1_acq_ona_sem_bra_onl_b2c_ya_link_____&ksid=e488f0c7-5253-42d9-b857-f0fec35a14d7&ksprof_id=426&ksaffcode=cr8744818155&ksdevice=desktop&kschadid=8744818155&kschname=yandex&kpid=Yandex%7C11212284%7C536241869%7C8744818155%7Ckwd-22043265496%7Cdesktop&yclid=2093460331452205104 – Касперский онлайн-безопасность для вас и вашей семьи
6. https://www.kaspersky.ru/resource-center/preemptive-safety/kids-online-safety – Защита детей в интернете, центр Касперский.
7. http://www.microsoft.com/ru-ru/security/default.aspx – Центр Безопасности в интернете от компании Microsoft
8. https://infourok.ru/urok-bezopasnost-shkolnikov-v-seti-internet-1296656.html – Урок безопасности
9. https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii/- Безопасный-интернет-детям, сайт МВД РФ.
10. https://www.твоятерритория.онлайн/ – Психологическая помощь подросткам, молодёжи ежедневно (телефон доверия).
11. https://www.youtube.com/watch?v=9OVdJydDMbg&t=14s – Безопасность школьников в сети интернет (видеоурок)
12. https://deti-online.com/ – Сайт для детей до 15 лет: аудио-видеоматериалы.
13. https://rosuchebnik.ru/material/dni-interneta-kak-rasskazat-shkolnikam-o-bezopasnosti-v-seti/ – Сайт для детей, родителей, педагогов: пособия, плакаты, презентации для уроков по безопасности в интернете
14. http://www.ligainternet.ru/encyclopedia-of-security/ – Сайт «Лига безопасного интернета»: материалы доля детей, родителей, педагогов.
15. https://internet-i-deti.ru/catalog/art/70/ – Браузер для детей «ГОГУЛЬ», федеральная программа детского безопасного интернета
16. http://cpmss.edu.ru/%d0%b4%d0%b5%d1%82%d1%8f%d0%bc-%d0%b8-%d0%bf%d0%be%d0%b4%d1%80%d0%be%d1%81%d1%82%d0%ba%d0%b0%d0%bc/ - Сайт ЦПМСС, информация всем участникам образовательного процесса

Календарный учебный график

дополнительной общеобразовательной общеразвивающей программы

«Безопасность в сети Интернет»

Год обучения	Дата начала обучения по программе	Дата окончания обучения по программе	Всего учебных недель	Количество учебных часов	Режим занятий
2022-2023 учебный год	01.09.2022	31.05.2023	33	11	По согласованию с образовательной организацией

Приложение 1

Правила безопасности в сети интернет. Памятка школьникам средних классов

Это надо знать:

При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Также, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.

Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.

Нежелательные письма от незнакомых людей называются «Спам». Если вы получили такое письмо, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылась вам спам.

Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.

Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя в вашем отношении неподобающим образом, сообщите об этом.

Если вас кто-то расстроил или обидел, расскажите все взрослому.

Приложение 2

Правила безопасности в сети интернет. Памятка школьникам старших классов

Это надо знать:

Не желательно размещать персональную информацию в Интернете.

Персональная информация – это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.

Если вы публикуете фото или видео в интернете – каждый может посмотреть их.

Не отвечайте на спам (нежелательную электронную почту).

Не открывайте файлы, которые прислали неизвестные Вам люди. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.

Не добавляйте незнакомых людей в свой контакт лист.

Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.

Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!

Никогда не поздно рассказать взрослым, если вас кто-то обидел.

Приложение 3

Правила безопасности в сети интернет. Учителям и преподавателям

Это надо знать:

Подготовьтесь. Изучите технику безопасности в Интернете, чтобы знать виды Интернет-угроз, уметь их распознать и предотвратить. Выясните, какими функциями обладают компьютеры подопечных, а также какое программное обеспечение на них установлено.

Прежде чем позволить ребенку работу за компьютером, расскажите ему как можно больше о виртуальном мире, его возможностях и опасностях.

Не позволяйте детям самостоятельно исследовать Интернет-пространство, они могут столкнуться с агрессивным контентом.

Выберите интересные ресурсы и предложите детям изучить их вместе.

Убедитесь, что на компьютерах установлены и правильно настроены средства фильтрации контента, спама и антивирусы.

Приложение 4

Физкультминутка (1 мин.)

Мы все вместе улыбнемся,
Подмигнем слегка друг другу,
Вправо, влево повернемся
И кивнем затем по кругу.
Все идеи победили,
Вверх взметнулись наши руки.
Груз забот с себя стряхнули
И продолжим путь науки.

Приложение 5

Анкета для учащихся

Дорогой друг! Мы приглашаем тебя принять участие в анкетировании, посвященном интернету. Пожалуйста, ответь на представленные ниже вопросы: отвечай быстро, не задумываясь – правильных и неправильных ответов нет, а есть разнообразие мнений и твое мнение нам очень важно.

