КРУГЛЫЙ СТОЛ «РЕБЁНОК И КОМПЬЮТЕР».

Целевая группа: родители учащихся IV класса.
Время проведения: I четверть.

Цель: повышение информационной компетентности родителей.
Задачи:
- познакомить родителей с возможными рисками при использовании интернета детьми и дать рекомендации по их предотвращению;
- повысить уровень грамотности родителей в вопросах кибербезопасности;
- подобрать и предложить родителям в помощь методические материалы по вопросу информационной безопасности.

Вопросы для обсуждения:
1. Гаджеты и здоровье.
2. Интернет без опасности.
3. Кибербезопасность детей.

Ход мероприятия:

При правильном подходе к занятиям на компьютере
можно извлечь максимум пользы для развития ребенка.
Б.Шлимович.

Вступительное слово классного руководителя.

Персональные компьютеры и смартфоны, выполняющие функции не только телефона, но и универсального мини-компьютера, записной книжки, фото- и видеокамеры прочно вошли в нашу повседневную жизнь и оказались тесно переплетенными с работой, учебой и досугом.

«Ребёнок и компьютер» – такова тема нашего родительского университета.

Обсуждение вопроса «Гаджеты и здоровье»

Каким образом использование компьютера и гаджетов влияет на здоровье и безопасность детей? Стоит ли ограничивать время их использования? Эти вопросы волнуют сегодня как родителей, так и педагогов.

Слово «гаджет» образовано от английского «gadget», переводится как «прибор, приспособление». Основные виды гаджетов, которые используют учащиеся, условно можно разделить на две категории.

1. Мобильные гаджеты – сюда можно отнести смартфоны, планшеты и другие средства коммуникации.

2. Смарт-часы – в эту категорию выделяют как электронные часы, снабженные множеством дополнительных функций, так и фитнес-браслеты, созданные специально для того, чтобы отслеживать активность.

Можно выделить следующие положительные моменты использования данных устройств:

✓ Обучение младших школьников. В интернете для детей можно подыскать различные обучающие программы, сайты о природе, искусстве, других удивительных вещах. Не выходя из дома, вы с ребёнком можете посетить виртуальный музей или принять участие в интеллектуальной олимпиаде.

✓ Доступ прямо из дома к большому количеству полезной информации. В интернете школьники могут прочитать последние новости, найти тексты книг, отыскать интересную информацию. Преимущество интернета перед библиотекой – мгновенное поступление новой информации.

✓ Связь с одноклассниками и учителями. Очень хороши специальные блоги и группы в социальных сетях, создаваемые для учеников определенного класса. Здесь учитель и ученики могут обмениваться информацией и новостями, совместно работать над проектами и др.

Ненормированное использование гаджетов может привести к ряду негативных последствий:

✓ Проблемы со здоровьем. Частое сидение за компьютером или планшетом может привести к ухудшению зрения, нарушению осанки, проблемам с мышцами (от их длительной неподвижности), кислородному голоданию мозга (в результате сдавливания сосудов и отсутствия свежего воздуха), расстройствам сна.

✓ Психологические проблемы. Дети, с раннего возраста много пользующиеся гаджетами и мало времени проводящие со сверстниками, могут иметь проблемы с социальной адаптацией. Им трудно общаться с людьми, находить с ними общий язык, они робки и застенчивы, мало знают о жизни за пределами компьютера и часто теряются в реальных жизненных ситуациях.

✓ Зависимость. Это самое серьезное последствие от использования персональных компьютеров и гаджетов. Оно формируется под влиянием многих аспектов (частое использование устройства, отсутствие других интересов в жизни, проблемы личного характера и т.д.).

Что мы можем сделать, чтобы гаджеты не оказывали негативного влияния на наших детей? Задача взрослых – научить детей правильно и с умом использовать гаджеты. И, конечно, самое главное – уделять как можно больше внимания общению со своим детьми.

Обсуждение вопроса «Интернет без опасности».

Дети воспринимают интернет как повседневную и естественную среду обитания и зачастую оказываются неспособны предвосхитить риски и угрозы сети, в результате чего оказываются среди наиболее уязвимых категорий ее пользователей. Поэтому при освоении цифровых технологий они нуждаются

в поддержке самых близких и значимых взрослых, ответственных за их жизнь, здоровье и безопасность – своих родителей.

