

ЗАЧАРОВАННЫЙ МИР, ИЛИ КАК ОБОЙТИ ЛОВУШКИ ИНТЕРНЕТА

*Методические рекомендации
по организации и проведению
познавательно-игрового квеза в библиотеке*



Ульяновск
2018

ОТ СОСТАВИТЕЛЕЙ

Влияние Интернета на подрастающее цифровое поколение всё усиливается: по данным социологических исследований, годовой прирост интернет-аудитории – минимум 16%. 89% детей являются активными пользователями Интернета, 7-10% юных пользователей имеют риск стать интернет-зависимыми, каждый второй ребенок пользуется мобильным интернетом. Современные подростки считают себя «продвинутыми пользователями» Интернета, но эта уверенность зачастую носит иллюзорный характер. Высокий уровень онлайн-активности, недостаточная компетентность и чрезмерная самоуверенность являются основными причинами столкновения детей с различными проблемами в Сети. Запретить Интернет мы не можем, но научить стратегиям технологической и психологической защиты, сформировать навыки и мотивации по использованию безопасного позитивного контента необходимо. Главная задача взрослых – помочь детям ориентироваться в новом цифровом пространстве, научиться быстро реагировать на те или иные проблемы, возникающие в Сети, правильно анализировать ту или иную ситуацию.



Все мы прекрасно знаем, что личный опыт – лучший учитель. И многие правила и установки запоминаются детьми именно в игре. В игре развивается понятийное мышление, во-

Зачарованный мир, или как обойти ловушки Интернета

: Методические рекомендации по организации и проведению познавательно-игрового квеста в библиотеке / сост. Т. И. Гаянова, Н. Н. Легченкова ; Ульяновская областная библиотека для детей и юношества имени С. Т. Аксакова. – Ульяновск, 2018. – 48 с.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

ображение, способность к прогнозированию результата действия, проектные качества мышления, ведущие к реактому повышению творческих способностей детей, поэтому важно дать возможность ребѣнку поучиться на собственном опыте, в игровой форме приобрести устойчивые знания и умения в области корректного и безопасного использования компьютерных технологий, ресурсов и различных приложений Интернета.

В предлагаемом познавательном квесте смоделированы технологические и коммуникационные риски и угрозы, проблемные ситуации, с которыми подростки сталкиваются в Интернете, предложены решения выхода из них. В ходе игры участники квеста осваивают ответственное и безопасное поведение в Сети, вместе с библиотекарями научатся адекватно выстраивать собственную интернет-безопасность, повысят свой уровень знаний в плане безопасного использования информационных ресурсов Интернета. Квест-игра поможет решить имеющиеся проблемы, вовремя распознать негативные моменты и выносить из них положительные уроки.

Пособие состоит из методических рекомендаций по организации квеста, сценария квеста, списка использованной литературы. В приложенных содержатся дополнительные материалы в помощь проведению квеста и бесед с читателями.

Материалы для квеста можно использовать целиком или частично – при проведении отдельных занятий по формированию основ информационной безопасности у детей. Используйте данные рекомендации, вы можете привнести что-то своё, придумать другие задания и формы проведения квеста.

Пособие предназначено для руководителей детского чтения: библиотечарей, педагогов и воспитателей.

РАБОТА С АУДИТОРИЕЙ

1. В первую очередь необходимо обратить внимание на возраст подростков. В зависимости от этого нужно выбрать уровень сложности заданий и манеру обращения к подросткам. В психическом развитии подросток 10 лет и подросток 14 лет заметно отличается.
2. Необходимо вести равномерный диалог со всеми детьми, дать возможность участвовать каждому.
3. Лучше, если участники квеста будут разделены на команды (2-3), чтобы был соревновательный момент.
4. Важно уметь установить контакт глаз с аудиторией, чтобы каждый чувствовал, что на него обращают внимание, а также быть внимательным к тому, что говорят дети: откликаться на их высказывания, следить за их реакцией на ваши слова.
5. Перед началом квеста можно задать участникам несколько вопросов о том, как часто они пользуются Интернетом, какие страницы посещают, в каких социальных сетях бываюут, с какими рисками и угрозами сталкивались в сети.
6. Продумать, какой приз можно дать в конце игры. Детям интересно участие, но реальное вознаграждение будет больше стимулировать и оставит приятные впечатления.
7. Быть готовым к различным вопросам, уметь давать интересующую информацию со знанием дела. Быть авторитетным в теме, о которой говорите.

ОФОРМЛЕНИЕ ВНУТРИБИБЛИОТЕЧНОГО ПРОСТРАНСТВА

(зон, интерактивных познавательных площадок, где будут даны задания, развёрнуто определенное действие)

1. Провести подготовительный этап квеста: заготовить и вырезать вопросы, карты-маршруты, ключи, стрелки, следы, тайный сундучок с заданием, «листочки-послания», исходя из темы задания, подготовить видеоролики, слайды презентации и др.
2. Продумать, где будут располагаться площадки квеста (уровни, зоны) в библиотеке. Если места мало, то всё равно постараться выделить разные зоны. Главное, чтобы дети не сидели, им нужно действовать, двигаться, бегать, искать.



3. Оформить площадь квеста. Можно использовать компьютерную символику, распечатанную на листочках и развешенную на полках, разные объекты: часы (будильники, наручные, настенные часы) на уровне «Украденное время»; нарисовать или соорудить паутину на уровне «Побег из паутины», разложить на столах толстые папки с документами на уровне «Секретные материалы» и т.д.

4. Напечатать яркие названия площадок квеста.

5. Если вы собираетесь показать какой-то ролик или презентацию с вопросами, необходимо установить оборудование: ноутбук или ПК и мультимедиа-проектор.

ЭТАПЫ ПРЕДВАРИТЕЛЬНОЙ ПОДГОТОВКИ:

* Перед стартом мероприятия аудиторию необходимо познакомить с правилами игры:

* Участники мероприятия делются на несколько команд, им выдаются карты-маршруты (см. Приложение 1). Выполнять задания ребята могут индивидуально или в команде (микрогруппе).

* Игра состоит из 6-ти площадок. На каждой разбираются опасные ситуации, которые могут возникнуть при использовании Интернета, даются задания. В зависимости от того, насколько быстро и правильно команда выполняет задания, она получает от 1 до 3 ключей на каждой площадке. (Ключи могут быть выполнены из картона. Приложение 2).

* Побеждает команда, набравшая большее количество ключей в течение всей игры. Вместо КЛЮЧЕЙ можно вручать заранее подготовленные «листочки-послания из виртуального мира» с правилами поведения в Интернете. Первая буква «посланий» СЛОВО – КОД, которое будет пропущено в задании для подведения итогов квеста или в компьютерный зал, где можно предложить участникам квеста бесплатное web-путешествие по каталогу «Вебландия». Или, кто первый правильно соберёт кодовое слово из набранного количества «листочков-посланий», тот получает приз или медаль победителя. Можно взять какой-то символ, картинку и сделать из неё пазлы. Во время прохождения площадок квеста за каждое правильное выполненное задание выдается пазл. В конце участники квеста должны сложить из фрагментов пазлов символическую картинку.



* Каждая микрогруппа или команда должна ответить на главный вопрос квеста: в чём проявляются опасности сети Интернет и как их можно избежать и им противостоять. В завершение ещё раз проговорить золотые правила поведения в Интернете, сделав акцент на том, что Интернет необходимо использовать ответственно и вести на его просторах так, чтобы он был верным помощником и другом.

СЦЕНАРИЙ КВЕСТА

Дорогие ребята и уважаемые взрослые!

Сегодня, в преддверии Международного дня безопасного Интернета, а он отмечается ежегодно 10 февраля, стартует на территории всей Российской Федерации Неделя безопасного Рунета, которая проводится в более 60 регионах нашей страны с 2008 года по инициативе Центра безопасного интернета РОЦИТ, и фонда «Не Допустим!» и Российской государственной детской библиотеки. Каждый год Неделя безопасного Рунета стартует во второй вторник февраля во всех муниципалитетских образованиях Ульяновской области под лозунгом «Безопасный Интернет – хороший Интернет». В Ульяновской библиотеке для детей и юношества имени С.Т. Аксакова, которая является координатором проведения Недели безопасного Рунета в регионе, такие мероприятия проводятся с 2010 года!

Мы живём в новом информационном обществе, практически каждый день нашей жизни связан с телевидением, радио, газетами и журналами и, особенно, Интернетом и информация играет большую роль в жизни каждого человека, влияя на экономическую, общественную жизнь людей.