Укажи свой возраст _____ пол _____ класс_____

1. Есть ли у тебя дома компьютер, подключенный к сети Интернет?
   - Да, имеется компьютер, подключенный к сети Интернет
   - Есть компьютер, не подключенный к сети Интернет
   - Компьютера нет
2. Есть ли у вас в школе Интернет?
   - Да
   - Нет
   - Не знаю
3. Пользуешься ли ты Интернетом в школе?
   - Да
   - Нет
4. Установлены ли в твоей школе программы, ограничивающие доступ на какие-либо сайты?
   - Да
   - Нет
   - Не знаю
   - Другое
5. Как часто ты пользуешься Интернет?
   - Один-два раза в неделю
   - Один-два раза в месяц
   - Один-два раза в день
   - Я живу в интернете
   - Не пользуюсь интернетом вообще
   - Другое
6. Сколько времени ты проводишь в Интернете за один сеанс?
   - от 10 – 20 минут
   - от 1 – 3 часов
   - от 5 – 10 часов
   - Другое:
7. Получаешь ли ты удовольствие от своей работы в Интернете?
   - Никогда
   - Иногда
   - Часто
   - Всегда
8. В Интернете я обычно пользуюсь электронной почтой
   - Часто

- Редко
- Никогда

9. В интернете я обычно общаюсь в чатах, «В Контакте», «одноклассниках» и других социальных сетях
   - Часто
   - Редко
   - Никогда
10. В интернете я обычно общаюсь с друзьями по WhatsApp, Telegram
   - Часто
   - Редко
   - Никогда
11. В интернете я обычно веду виртуальный дневник (блог)
   - Часто
   - Редко
   - Никогда
12. В интернете я обычно ищу информацию для учебы
   - Часто
   - Редко
   - Никогда
13. В интернете я обычно ищу информацию для культурного и духовного развития
   - Часто
   - Редко
   - Никогда
14. В интернете я обычно развлекаюсь
   - Часто
   - Редко
   - Никогда
15. В интернете я обычно качаю программы, музыку, фото, видео
   - Часто
   - Редко
   - Никогда
16. В интернете я обычно слушаю Интернет-радио
   - Часто
   - Редко
   - Никогда
17. В интернете я обычно смотрю Интернет-телевидение
   - Часто
   - Редко
   - Никогда
18. В интернете я обычно узнаю о последних событиях и новостях в стране и мире
   - Часто
   - Редко
   - Никогда
19. В интернете я обычно играю в онлайн-игры
   - Часто
   - Редко
   - Никогда
20. В интернет я обычно принимаю участие в интернет-акциях, голосовании и др.
   - Часто
   - Редко
   - Никогда
21. В интернет я обычно просматриваю сайты, которые мои родители запретили бы мне смотреть

- Часто
- Редко
- Никогда

22. Напиши, чем ты еще занимаешься в Интернете, но это не попало в список

_____

_____

23. В реальной жизни мы нередко сталкиваемся с неприятностями и опасностями. Как ты считаешь, есть ли опасность в интернете?

- Да
- Иногда
- Нет
- Не знаю

24. Сталкиваешься ли ты с вирусами в интернете?

- Часто
- Редко
- Никогда

25. Сталкиваешься ли ты с мошенничеством/кражами в интернете?

- Часто
- Редко
- Никогда

26. Сталкиваешься ли ты с оскорблением и унижением со стороны других пользователей в интернете?

- Часто
- Редко
- Никогда

27. Сталкиваешься ли ты с сексуальными домогательствами со стороны других пользователей в интернете?

- Часто
- Редко
- Никогда

28. Сталкиваешься ли ты с порнографией в интернете?

- Часто
- Редко
- Никогда

29. Сталкиваешься ли ты с психологическим давлением со стороны других пользователей в интернете?

- Часто
- Редко
- Никогда

30. Сталкиваешься ли ты с терроризмом в интернете?

- Часто
- Редко
- Никогда

31. Сталкиваешься ли ты с экстремизмом в интернете?

- Часто
- Редко
- Никогда

32. Сталкиваешься ли ты призывами причинить вред себе и/или окружающим в интернете?

- Часто
- Редко
- Никогда

33. Часто ли ты сталкиваешься с информацией, которая раздражает и вызывает неприятные эмоции?

- Часто
- Редко
- Никогда

34. Назови, с чем еще ты сталкивался в интернете, но это не попало в список

_____

_____

35. Ты даешь в интернете малознакомым (едва знакомым) людям адрес своей электронной почты?

- Да
- Нет
- Иногда

36. Ты даешь в интернете малознакомым (едва знакомым) людям номер своего мобильного телефона?

- Да
- Нет
- Иногда

37. Ты даешь в интернете малознакомым (едва знакомым) людям номер своего домашнего телефона?

- Да
- Нет
- Иногда

38. Ты даешь в интернете малознакомым (едва знакомым) людям номер своей школы или класса?

- Да
- Нет
- Иногда

39. Ты даешь в интернете малознакомым (едва знакомым) людям свою фотографию и фотографии своих родственников?

- Да
- Нет
- Иногда

40. Ты пытаешься встречаться с людьми, с которыми познакомился в интернете?