Родители, приходя вечером с работы и видя свое чадо с искрящимися глазами возле ноутбука, задают себе один и тот же вопрос: что за магнит есть в просторах интернета и притягивает внимание всех детей?

На самом деле, все предельно просто. Дети – это маленькие растущие личности, которые глотают общение и информацию, как воздух – жадно и восхищенно. Для них интернет – другая планета, на которой они чувствуют себя комфортно и свободно. Почему? Потому что можно покрутить ее, как глобус, и найти тот континент, ту потребность, которой так не хватало, и реализовать ее одним щелчком мыши .

Если вы хотите, чтобы ваш ребёнок с пользой использовал сеть интернет, изучите его потребности, предложите ему ресурсы. Например, вы можете воспользоваться материалами мультимедийного учебного дистанционного курса безопасного пользования ресурсами сети интернет (далее - Курса). *Доступ по ссылке: https://onlinesafety.info/#/home.*

Основная задача Курса – донести ребёнку общие сведения о безопасности в интернете. Курс построен таким образом, что в самом начале ребенок может выбрать себе проводника (мальчика или девочку), который поможет пройти весь курс. Все элементы Курса озвучиваются голосом выбранного героя. В процессе прохождения курса ребёнок периодически отвечает на вопросы, что позволяет эффективно закрепить полученные знания .

Обсуждение вопроса «Кибербезопасность детей».

В сети ребенок не менее уязвим, чем в реальном мире. Поэтому очень важно не только самим знать правила поведения в виртуальном мире, но и рассказать о них детям.

Законные представители знакомятся с памяткой «Правила цифровой гигиены» .

Научить ребенка основам кибербезопасности быстро вряд ли получится. Это процесс комплексный, требующий сил, терпения и времени. Приступать к обучению лучше всего с момента, когда ребенок получает первый гаджет.

В целом, существует три категории угроз, с которыми дети сталкиваются в интернете:

1. Незнакомцы. Злоумышленники скрываются на сайтах, привлекающих детей, таких как сайты социальных сетей и онлайн-игр. Такие злоумышленники часто сами притворяются детьми. Этот метод называется кэтфишинг. Также существуют хакеры и киберпреступники, атакующие всех пользователей с недостаточно высоким уровнем безопасности, не важно, ребенок это или взрослый. Они также могут попытаться обманом выяснить у ребенка пароли или платежную информацию.

2. Сверстники. Ваш ребенок может подвергаться издевательствам или травле со стороны своих знакомых. Это часто происходит в личных чатах в

социальных сетях и приложениях для обмена сообщениями. Иногда другие дети могут публиковать личную информацию вашего ребенка, что доставляет ему сильные страдания. Если такая информация имеет сексуальный характер, например, интимные фотографии, это может быть уголовным преступлением.

3. Сами дети. Дети без присмотра могут сами создать для себя опасные ситуации в сети. Они часто нажимают кнопки или устанавливают программное обеспечение, не понимая последствий своих действий, а также публикуют личную информацию, например, дату рождения или адрес.

Некоторые из этих угроз являются социальными угрозами – они связаны с вымогательством или манипуляциями. Часто незнакомец завоевывает доверие ребенка, а затем пользуется этим. Чтобы защититься от этих угроз, ребенку необходимо знать, как безопасно общаться с другими людьми.

Другой тип угроз – это цифровые угрозы, когда кто-то использует технологии для доступа к данным. Это могут быть вредоносные программы (например, для кражи личных данных), или фишинг (вынуждение обманным путем посетить поддельный веб-сайт). Для защиты от такого типа угроз необходимо объяснить ребенку, как правильно использовать интернет и установить надёжные антивирусные программы .

Цифровой мир не должен пугать детей и родителей. Гораздо правильнее не беспокоиться о том, что может случиться, а сосредоточиться на обучении детей навыкам, необходимым для безопасности в сети.

Вместе со своими детьми вы можете посмотреть и обсудить образовательные мультфильмы «Фикси-советы. Осторожней в Интернете!» *Доступ – по ссылке (https://www.youtube.com/watch?v=TUodzCtBSWU).*

Если вы заметили, что, побывав в сети, ваш ребенок ведет себя непривычно тихо (или же наоборот чересчур возбужден и раздражителен), вероятно, с ним произошло что-то нехорошее – это стоит обсудить.