За последние 20 лет существования нового информационного пространства – Интернета – и при его активном использовании для образования, развития, проведения досуга, так и возникло немало новых угроз. Мы можем столкнуться с недоброжелательной информацией, агрессивной и просто опасной, которая может принести вред физическому, психическому и нравственному здоровью и интеллектуальному развитию, поэтому надо знать технологии защиты и противостояния различным угрозам и опасностям Интернета. Безусловно, часами находясь в Интернете, мы всё чаще задаёмся вопросом, возможно ли представить себе сегодняшний мир без Интернета? Как испол-



зывать с пользой для себя его возможности, диктует ли новое информационное пространство правила общения на его просторах?

Сегодня в ходе познавательного-игрового квеста «Зачарованный мир, или как обойти ловушки Интернета», пройдя по загадочным и познавательным площадкам библиотеки, вы познакомитесь с правилами поведения в Интернете, узнаете о том, как использовать различные приложения, избежать вредной и опасной информации, обезопасить свой компьютер от вирусов и спам-атак, противостоять давлению Интернет-троллей в социальных сетях.

ПРАВИЛА КВЕСТА:

Ребята, давайте мы поделимся на команды. Каждая команда получает карту-маршрут. Площадки квеста расположены в различных залах (местах) библиотеки, порядок их посещения указан на карте-маршрутах. На каждой площадке разбираются «ловушки и угрозы Интернета» – опасная информация, которая может навредить вам. Сообщается полезная информация, которая даст вам толчок к принятию верного решения при использовании Всемирной паутины и её различных приложений, научит избегать технологических и коммуникационных рисков. Внимательно читайте или слушайте задание, не торопитесь. Используйте имеющийся базис знаний, по пути выполняйте задания вы можете использовать энциклопедию, справочники, книги, которые будут выставлены на каждой площадке маршрута, ресурсы Интернета, выходить в Интернет со своих готовых телефонов, проговаривая или сообщая, каким проверенным источником вы воспользовались, или сообщите об этом координатору игры в конце состязания.

1 площадка. Секретные материалы The X-Files.

2 площадка. Украденное время.

3 площадка. Побег из Паутины.

4 площадка. Виртуальные помощники, или программы, атакующие вирусы или – «Агенты 007 – Борцы с вирусами».

5 площадка. «Великие и независимые. Узнайте их...».

6 площадка. В лабиринтах обмана (мошенничество).

Ведущий: Ваша задача: пройти испытания на всех площадках, выполнить предложенные на них задания, получить КЛЮ-

ЧИ за правильные ответы. В зависимости от того, насколько быстро и правильно вы выполнили задания, вы получаете от 1 до 3 ключей на каждой площадке.

Выдаются карты-маршруты.

(Пример: см. Приложение №1)

1 ПЛОЩАДКА

СЕКРЕТНЫЕ МАТЕРИАЛЫ THE X-FILES

(ненужная, ложная информация, реклама,

спам, поиск полезной информации)

Ведущий: Ребята, вы находитесь на площадке, на которой опасность (ловушку) представляет ненужная, ложная информация, реклама, спам.

Спам – это рассылка сообщений и рекламных материалов. Пользователи интернета всегда ищут способы заблокировать навязчивую рекламу, чтобы она не мешала восприятию информации и сёрфингу по страницам сайта.

Как убрать спам в почте. Для того, чтобы не получать спам на почту в виде писем, достаточно отметить письмо, нажимая кнопку «Спам». После этого все письма нежелательного почтового ящика будут гарантированно попадать в папку «Спам», содержимое которой необходимо иногда удалять. Если вы вообще не хотите ничего получать с определенного адреса, можно воспользоваться функцией черного списка. Это не позволит присылать вам с данного почтового адреса письма, содержащие спам.

Навязчивую рекламу убрать сложнее. Но у каждого браузера имеется свой функционал блокировки всплывающих окон рекламы. Весь этот функционал идет по умолчанию, и при блокировке окна отображается значок в строке браузера, нажав на который, можно выполнить действия с всплывающим окном.

Как часто вы используете Интернет? Для каких целей? (дети отвечают: соцсети, новости, игры, для учёбы). Всегда ли вам удается найти ту информацию, которая была необходима? Бывает ли такое, что вы забываете о том, что искали, переходя по многочисленным ссылкам? Всегда вы уверены в достоверности информации, которую находите в Интернете? (да, нет)



Как же правильно найти информацию?

Задание:

Перед вами – «секретные материалы». Здесь зашифрованы интернет-слова, ваша задача – найти их и объяснить значение каждого слова. А на помощь вам придут словари, энциклопедии, Яндекс-словари, Википедия (ru.wikipedia.org), словари и энциклопедии на Академике (<https://dic.academich.com/>), крупнейший энциклопедический ресурс Интернета-Рубрикон (<http://www.rubricon.com/>).

ШВГАРМИБРАУЗЕРИРООБТРОВИРУСМЛПТЬБТПДАМЕ-
МОДЕРАТОРУКАПНРГОЛДНИКЕНИТГАУКЕПОНЛАННИРНС-
ВАКЕПРИСМАЙЛЭТОРНГАРМНЕНШССЫЛКАОЛГНРГПШЬТЕК-
ТЕГИЦЫЧЕНРИМАФОРУМБЛОДЛОГИНКНЕКРДШПОАВАТАР-
ПРИМКЕНГШФИШИНГ НГШЕАОДРАЙВЕРСПРЕЕНРТШАЦЫ
ИНТЕРФЕЙС УКАСТОЛШКОНТЕНТРПОРЕЦДЖБЬЮЖД ХАКЕР-
НРЧЧИТЛГ ЧАТКГОЛТИПАККВУЫ ЮЗЕРКАПРИНОЛИТ *

Ответы:

ШВГАРМИБРАУЗЕРИРООБТРОВИРУСМЛПТЬБТПДАМЕ-
МОДЕРАТОРУКАПНРГОЛДНИКЕНИТГАУКЕПОНЛАННИРНС-
ВАКЕПРИСМАЙЛЭТОРНГАРМНЕНШССЫЛКАОЛГНРГПШЬТЕК-
ТЕГИЦЫЧЕНРИМАФОРУМБЛОДЛОГИНКНЕКРДШПОАВАТАР-
ПРИМКЕНГШФИШИНГНГШЕАОДРАЙВЕРСПРЕЕНРТШАЦЫ
ИНТЕРФЕЙС УКАСТОЛШКОНТЕНТРПОРЕЦДЖБЬЮЖД ХАКЕР-
НРЧЧИТЛГ ЧАТКГОЛТИПАККВУЫ ЮЗЕРКАПРИНОЛИТ

10-12 лет

1. интернет
2. онлайн
3. смайлик
4. ссылка
5. вирус
6. логин
7. аватар
8. чат
9. форум
10. хакер

13-16 лет

1. модератор
2. логин
3. тег
4. форум
5. фишинг
6. интерфейс
7. контент
8. юзер
9. драйвер
10. браузер

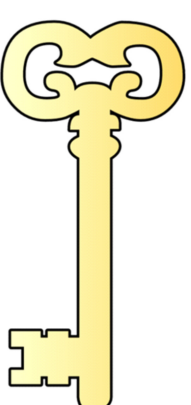
*Набор терминов может быть дополнен, исходя из имеющегося уровня знаний читателей и возрастной категории участников квеста.

Вы нашли значение этих слов, используя предложенные источники. Вы заглянули в Википедию – общедоступную многоязычную универсальную интернет-энциклопедию со свободным контентом, кто-то избрал печатный источник или словари на портале «Яндекс Словари». Как вы считаете, какие источники дают на 100% самую достоверную информацию? (дети размышляют и отвечают, сравнивают предлагаемую трактовку понятий из разных источников).

Запомните! Для того, чтобы факты были достоверными и максимально объективными, необходимо использовать правило «Трёх источников», т.е. информацию необходимо проверить не менее чем из трёх источников, не связанных друг с другом (как в разведке!).

Теперь вы знаете, как, где и в каких источниках можно найти достоверную информацию. Какая команда отметила больше слов, та и получает КЛЮЧ.

Молодцы, вот вам первый ключ (ключи)!



Ведущий: Молодцы! А выбратьсь из параллельного мира и получить ключ можно будет, только если вы скажете, как же избавиться от компьютерной зависимости. (Дети говорят: меньше сидеть за компьютером, больше читать, гулять, общаться со сверстниками, заниматься спортом, выполнять просьбы родителей и т.д.)

Если позволяет время, детям предлагается художественная литература, в которой литературные герои активно исполняют возможностям Интернета и уходят от действительности.