- Да
- Нет
- Иногда

41. Какие сайты ты посещаешь чаще всего?

- игровые
- сайты с музыкой и фильмами
- сайты Интернет-знакомств
- сайты для детей
- сайты для взрослых
- другое (*Напиши название своих любимых сайтов, форумов и т.д.)*_____

_____

42. Рассказываешь ли ты родителям о том, чем занимаешься в сети?

- Всегда
- Иногда
- Редко
- Не рассказываю

43. Установлены ли на твоем домашнем компьютере программы, ограничивающие вход на какие-либо сайты?

- Да
- Нет
- Не знаю

44. Как твои родители относятся к твоей деятельности в интернете?

- разрешают свободно пользоваться и не ограничивают во времени;
- устанавливают временной режим и следят за тем, какие сайты я посещаю;
- разрешают заходить в Интернет только в своем присутствии;
- запрещают пользоваться Интернетом вообще;
- Другое:

45. По твоему мнению, интернет – это …

_____

_____

Приложение 6

Консультационный этап. Примерные материалы родительского собрания на тему «Безопасность в сети интернет» (по запросу ОУ)

Вопросы:

- Чем является компьютер в вашей семье? Приведите примеры ситуаций из вашей жизни, связанных с положительными и отрицательными эмоциями по поводу использования компьютера.
- Что сделаем, чтобы не повторять ежедневно: “Ты опять весь день просидел (а) за компьютером”?
- Какую пользу извлекает Ваш ребенок при использовании сети Интернет?
- Какие опасности ждут Вашего ребенка в сети Интернет?

Пять типов Интернет-зависимости на сегодняшний день:

- бесконечный веб-серфинг – постоянные «путешествия» по Интернету с целью поиска информации.
- пристрастие к виртуальному общению и виртуальным знакомствам, характеризуется большими объёмами переписки, постоянным участием в чатах, форумах, избыточностью знакомых и друзей из Интернета.
- игровая зависимость – навязчивое увлечение сетевыми играми.
- навязчивая финансовая потребность – игра по сети в азартные игры, ненужные покупки в интернет-магазинах.
- киберсексуальная зависимость – навязчивое влечение к посещению порносайтов.

Советы по безопасности, или как Вы можете защитить своих детей:

- Создайте список домашних правил интернета при участии детей.
- Используйте программы по защите детей в сети. Существует ряд программ, позволяющих защитить собственного ребенка от посещения, нежелательных сайтов.

Программа «Интернет-Цензор» – интернет-фильтр, предназначенный для блокировки потенциально опасных для здоровья и психики подростка сайтов.

- Беседуйте с детьми об их друзьях в интернете и о том, чем они занимаются так, как если бы вы говорили о чем-то другом.
- Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по интернету.
- Позволяйте детям заходить на детские сайты только с хорошей репутацией. Научите детей никогда не выдавать личную информацию по электронной почте, в чатах, системах мгновенного обмена сообщениями, регистрационных формах, личных профилях и при регистрации на конкурсы в интернете.
- Научите детей не загружать программы без вашего разрешения — они могут случайно загрузить вирус или шпионскую программу.
- Чтобы ребенок не мог заниматься чем-то посторонним без вашего ведома,

создайте для него учетную запись с ограниченными правами.

- Приучите детей сообщать вам, если что-либо или кто-либо в сети тревожит их или угрожает. Оставайтесь спокойными и напомните детям, что они в безопасности, если рассказали вам об этом. Похвалите их и побуждайте подойти еще раз, если случай повторится.
  Расскажите детям о порнографии в интернете и направьте их на хорошие сайты о здоровье и половой жизни.
- Настаивайте на том, чтобы дети предоставили вам доступ к своей электронной почте, чтобы вы могли убедиться, что они не общаются с незнакомцами.
- Расскажите детям об ответственном поведении в интернете. Ребята ни в коем случае не должны использовать сеть для хулиганства, сплетен или угроз другим.
- Если вы обеспокоены безопасностью ребенка при его работе в интернете или при использовании мобильной связи, обратитесь на линию помощи «Дети онлайн». Эксперты помогут решить проблему, а также проконсультируют по вопросу безопасного использования детьми мобильной связи и интернет, телефон 8−800−25−000−15 (звонок по России бесплатный, прием звонков осуществляется по рабочим дням с 9−00 до 18−00 мск).

Или направьте Ваше письмо по адресу: helpline@detionline.com

Подробнее о Линии помощи вы можете узнать на сайте http://detionline.com

И будьте внимательны к своим детям!

Приложение 7

Отзыв о занятии, посвященном безопасности в интернете

Школа _____ класс _____

Понравилось ли вам занятие _____

Оцените по 10-ти бальной шкале _____

Как вы думаете, занятие поможет вам разрешить проблемные жизненные ситуации, связанные с компьютером, интернетом? _____

Хотели бы вы продолжить встречи по данной теме? _____

Желаемая форма занятий: индивидуальная групповая (подчеркните, пожалуйста)

Обратитесь ли вы в случае проблем в интернете на линию помощи «Дети онлайн» 8 800 25 000 15 _____

Благодарим вас за ответы!