Роль беседы с глазу на глаз трудно переоценить. С одной стороны, она позволяет выявить проблему прежде, чем та выйдет из-под контроля. А с другой, дает ребенку понять, как он важен для вас. Относитесь к вопросам кибербезопасности всерьез. Тогда вы послужите примером для своих детей, и они будут без страха и с удовольствием пользоваться интернетом. А когда подрастут, у них уже будет сформировано представление о сетевом этикете.

Родителям вручается памятка «Как не стать жертвой киберпреступника».

Подведение итогов.

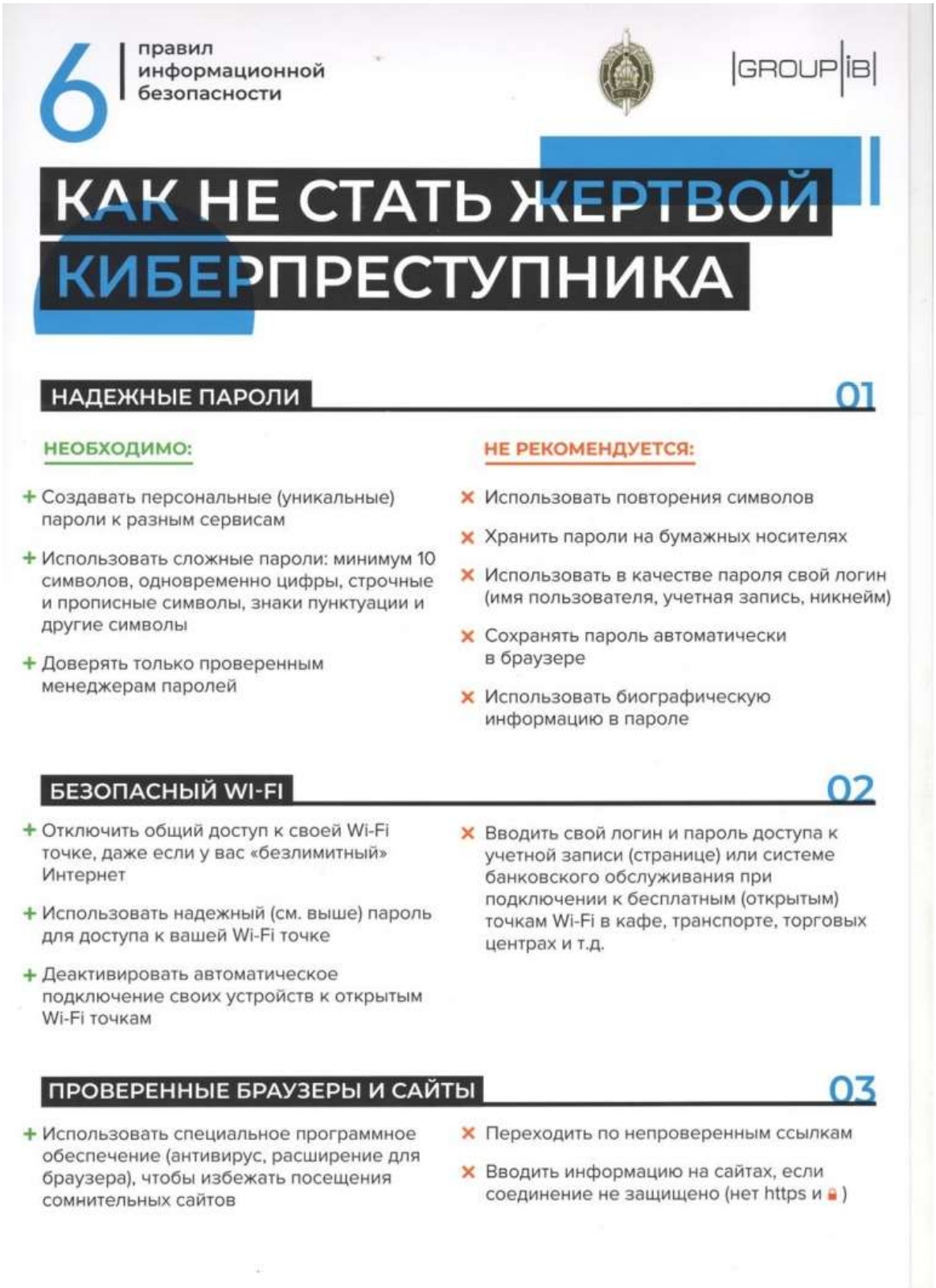
Завершить нашу встречу я хочу следующими вопросами. Может ли компьютер или смартфон заменить общение с родителями? А общение с друзьями, другими людьми, природой? Кто должен учить детей цифровой грамотности? Вопросы риторические. Но каждый из вас должен ответить на них сам себе.