СПИСОК ЛИТЕРАТУРЫ, РЕКОМЕНДУЕМОЙ ДЕТЯМ ДЛЯ ЧТЕНИЯ:

1. Дзюба, О. В Интернете снега нет. – Москва : Астрель АСТ Транзиткнига, 2006. – 160с.
2. Жвалевский, А. Типа смотри короче / А. Жвалевский, Е. Пастернак. – Москва, 2014. – 254 с. – (Серия «Время – детство»).
3. Жвалевский, А. Время всегда хорошее / А. Жвалевский, Е. Пастернак. – Москва, 2014. – 256 с. : ил. – 7-е изд., стереотип. – (Серия «Время – детство!»).
4. Крюкова, Т. Призраки Сети / Т. Крюкова. – Москва : Аквилегия – М, 2007. – 400 с.
5. Лубенец, С. Одноклассники. Лучшие романтические истории / С. Лубенец. – Москва : Эксмо, 2011. – 352 с. – (Большая книга романов о любви для девочек). (Из этой книги представляется интерес повесть «Свидание на крыше» – о травле героини книги Веры Филимоновой на сайте «Лучшие друзья». Как разворачиваются события и кто смог помочь Вере в этой непростой ситуации – вы прочитаете в повести Светланы Лубенец «Свидание на крыше»).

3 ПЛОЩАДКА ПОБЕГ ИЗ ПАУТИНЫ

С помощью верёвки создаётся импровизированная паутина (ставятся стулья и вокруг ножек крест-накрест протягиваются верёвки), на противоположных сторонах верёвки крепятся карточки с терминами, описывающими различные современные технологические понятия, связанные с использованием IT-технологий, различных приложений Интернета, программного обеспечения, технологическими рисками, проявлениями мошенничества и обмана во Всемирной паутине: с одной стороны крепятся названия терминов, с другой – объяснение этих понятий. Продвигаясь через паутину, необходимо правильно соотносить название термина с его определением.

Чат – (англ. chat – болтовня, беседа, разговор) – это обмен мгновенными сообщениями по компьютерной сети в режиме реального времени посредством специального программного обеспечения.

Хакер – (англ. tohack – разрубать) – квалифицированный взломщик компьютерных программ и сетей, специализирующийся на поиске и использовании их уязвимостей с целью получения секретной информации, извлечения выгоды, создания нового нанесения ущерба владельцам программ, компьютерных сетей или Интернет-ресурсов. Изначально, хакерами называли программистов, которые исправляли ошибки в программном обеспечении каким-либо быстрым и далеко не всегда профессиональным способом; такие правки ассоциировались с «топорной работой» из-за их грубости, отсюда и произошло название «хакер».

Аватарка / юзерпик – (просторечн. ава, аватарка от англ. avatar) – публичное графическое представление пользователя, созданное самим пользователем.

Кибербуллинг – виртуальный террор получил свое название от англ. слова bill – бык, с родственными значениями: агрессивно нападать, бередить, задирать, придирается, провоцировать, донимать... Травля осуществляется в Интернете посредством электронной почты, программ для мгновенного обмена сообщениями (например, ICQ) в социальных сетях, а также через размещения на видеопорталах (например, YouTube) видеоматериалов, либо посредством мобильного телефона (на пример, с помощью SMS-сообщений или надоедливых звонков.



Лица, которые совершают данные хулиганские действия, часто называют «Булгли» или «Мобберы», действуют анонимно, жертва не знает от кого происходит агрессивные действия.

Флейминг – Флейм (flame) – словесная война на интернет-сайте, например, на форуме. В процессе бурного обсуждения участники заботятся о первоначальной тематике и переходят на личности, а порой и оскорбления. В большинстве случаев тема обсуждения из-за вышеуказанных причин до конца не раскрыта и полезную информацию из подобного общения получить трудно.

Фишинг – Технология Интернет-мошенничества, заключающаяся в краже личных конфиденциальных данных, таких как пароли доступа, данные банковских карт и основана на использовании спамерских рассылок или почтовых «червей». Потенциальным жертвам рассылаются подложные письма, от правленными якобы от имени легальных организаций. Текст письма предлагает зайти на сайт такого учреждения и подтвердить пароли, PIN-коды и другую личную информацию. По предположенным ссылкам пользователь вместо официального сайта попадает на сайт, подделанный преступниками. Собранная информация используется злоумышленниками для кражи денег со счетов жертвы и для совершения других преступлений.

Троллинг – форма социальной провокации или издевательства в сетевом общении, то есть сознательный обман, клевета, возбуждение ссор и раздоров, призыв к неблагоприятным действиям. Это вызывающее поведение, оскорбления и провокации в интернете, вид деятельности, призванный вывести кого-либо из себя или просто над кем-либо посмеяться.

Пост – статья в блоге или отдельное сообщение в форуме.

Спам – (англ. spam) – массовая рассылка коммерческой, политической и иной рекламы или иного вида сообщений лицам, которые не давали согласие получать эту информацию.

Логин – имя учётной записи пользователя в любой форме. Указывается при регистрации почти на каждом сервисе и является необходимым условием для входа в свой аккаунт. Логин следует хранить в надёжном месте и не терять его.

Рунет – русскоязычная часть всемирной сети Интернет.

Более узкое определение гласит, что Рунет – это часть Всемирной паутины, принадлежащая к национальным доменам .su, .ru.

Яндекс – российская поисковая система, являющаяся



крупнейшим англоязычным поисковым сервером.

Браузер – или веб-обозреватель (англ. webbrowser, устар. браузер) – прикладное программное обеспечение для просмотра веб-страниц; содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями; а также для решения других задач. Браузеры распространяются, как правило, бесплатно. К примеру, браузеры InternetExplorer и MicrosoftEdge; MozillaFirefox; Safari; Google Chrome, Opera и другие браузеры – это самостоятельные приложения во множестве вариантов для различных операционных систем.

Кэш (англ. cache – тайник, запас) – массив сверхоперативной памяти компьютера, являющийся буфером между достаточно медленной системной памятью и процессором. В этом массиве хранятся данные, с которыми процессор работает в данный момент. При выключении питания компьютера эти данные не сохраняются. Кэширование – накопление данных в оперативной памяти для их быстрого извлечения по мере необходимости. Кэширование ускоряет процесс обработки информации.

Вирус – (компьютерный вирус) – вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загруженные секторы, а также распространять свои копии по разнообразным каналам связи.

Целью вируса является нарушение работы программно-аппаратных комплексов: удаление файлов, блокирование работы пользователя или же приведение в негодность аппаратных комплексов компьютера и др.

Файрвол – переводится термин (firewall) как «стена огня» или «огненная стена». Это компьютерная программа, обеспечивающая защиту компьютера пользователя при нахождении в сети интернет от несанкционированного доступа других пользователей сети к информации на компьютере, содержащейся на жёстком диске, во избежание хищения конфиденциальной информации и заражения компьютера вирусами.

Боты – (сокр. от робот). Специальная программа, выполняющая автоматически и/или по заданному расписанию какие-либо действия через те же интерфейсы, что и обычный пользователь. Программное обеспечение вредоносное, поражает компьютер и позволяет осуществлять скрытое удаленное управление им. Бот может выполнять без ведома владельца компь-



ютера такие действия как: похищение данных, распространение спама, доставку и установку вредоносного программного обеспечения и др.

Блог – (англ. blog, от weblog – интернет-журнал событий, онлайн-дневник) – веб-сайт, основное содержимое которого – регулярно добавляемые записи (посты), содержащие текст, изображения или мультимедиа. Для блогов характерны недлинные записи, отсортированные в обратном хронологическом порядке (последняя запись сверху). Отличие блогов от традиционных дневников в том, что блоги обычно публичны, то есть общедоступны. Читатели блога могут вступать в публичную полемику с автором (в комментариях к посту или своих блогах). Людей, ведущих блог, называют блоггерами. Совокупность всех блогов Сети принято называть блогосферой.

Форум – англ. forum – конференция, свободная дискуссия). В интернете под форумом чаще всего подразумевается веб-форум – класс веб-приложений для организации общения посетителей веб-сайта. Специально для общения людей (обычно по теме или темам ресурса) на сайте создаётся раздел, где посетители могут вести дискуссии, оставлять свои комментарии к уже существующим темам и начинать новые. Этот раздел тоже называется форумом, это своего рода клуб по интересам.

Кто дал наибольшее количество правильных ответов – не менее 5, получает КЛЮЧ (ключи).