Приложение 1.

Памятка для родителей «Правила цифровой гигиены».

Приложение 2.

Памятка для родителей «Как не стать жертвой киберпреступника».



6 правил информационной безопасности

GROUP-IB

КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПНИКА

НАДЕЖНЫЕ ПАРОЛИ 01

НЕОБХОДИМО:

+ Создавать персональные (уникальные) пароли к разным сервисам
+ Использовать сложные пароли: минимум 10 символов, одновременно цифры, строчные и прописные символы, знаки пунктуации и другие символы
+ Доверять только проверенным менеджерам паролей

НЕ РЕКОМЕНДУЕТСЯ:

× Использовать повторения символов
× Хранить пароли на бумажных носителях
× Использовать в качестве пароля свой логин (имя пользователя, учетная запись, никнейм)
× Сохранять пароль автоматически в браузере
× Использовать биографическую информацию в пароле

БЕЗОПАСНЫЙ WI-FI 02

+ Отключить общий доступ к своей Wi-Fi точке, даже если у вас «безлимитный» Интернет
+ Использовать надежный (см. выше) пароль для доступа к вашей Wi-Fi точке
+ Деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам

× Вводить свой логин и пароль доступа к учетной записи (странице) или системе банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т.д.

ПРОВЕРЕННЫЕ БРАУЗЕРЫ И САЙТЫ 03

+ Использовать специальное программное обеспечение (антивирус, расширение для браузера), чтобы избежать посещения сомнительных сайтов

× Переходить по непроверенным ссылкам
× Вводить информацию на сайтах, если соединение не защищено (нет https и 🔒)

БЕЗОПАСНОСТЬ ЭЛЕКТРОННОЙ ПОЧТЫ 04

НЕОБХОДИМО:

+ Подключить двухфакторную аутентификацию
+ Использовать минимум 2 типа e-mail адресов: закрытый (только для привязки устройств и средств их защиты) и открытый (для переписки, подписок и т.д.)
+ Использовать СПАМ-фильтры

НЕ РЕКОМЕНДУЕТСЯ:

× Реагировать на письма от неизвестного отправителя: скорее всего это спам или мошенники
× Открывать подозрительное вложение к письму: сначала позвоните отправителю и узнайте, что это за файл

ИСПОЛЬЗОВАНИЕ ПРИЛОЖЕНИЙ, СОЦСЕТЕЙ И МЕССЕНДЖЕРОВ 05

+ Устанавливать приложения только из PlayMarket, AppStore или из проверенных источников
+ Обращать внимание, к каким функциям гаджета приложение запрашивает доступ
+ Обмениваться сообщениями в соцсетях и мессенджерах, только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения

× Размещать персональную и контактную информацию о себе в открытом доступе
× Использовать указание геолокации на фото в постах
× Отвечать на обидные выражения и агрессию в соцсетях – лучше напишите об этом администратору ресурса
× Употреблять ненормативную лексику при общении
× Устанавливать приложения с низким рейтингом и отрицательными отзывами

ЗАЩИТА ДАННЫХ БАНКОВСКОЙ КАРТОЧКИ 06

+ Хранить в тайне пин-код карты
+ Прикрывать ладонью клавиатуру при вводе пин-кода
+ Оформить отдельную карту для онлайн-покупок и не держать на ней большие суммы
+ Использовать услугу «3-D Secure» и лимиты на максимальные суммы онлайн-операций
+ Скрыть CVV-код на карте (трехзначный номер на обратной стороне), предварительно сохранив его

× Хранить пин-код вместе с карточкой / на карточке
× Сообщать CVV-код или отправлять его фото
× Распространять свои паспортные данные (информацию личного характера, номер мобильного телефона), «логин» и «пароль» доступа к системе «Интернет-банкинг»
× Сообщать данные, полученные в виде SMS-сообщений, сеансовые пароли, код авторизации, пароль 3-D Secure и т.д.