ВТОРАЯ ЧАСТЬ ИГРОВОЙ ПОЗНАВАТЕЛЬНОЙ ПРОГРАММЫ

На стене прикрепляется диск для игры в дартс. Крул нумеруется от 1 до 5. Каждая цифра соответствует логотипу (изображению) известной антивирусной программы:

При попадании в кружок с обозначением цифры-программы (изображение антивируса), даётся краткая его характеристика: кто разработчик, особенности программы в борьбе с вирусами, троянами и др. рисками. Детям попутно задаются вопросы: Какие программы они знают и какие используют на своих домашних ПК, планшетах и сотовых телефонах? Как часто они сталкиваются различными технологическими рисками? Что это такое? Дети отвечают (компьютерные вирусы, у меня дома такой-то антивирус, а я знаю такой-то...).

Ведущий: Правильно, вредоносные программы (вирусы, черви, «троянские кони», шпионские программы, боты и др.) могут нанести вред вашему компьютеру и хранящимся на нем данным. Они также могут снизить скорость обмена данными и даже использовать ваш компьютер для распространения вируса, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.



4 ПЛОЩАДКА «ВИРТУАЛЬНЫЕ ПОМОЩНИКИ ИЛИ ПРОГРАММЫ, АТАКУЮЩИЕ ВИРУСЫ» ИЛИ «АГЕНТЫ 007 – БОРЦЫ С ВИРУСАМИ»

Будущий: Ребята, сейчас мы по очереди поиграем в любимую игру – в дартс. Вы должны попасть в кружки с обозначением известных антивирусных программ (выдаётся 6 дротиков). Играя, вы будете мне помогать давать характеристику этим программам, которые предотвращают столкновение с вредоносными программами и их проникновение в компьютер.

Описание изображений антивирусных программ, их краткая характеристика.

KASPERSKY



Первое изображение:

Антивирус Касперского

Антивирус Касперского (Kaspersky Antivirus, KAV) – антивирусное программное обеспечение, разработанное «Лабораторией Касперского». Первоначально, в начале 1990-х, оно носило имя – V, затем – AntiViralToolKitPro. «Лаборатория Касперского» – самый известный в России производитель систем защиты от вирусов, спама и хакерских атак, эта фирма работает на рынке систем безопасности более 10 лет. Антивирус Касперского является надежной и эффективной программой для борьбы с вредоносным программным обеспечением. Он предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, программ, содержащих рекламу (adware).

Антивирус Касперского выполняет следующие основные функции.

- Защита от вирусов и вредоносных программ.
- Постоянная защита компьютера – проверка всех запускаемых, открываемых и сохраняемых на компьютере объектов на присутствие вирусов.



- Проверка компьютера по требованию – проверка и лечение как всего компьютера в целом, так и отдельных дисков, файлов или каталогов.

• Восстановление системы и данных – наличие инструментов для создания аварийного восстановления.

- Проверка и лечение входящей/исходящей почты.

• Обновление вирусных баз и программных модулей – пополнение вирусных баз информацией о новых вирусах и способах лечения зараженных ими объектов, а также обновление собственных модулей программы.

• Карантин – помещение объектов, возможно зараженных вирусами или их модификациями, в специальное безопасное хранилище, где они не представляют опасности.

• Формирование отчета – фиксирование всех результатов работы антивируса в отчете. Однако надежная защита дается ценой очень высокой ресурсоемкости этого антивируса, поэтому если компьютер не отличается большой вычислительной мощностью, то использование данного антивируса будет значительно «тормозить» работу компьютера.

Второе изображение:

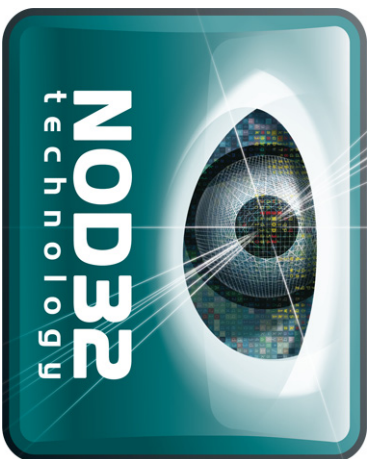
Антивирус Dr. Web



Антивирусное программное обеспечение, разработанное ООО «Санкт-Петербургская антивирусная лаборатория Данилова» (ООО «СалД»). Этот антивирус является вторым по известности в России.

Санкт-Петербургская антивирусная лаборатория Данилова основана в 1993 году. Антивирусы этого семейства предназначены для защиты от почтовых и сетевых червей, файловых вирусов, троянских программ, макровирусов, вирусов, поражающих документы MicrosoftOffice, шпионского ПО (spyware), программы-похитителей паролей, клавиатурных шпионов (то есть программы, записывающих нажатие клавиш клавиатуры), рекламного ПО (adware), программ-шуток, вредоносных скриптов и других вредоносных объектов, а также от спама.





Третье изображение:

Антивирус NOD32 – антивирусное программное обеспечение, разработанное словацкой компанией Eset. Первая версия была выпущена в конце 1987 года.

Название изначально расшифровывалось как (NemospisacaOkrajidisku) «Большница на краю диска».

Этот антивирус позволяет обеспечить сохранность информации и данных от проникновения вредоносных программ (троянских программ, червей, шпионского ПО, рекламного ПО, почтовых рекламных рассылок и т.д.) через Интернет и электронную почту, и защитить эти и другие данные от всех типов как известных, так и новых угроз. Этот антивирус является одним из лидеров среди антивирусного программного обеспечения.

Антивирус NOD32 на протяжении нескольких лет подряд по-прежнему при тестировании высокую эффективность находят при вирусав, отличается высокой скоростью работы, низким потреблением системных ресурсов, обладает всеми современными средствами защиты компьютера. Есть русская версия программы.



Четвертое изображение:

Антивирус Norton AntiVirus – одна из самых известных в мире антивирусных программ, которая производится американской компанией Symantec. Компания неоднократно занимала призовые места в крупнейших международных антивирусных тестах.

Основные характеристики

Norton AntiVirus:

- поиск и удаление вирусов и программ-шпионов;
- автоматическое блокирование программ-шпионов;
- блокирование рассылки зараженных писем;



- автоматическое распознавание и блокировка вирусов и троянских программ;
- обнаружение и устранение угроз, скрытых в операционной системе;
- защищает от интернет-червей;
- реализована функция просмотра электронной почты и мгновенных сообщений, программа находит и удаляет или блокирует зараженные вложения.



Пятое изображение: Ан-

тивирус Avast! – антивирусная программа для операционных систем Microsoft Windows и GNU/Linux, а также для КПК; разработанная чешской компанией ALWIL Software. В настоящее время Avast! является одним из лучших бесплатных антивирусов в мире, к тому же он специально разработан для использования на домашних компьютерах. Продукт потребляет минимальное количество ресурсов и практически не оказывает негативного влияния на скорость загрузки операционной системы и общую производительность компьютера. У него удобный и понятный интерфейс, который обеспечивает быстрый доступ ко всем параметрам программы.



Шестое изображение:

Avira AntiVir – это антивирусная программа, которая предоставляется бесплатно для домашнего использования. Программа умеет определять и удалять вирусы и троянские программы, в том числе и еще неизвестные макровирусы. Поддерживается ее автоматическое обновление через Интернет. В базе данных программы содержится информация более чем о 150 тыся-



чах вирусов и имеется возможность пополнения этой базы через Интернет.

Будущий данной площадке: Некоторые из вас сегодня были меткими стрелками, и эти ребята получают заслуженные КЛЮЧИ. Ребята, много узнав об особенностях этих программ, их функциях, какой можно сделать вывод? Вывод однозначен: Необходимо использовать только лицензионные программы и данные, полученные из надежных источников, покупать в проверенных магазинах. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.

* Периодически полностью проверять свои домашние компьютеры, обновлять имеющиеся антивирусные программы. Делать резервную копию важных данных.

* Всегда устанавливать на свои домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечения и порти данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, так и атаки, использующие вредоносные приложения.

Будьте внимательными во время работы со своими гаджетами и в Интернете, постоянно обновляйте свои антивирусные программы. 100 % защиты не бывает, но используйте все возможности.

5 ПЛОЩАДКА. «ВЕЛИКИЕ И НЕЗАВИСИМЫЕ. УЗНАЙТЕ ИХ...»

Друзья, если я спрошу каждого из вас, что вы делаете в свободное от учебы время, вы наверняка ответите, что большую часть своего времени вы проводите в Интернете: сидите в социальных сетях, смотрите фильмы и сериалы, ролики на YouTube, кто-то читает книги. Но есть люди, для которых компьютер и интернет – это не только способ получения информации и общения, но и область применения своих знаний, та площадка, где они смогли профессионально показать себя.

Перед вами лежат портреты самых известных людей планеты, подкажака, – все они являются выдающимися личностями в области IT-технологий и Интернета, вам нужно узнать, про кого сейчас **БУДУТ** зачитываться цитаты их высказываний и факты их биографий.

Зачитываются отрывки из личной и профессиональной жизни известных программистов, создателей социальных сетей и программ-браузеров, разработчиков новых гаджетов.

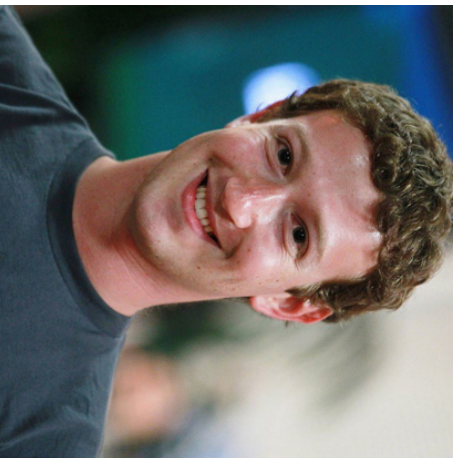
Лежат распечатанные портреты П. Дурова, Ст. Джобса, Б. Гейтса, М. Цукерберга, С. Брин, А.Ю. Волож.

1. «Будучи студентом, он разрабатывал и внедрил несколько интернет-проектов для научной и общественной жизни студентов. Они имели некоторый успех и собрали сравнительно небольшую студенческую аудиторию. Но то, что студенты на форуме общаются не под настоящими именами, а под никами и придуманными аватарами, ему не понравилось. Он решил найти иную форму сайта для общения. В это время из штатов вернулся один его приятель, который рассказал о сети Facebook. Наш герой тут же уцепился за эту идею и немедленно приступил к созданию подобного сайта для российской аудитории. Социальная сеть начала свое существование 1 октября



2006 года. Первоначально на сайте была закрытая регистрация, но уже через несколько месяцев он стал обладать свободным доступом, на сегодняшний день это соц. сеть является самой популярной на территории России и стран СНГ.

Ответ: Павел Валерьевич Дуров – род. 10 октября 1984, Ленинград, СССР. Российский предприниматель, программист, рублёвый миллиардер... создатель социальной сети «ВКонтакте», один из создателей социальной сети «ВКонтакте» и одноимённой компании; создатель кроссплатформенного мессенджера «Telegram». Бывший генеральный директор ВКонтакте. В студенческие годы лауреат стипендий Президента РФ и Правительства РФ, трёхкратный лауреат Потанинской стипендии)



2. «В 9-м классе наш герой создал достаточно необычную программу. Она собирала данные о том, какую музыку слушает человек на своем компьютере, каким именно суток отдаёт предпочтение. А затем, на основании этих данных, создавала плейлист, проигрывая именно те мелодии, которые, возможно, выбрал бы в эту минуту сам меломан. Учась в Гарварде он тут же приобрел репутацию крутого хакера и программиста. Он умудрился взломать сервер с информационной базой и фотографиями всех студентов и устроил своеобразный конкурс красоты гарвардских девушек. После чего администрация едва не выгнала его из университета, но при этом все же отметила в своем заключении, что этот студент обладает исключительными способностями.

Об основании самой популярной в мире социальной сети ее создатель говорил: «Реальная история создания Facebook выглядела так: мы просто сидели шесть лет за компьютерами и занимались программированием».

Ответ: Марк Цукерберг – род. 14 мая 1984, Уайт-Плейнс, штат Нью-Йорк, США. Американский программист и предприниматель в области интернет-технологий, долларовый миллиардер, один из разработчиков и основателей социальной сети Facebook. Руководитель компании Facebook Inc.



3. «Сфера высоких технологий стала для него домом в буквальном смысле: ребенок рос в центре компьютерных инноваций, Силиконовой Долине. Забитые разнообразной электроникой гаражи и кладовки стали привычным делом в этом молодом районе. Такое окружение вселило в юного гения благоговейное отношение к технологиям и прогрессу. Возможно, именно этот восторг от соединения IT с повседневностью породило увлеченную дружбу между двумя учредителями одной из успешнейших корпораций современности. Созданная им компания начала свое восхождение в гараже у нашего героя... Главным делом жизни было создание компьютеров и программного обеспечения к ним. Созданная им линейка компьютеров – ...увидела свет в 1977 г. и стала революцией в мире компьютеров.



Но прославилась эта корпорация по большей части за счёт создания новой линейки смартфонов, планшетов и ноутбуков. Сейчас даже тяжело представить, что у истоков мирового компьютерного «монстра» ... стоял обычный парень, хиппи, из небольшого американского городка, без высшего образования, но с космическими амбициями и настоящим талантом видеть то, что понравится людям».

Ответ: (Стив Джобс) – 24 февраля 1955, Сан-Франциско, Калифорния – 5 октября 2011, Пало-Алто, Санта-Клара, Калифорния. Американский предприниматель, получивший широкое признание в качестве пионера эры IT-технологий. Один из основателей, председатель совета директоров и CEO корпорации Apple. Один из основателей и CEO киностудии Pixar. Создатель «яблочного» ноутбука. Он в одиночку смог сдвинуть с места не только компьютерную индустрию, породив Apple II и Macintosh, но и музыкальную, создав iPod, телефонную, благодаря iPhone, и мультипликационную вместе со смежными экспериментами студии Pixar.





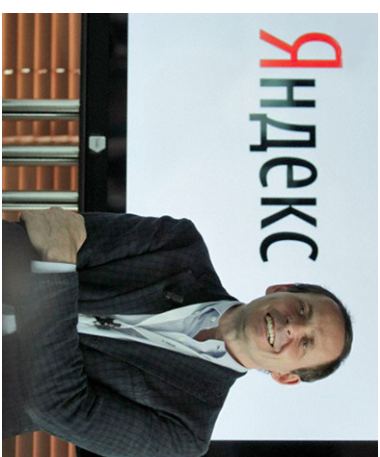
4. «Родители ожидали, что он пойдет по стопам отца и поступит в Гарвардскую школу права. Однако сын не преуспевал в грамматике, граждановедении и других предметах, которые он считал скучными, к седьмому классу он увлекся математикой и мечтал стать профессором. Одной из первых программ, которую написал герой был простенький симулятор, который позволял играть против машины. Ещё одним его проектом в школьные годы стала программа для составления расписания занятий.

Про себя 15-летнего он отзывался так: «Я был тем парнем, который сказал: «Давайте позвоним реальному миру и предложим продать ему что-нибудь». И самое интересное, что действительно нашёл и продавал – например, он разработал программу для оптимизации личного движения и продал ее за 20 000 долларов.

Этот человек – признанный отец промышленности программного компьютерного обеспечения, является олицетворением адлеровского портрета преуспевающей личности. «Ю-Эс-Эй Ту-Дей» пишет, что «...– это человек, который соревнуется даже в том, кто лучше устроит вечеринку, а в делах проявляет себя как решительный, боевой и безжалостный». Журнал «Инк» описывает его как «беспокойный сгусток энергии».

Сейчас он один из богатейших людей мира, компьютерный магнат, основатель компьютерной корпорации. Он вписал своё имя в мировую историю, независимо от того, что думают и говорят о нём современники.

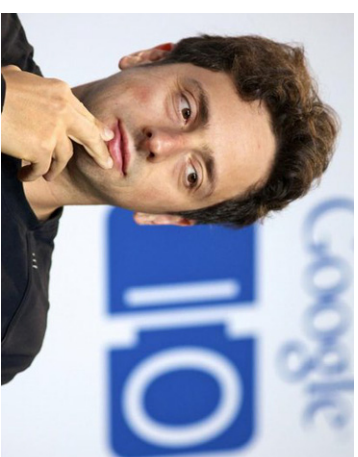
Ответ: Билл Гейтс – 28 октября 1955 г. (62 года), Сياتл, США. Американский предприниматель и общественный деятель, филантроп, один из создателей и бывший крупнейший акционер компании Microsoft. До июня 2008 года являлся руководителем компании, после ухода с поста остался в должности её неисполнительного председателя совета директоров. Также является председателем благотворительного фонда Билла и Мелинды Гейтс, членом совета директоров Berkshire Hathaway, ген. директор CascadeInvestment



5. В 1986 году окончил Институт нефти и газа им. И. М. Губкина по специальности «прикладная математика». В 1999 году он был одним из тех, кто повлиял на судьбу легализации IP-телефонии в России. В 1997 году он сделал первый шаг по созданию компании – на 10 тыс. долларов были закуплены 3 сервера с жёсткими дисками ёмкостью в 1 Гб, на которые было проиндексировано всё содержимое Рунета. Итогом этих инвестиций стало попадание программы в семёрку наиболее популярных сайтов русскоязычного сегмента Интернета в 1999 году.

В марте 2013 года попал в рейтинг миллиардеров, ежегодно составляемый журналом «Forbes», его личное состояние было оценено в \$1,15 млрд.

Ответ: Аркадий Юрьевич Волож – родился 11 февраля 1964 г. в городе Гурьев Казахской ССР (ныне Атырау). Сооснователь и генеральный директор компании «Яндекс».



6. Этот человек – легенда компьютерного бизнеса, сооснователь и президент по технологии самого большого поискового сервера в мире, миллиардер, ныне один из самых богатых людей Америки. Он – русский, впервые названный газетой «Financial Times» «человеком года» не как актёр, политик или олигарх, а как математик, прославившийся на весь мир творением собственного ума.

«Когда мы заглядывали в интернет, мы не читали там гороскопы и не заходили на сайты знакомств. Нас интересовал поиск – та информация, которая по-настоящему влияет на жизнь людей», – вспоминает наш герой.

Ответ: Сергей Брин – 21 августа 1973, Москва, СССР), Аме-

риканский предприниматель и учёный в области вычислительной техники, информационных технологий и экономики, миллиардер - разработчик и основатель поисковой системы Google. Проживает в городе Лос-Альтоc.

Кто ответил на большее количество вопросов, получает КЛЮЧ (ключи).

6 ПЛОЩАДКА В ЛАБИРИНТАХ ОБМАНА (мошенничество)

Ребята, вы находитесь в библиотеке – огромном информационном пространстве. Здесь вы видите на полках очень много литературы на самые разные темы. А Интернет – это необъятное информационное пространство. Чтобы не заблудиться в нём, нужно обладать элементарной информационной грамотностью. Потому что, на каждом шагу в глобальной сети поджидают мошенники. Вариантов мошеннических схем очень много. Обманщики иногда подходят к этому вопросу с такой выдумкой и виртуозностью, что даже опытейшие пользователи интернета легко попадают на крючок. От этого не застрахован никто.

Интернетом вы пользуетесь и в компьютере, и в своем телефоне. Давайте представим, что мы перемещаемся в Интернет-пространстве и встречаем на пути различные опасности. Попытаемся разобраться, какие виды мошенничества существуют, и как избежать этих опасностей.

Задание:

В этом зале спрятаны листочки, на которых написаны виды мошенничества и правила, как этого избежать. Вам нужно собрать их и определить – действительно ли это мошенническая схема, или всё в порядке и опасности нет. Но собрать их не легко, во-первых – они рассредоточены в разных местах, следы подсказки вам помогут. Собрать нужно ровно 9 штук (можно меньше). Листки спрятать на стеллажах, под крышку принтера, на ветках растения, между книгами... Около этого места на полу можно разместить стрелки-указатели. Можно размес-

тить стрелки, которые сбивают с пути (на них написать обычные слова, например небо, дерево, и т.д.) А на правильных стрелках написать компьютерные слова (сайт, Интернет, Яндекс, мышка).

На экране появляется окно с надписью «Посмотри, как ты будешь выглядеть с новой прической» И дана ссылка на сайт. Будешь ты переходить по этой ссылке?

Дети отвечают. Они должны порассуждать, выдвинуть свои предположения, только затем услышать ответ.

Ответ: (зачитывает или рассказывает библиотекарь).

Любопытный пользователь по ссылке переходит на сторонний сайт, где ему предлагается ответить на несколько вопросов, о манере питания и образе жизни, если речь идет о себе похудеть; либо о дате рождения и имени, если интересуется гороскоп; загрузить фотографию для моделирования причёски и пр.

Развитие дальнейших событий возможно по одному из двух сценариев.

1. Пользователю предлагают ввести номер своего мобильного телефона на сайте и ответить на пришедшее смс для подтверждения, что он человек, а не вредоносная программа. При ответе на смс со счета мобильного телефона снимается сумма в 200-300 рублей. Как правило, на сайте, если хорошо поискать, можно найти информацию о том, что услуга является платной, но это либо тщательно прячется, либо указано в длинном письме пользователю с согласием, написанном мелким шрифтом, которое, как правило, никто не читает.

2. Пользователю так же предлагают авторизоваться с помощью мобильного, и оказывается, что совершив данные манипуляции, он соглашается на платную подписку. Суммы обычно незначительны – 5-10 рублей в день, но списываются ежедневно, что в конечном итоге может вылиться в несколько тысяч рублей, списанных со счета мобильного, прежде чем подписка будет обнаружена и аннулирована пользователем.



Вы играете в компьютерную игру. И вдруг появляется сбоку окно с надписью «Получи секретный код и огладей супермощным оружием» и т.п.). Как вы действуете, если проити по ссылке и скачать секретный код для игры, это опасно? Или нет ничего страшного?

Ответ: О том, что услуга платная, чаще всего не написано. Далее уже известная схема: авторизация на сайте, ввод номера мобильного телефона и ответ на смс либо ввод кода, полученного на сайте. Денги списываются, а ни статусов, ни нового оружия нет.

Вам предлагают установить шпионскую программу, которая позволяет следить за всеми людьми в Интернете. Вы скачаете такую программу себе?

Ответ: Как правило, это не предусмотрено основными функциями социальной сети. Далее при помощи смс либо путем кражи логина-пароля и доступа к кредитной карте мошенники лишают пользователя денежных средств.

На электронную почту или на ваш телефон пришло сообщение: Вы выиграли 100 тысяч в лотерею!!! Компьютер случайным образом выбрал ваш телефон! Позвоните SMS на номер 8929XXXXXXX, чтобы подтвердить выигрыш!

Ответ: Если Вам прислали письмо о выигрыше, это повод насторожиться. Если вы в лотерею не участвовали осознанно — не нужно и надеяться, что это правда. Вы должны усвоить важное правило: никогда не вводить номер своего мобильного, не обсуждая это с родителем.

В Интернете появилось объявление от благотворительной организации, детского дома, приюта с просьбой о материальной помощи большим детям или бездомным животным? Вы можете им? Переведете им деньги?

Ответ: Конечно, нужно помогать людям, и это очень похвально. Но не нужно и забывать, что злоумышленники часто создают сайт-дублер, который является точной копией настоящего, меняют реквизиты для перечисления денег. Поэтому, обязательно проверьте всю информацию, посмотрите и сравните разные сайты, а лучше — посоветуйтесь с родителями.

На мобильный телефон приходит сообщение: «Вам пришла открытка от друга». Для просмотра просьбы перейти по ссылке. Ваши действия?

Ответ: Если это сделать, активироваться злоумышленник в ссылке регистрации код для номера телефона пользователь. Таким образом, нажимая на ссылку, пользователь автоматически регистрируется на сайте с платной услугой и начинает получать всевозможный спам. Избежать такого мошенничества можно только, если не переходить по ссылке.

Вам в социальных сетях пришло сообщение от одноклассника или вашего друга с просьбой перечислить ему деньги на счёт и дан номер неизвестного сотового телефона, или с просьбой сообщить код, который пришёл вам на ваш сотовый. Иногда друг пишет много СМС-сообщений и говорит, что объяснит всё потом, так как сейчас срочно нужны деньги. Что будете делать?

Ответ: Страницу в соц.сетях могут взломать злоумышленники, и от имени одноклассника слать вам сообщения. Такие сообщения могут приходиться вам на телефон с незнакомого номера. Вам не стоит торопиться отсылать деньги. Лучше перезвоните ему на прежний номер и выясните, всё ли правда, или это обман.

Вы добавили нового друга (подружку) в социальных сетях, и долго уже с ним общаетесь. Наконец, он предлагает вам встретиться и погулять где-нибудь. Что вы будете делать?

Ответ: Человек в интернете может представляться кем угодно, но это не значит, что он таким и является. Если с тобой общается, к примеру, голливудский актёр или великий футболист

— скорее всего, тебя обманывают. Даже девочка Маша, которую вы никогда не видели, может оказаться совсем не девочкой, и не Машей. Это всё равно незнакомый человек, о котором вы ничего не знаете, и он может оказаться не просто мошенником, а гораздо хуже.

Общаясь с незнакомцами, не будь слишком открытым. Искренность хороша лишь с близкими друзьями. Не рассказывай, где и в каких условиях ты живёшь, в какую школу ходишь, какой твой распорядок дня. Не рассказывай ничего того, чего можешь потом стесняться или о чём ты бы не хотел, чтоб узнали все.

Насторожься, если новый знакомый задаёт вопросы с финансовым подтекстом: сколько стоит ваш автомобиль? Где работают родители? В какие магазины вы ходите? Когда папа приносит зарплату? Никогда не отвечай на такие вопросы и не рассказывай никому подробности вашего семейного бюджета.

Если новый знакомый сразу после знакомства предлагает прислать тебе какой-то файл (игру, книгу, интересный видеоролик) — не принимай его и ни в коем случае не открывай. Возможно, таким образом, тебе хотят подбросить компьютерный вирус.

Также с осторожностью относись к ссылкам, присланным незнакомцами. Не переходи на другие сайты, если не уверен точно, что знаешь, куда тебя приглашают.

Если виртуальный знакомый предлагает тебе встречу — обязательно сообщи об этом родителям. Пусть они проведут тебя и заодно тоже познакомятся с твоим новым другом.

Не принимай на веру всё, что пишут незнакомые тебе люди. Даже если они напишут, что твоя мама сидит у них в гостях и просит тебя прийти — не верь и для начала сам поезди к маме или папе. Что бы тебе ни рассказывали, если информация тебя заставляет удивлять или предполагает какие-то действия с твоёй стороны — сначала перепроверь.

Если незнакомый человек просит тебя прислать свою фотографию, или фотографию своего дома, комнаты, родительской машины — в общем, чего-то личного, что касается только тебя и твоей семьи — не присылай ничего.

Не рассказывай незнакомцам о своих планах на будущее — о ближайших поездках, покупках, мероприятиях.

Если общение с новым человеком тебе неприятно, но ты не можешь его прекратить — сообщи родителям и попроси помощи. Иногда без вмешательства взрослых просто не справиться.

После того как листки с видами мошенничеств собраны, команде выдаются КЛЮЧИ (ключи).

Ведущий: Молодцы, ребята. Теперь вы знаете, какие виды мошеннических схем существуют в Интернете, и как избежать этих ловушек. Держите честно заработанные ключи.

Дети собираются в том месте, откуда был дан старт квесту. После того, как дети собрали ключи на всех площадках, каждая команда подсчитывает своё количество ключей; определяется, кто заработал больше ключей. Та команда, которая набрала самое большее количество ключей, получает специальный приз (книгу, закладки, приглашение на выставку новых технологий и др.) или медаль победителя (сделанную своими руками). Делается фото на память.

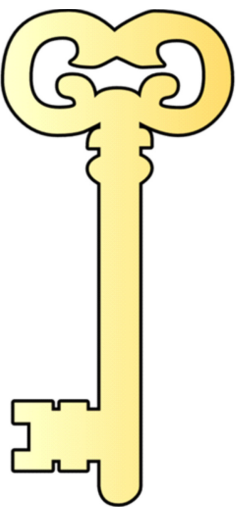
Заранее можно распечатать Памятки по правилам поведения на просторах Интернета, сделать закладки и вручить участникам квеста.

Приложение 1.

ПРИМЕР КАРТЫ-МАРШРУТА



Приложение 2.



Приложение 3.

ПОСЛАНИЯ

✉ Установи в поисковой системе функцию «безопасный режим». Она помогает не наткнуться на опасный сайт при поиске полезной информации. Но никакой фальшивке не идеален. Если ты случайно попал на нехороший сайт, не вини себя. Просто уходи оттуда

✉ Не всё, что написано в Интернете, правда. При поиске необходимых сведений используй прайво: найди информацию на трёх разных качественных сайтах и сверни. Если данные совпадают и указан источник получения информации, то её почти наверняка можно использовать. Информа-

ции на сайтах, созданных школами, институтами, библиотеками или учеными, обычно можно доверять. Но лучше проверить её в энциклопедиях.

✉ Не рассказывай собеседнику в сети о себе и не посылай свои фотографии. Собеседник в интернете невидим. Он может выдать себя за кого угодно, родственника или знакомого, выманивать личные сведения: телефон, адрес, пароли от почты или даже номер банковского счёта родителей и воспользоваться этой информацией во вред!

✉ Не проводи в Интернете слишком много времени. Ведь общение в сети будет тем увлекательнее, чем насыщенная реальная, офлайн жизнь!

✉ Не верь заглавным сообщениям, приходищим тебе в социальных сетях и на электронную почту.

✉ Не груби никому в Интернете и прекращай общение, если грубить начинаю тебе. Многие люди забывают, что чинить оскорбительные слова не менее обидно, чем их слышать, выходя в сеть. Не забывай, что вежливым нужно быть всегда, и за экраном компьютера тоже.

✉ Проверь скачиваемые файлы специальной программой – антивирусом. В Интернете можно заразить компьютер ви-

русом. Чтобы этого не случилось, сохраняй на компьютер только лицензионную информацию. Не скачивай и не открывай файлы, которые прислали незнакомцы.

✉ Встречаясь с Интернетом - знакоми только с родственниками или взрослыми друзьями! Обязательно строгие разрешение на встречу у старших.

✉ Не вводи свой номер телефона, адрес и другие данные! В Интернете распространены случаи мошенничества, вымогательства денег. Часть Интернет магазинов – фальшивые. Поэтому покупки в них можно совершать только вместе со старшими. Многие сайты, на которых предлагаются скачать музыку, фильмы или другие файлы, просят ввести номер телефона или отправить СМС.

ПОЛЕЗНЫЕ ССЫЛКИ, КОТОРЫЕ МОЖНО РЕКОМЕНДОВАТЬ ДЕТЯМ ПОСЛЕ КВЕСТА, ОФОРМИВ ЗАКЛАДКИ, РЕКЛАМНЫЕ ПАМЯТКИ

ОНЛАЙН-ИГРА «ИЗУЧИ ИНТЕРНЕТ – УПРАВЛЯЙ ИМ»

Онлайн-игра «Изучи Интернет – управляй им» поможет юным пользователям Сети научиться ориентироваться в Интернет-пространстве. Участники игры узнают о техническом устройстве Сети, ее разнообразных сервисах и возможностях. В игре также рассказывается об основных угрозах, которые подстерегают пользователей Интернета, и о том, как избежать этих рисков. Игра создана при поддержке Координационного центра национального домена сети Интернет.

СМЕШАРИКИ

Смешарики – популярный мультипликационный сериал, созданный в 2003 г. в рамках Федеральной целевой программы по Толерантности и общественной социально-культурной программы «Мир без насилия». Смешарики – это круглые мультипликационные персонажи, каждый из которых имеет свой характер, историю и увлечения. Проект рассчитан на совокупную детскую аудиторию от трех до 15 лет. В рамках проекта действует комплексный развивающий детский портал www.smeshariki.ru, который представляет собой цельную игровую развивающую среду. Детская социальная сеть Смешариков – Шарарам представляет собой интерактивное образовательное пространство, где дети могут общаться друг с другом и получать полезные навыки, в том числе и в части правил безопасности в Интернете.

ТВИДИ

Твиди – Интернет-портал для детей и подростков 6-16 лет. На сайте зарегистрировано более 1,5 млн пользователей. Для них разработаны онлайн-игры, виртуальные миры, форумы, конструктор комиксов, новости, чаты, социальная сеть, онлайн-кинотеатр, сервисы хранения фото-, видео- и аудиофайлов. Портал содержит советы и рекомендации по безопасному использованию Интернета.



ГОРЯЧИЕ ЛИНИИ И СЛУЖБЫ ПОДДЕРЖКИ ПО ВОПРОСАМ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

ЛИНИЯ ПОМОЩИ «ДЕТИ ОНЛАЙН»

Линия помощи «Дети Онлайн» – служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования Интернета и мобильной связи. На Линии помощи профессиональную психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М.В. Ломоносова и Фонда Развития Интернет.

Звонки по России бесплатны. Линия работает с 9 до 18 (по московскому времени) по рабочим дням. Тел.: 8 800 25 000 15, email: helpline@detionline.com

ГОРЯЧАЯ ЛИНИЯ ЦЕНТРА ДЕТСКОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННОМ ОБЩЕСТВЕ «НЕ ДОПУСТИ!»

Горячая линия Центра детской безопасности в информационном обществе «Не Допустит!» позволяет любому пользователю сообщить о противоправном контенте в Сети. Аналитики «Горячей линии» осуществляют проверку всех сообщений и передают информацию хостинг- или контент-провайдеру (в ряде случаев – регистратору домена) с целью прекращения оборота противоправного контента, а также в установленных случаях – в правоохранительные органы. Линия работает по следующим основным категориям: сексуальная эксплуатация детей (детская порнография); деятельность преступников по завлечению жертв в Интернете (grooming); разжигание расовой, национальной и религиозной розни; пропаганда и публичное оправдание терроризма; киберунижение и киберпреследование; пропаганда наркотиков и их реализация через Интернет; интернет-мошенничество и программно-технические угрозы и другое. Сервис является анонимным и бесплатным. На портале можно также сообщить информацию о пропавших детях.

ВСЕРОССИЙСКАЯ БЕСПЛАТНАЯ ГОРЯЧАЯ ЛИНИЯ ПО ПРОТИВООДЕЙСТВУЮ СЕКСУАЛЬНОМУ НАСИЛИЮ НАД ДЕТЬМИ

Горячая линия принимает сообщения об информационных материалах с признаками детской порнографии онлайн или по телефону: 8-800-250-98-98 (Службу поддерживает некоммер-



ческое партнерство «Мониторинговый центр по выявлению опасного и запрещенного законодательством контента»)

ГОРЯЧАЯ ЛИНИЯ ПО ПРИЕМУ СООБЩЕНИЙ О ПРОТИВОПРАВНОМ КОНТЕНТЕ В СЕТИ ИНТЕРНЕТ

Горячая линия по приему сообщений от пользователей Интернета о ресурсах, содержащих материалы с признаками противоправности, функционирует при поддержке Лиги безопасного Интернета. Специалисты горячей линии принимают и анализируют сообщения пользователей по двум категориям: детская порнография и пропаганда и сбыт наркотиков. Сервис является анонимным и бесплатным.

ЛИНИИ ПОМОЩИ И ТЕЛЕФОНЫ ДОВЕРИЯ:

* Всероссийский детский телефон доверия. Телефон: 8-800-2000-122. Звонок с любого телефонного номера, в том числе мобильного, – бесплатный, звонить можно в любое время суток.

* Центр экстренной психологической помощи МЧС России. Телефон горячей линии (495) 626-37-07, (812) 718-25-16. Горячие линии работают круглосуточно.

* Детский телефон Доверия. Доступен круглосуточно. Телефон: (495) 624-60-01.

* Службы психологической помощи по регионам России на сайте: ya-goditel.ru.

* Центр экстренной психологической помощи Московского психолого-педагогического университета. Работает с понедельника по пятницу с 9.00 до 20.00, в субботу 10.00 до 20.00. Телефон: (499) 795-15-01.

* Центр психолого-медико-социального сопровождения «Озон» оказывает комплексную помощь детям и их семьям по широкому кругу вопросов. Телефон: (499) 265-01-18.

* В фонде НАН вы можете получить информацию о диагностике и лечении игровой компьютерной зависимости. Телефон: (499) 126-04-51. Адрес в Интернете: nan.ru.

* Детско-подростковый реабилитационный комплекс «Квартал» НД №12 предоставляет консультации по вопросам игровой зависимости. Телефон: (499) 783-27-67.

СПИСОК РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

1. О защите детей от информации, причиняющей вред их здоровью и развитию: Федеральный закон от 29.12.2010 № 436 // Российская газета. – 2010. – 31 декабря. – С. 15.
 2. Концепция информационной безопасности детей : [4 декабря 2013 г. в Роскомнадзоре состоялась пресс-конференция, посвящённая обсуждению Концепции информационной безопасности детей. Обзор] // Библиотека в школе. – 2014. – № 2. – С. 6.
 3. «Концепция информационной безопасности детей». Фрагменты подраздела 20.5 «Опыт, формы и методы информационного образования детей в России (по возрастным категориям)» : [фрагменты, которые касаются непосредственно школьных библиотек] // Школьная библиотека. – 2014. – № 2. – С. 15 – 19.
 4. Концепция информационной безопасности детей // Семья и школа. – 2015. – № 11 – 12. – С. 74 – 77.
 5. Концепция информационной безопасности детей. Утверждена распоряжением Правительства Российской Федерации от 2 декабря 2015 г. № 2471-р // Школьная библиотека. – 2016. – № 2. – С. 4 – 8.
 6. Концепция информационной безопасности детей // Библиотека и закон. – 2016. – Вып. 40 (№1 – 2016). – С. 132 – 137.
- * * *
1. Анохин, С. М. Информационно-психологическая безопасность российских детей : [информационно-коммуникационные сети, защищённость психики, интернет-ресурсы, манипуляция сознанием, цензура, медиабезопасность] / С. М. Анохин, Н. Ф. Анохина // Народное образование. – 2013. – № 3. – С. 14 – 20.
 2. Асанова, Н. Сделать сеть безопасной. Как не запутаться в паутине... : [безопасные поисковые системы для детей и родителей] / Н. Асанова // Библиотека. – 2015. – № 10. – С. 17 – 19.
 3. Безопасный Интернет : [рекомендации пользователям Интернета по информационной безопасности] // Не будь зависим. Скажи «нет» наркотикам, алкоголю, курению, игромании. – 2015. – № 11-12. – С. 10 – 11 : фото.
 4. Благовещенский, А. Мойте руки перед кликом: [о новых вирусах в Интернете и правилах безопасности в сети] / А. Благовещенский, Т. Фомченков // Российская газета. – 2017. – 29 июня (№ 140). – С. 5.



5. Бокова, Л. Нужно выстроить новое детское информационное пространство: [председатель временной комиссии Совета Федерации по развитию информационного общества рассказывает о Едином уроке безопасности в сети Интернет и новом проекте по этой теме] / Л. Бокова // Российская Федерация сегодня. – 2017. – № 4. – С. 26 – 29 : ил.
6. Бондаренко, Е. А. Подросток в море СМИ: плыть? бороться? использовать? : [региональные аспекты медиаобразования в постиндустриальном обществе – интеграция медиаобразования в систему работы педагога, аудиовизуальное творчество детей] / Е. А. Бондаренко // Народное образование. – 2015. – № 3. – С. 213 – 218.
7. Бочаров, М. И. Информационные угрозы и защита от них в младшей школе: [подходы к обучению учащихся младших классов информационной безопасности, ситуационное обучение] / М. И. Бочаров // Народное образование. – 2010. – № 8. – С. 265 – 273.
8. Воробьев, А. Колличество рисков растёт, но растёт и медиаграмотность / А. Воробьев // Дети в информационном обществе. – 2017. – № 26. – С. 12 – 15 : фот.
9. Вураско, А. За картинкой в сети дети не видят зловышленника / А. Вураско // Дети в информационном обществе. – 2017. – № 26. – С. 20 – 21 : фот.
10. Гаянова, Т. И. Дети в Интернете: библиотека в помощь формированию культуры использования информационного пространства Интернета: [Неделя безопасного Рунета в Ульяновской областной библиотеке для детей и юношества им. С.Т. Аксакова] / Т. И. Гаянова // Школьная библиотека. – 2011. – № 1 – 2. – С. 129 – 136.
11. Гаспарян, С. Цифровая зона опасности. Пять советов тем, кто работает с юными пользователями сети Интернет / С. Гаспарян // Библиотека. – 2015. – № 4. – С. 54 – 56.
12. Гончарук, Д. «Даркнет»: тёмная сторона Интернета : [7 апреля – День рождения Рунета, основное достоинство которого – общедоступность и открытость, но есть в нём и тёмные закоулки, где действуют свои правила, главное из которых – анонимность] / Д. Гончарук // Российская Федерация сегодня. – 2017. – № 4. – С. 20-25 : ил.
13. [Губанова, А. «Белая книга» интернета: о критериях оценки контента для детей / А.Губанова // Библиотечное дело. – 2015. – № 8. – С. 18-21 : ил.

14. Дерендяева, Н. С. О защите сознания и самосознания: [деятельность библиотеки по формированию культуры информационной безопасности – опыт библиотек Ямало-Ненецкого и Ханты-Мансийского автономных округов] / Н. С. Дерендяева // Народное образование. – 2015. – № 5. – С. 208 – 215.
15. Интернет и социокультурные трансформации : [материалы Всероссийской научно-практической конференции. Москва, 21-22 апреля 2015 года, отражены негативные последствия развития и использования Интернета] // Школьная библиотека. – 2015. – № 5 – 6. – С. 15 – 20.
16. Колосова, Е. А. Десятилетие Недели безопасного Рунета в библиотеках : значимые результаты и дальнейшие перспективы: [проблемы цифровой безопасности] / Е. А. Колосова // Библиотечное дело. – 2017. – № 15. – С. 2 – 4 : фот.
17. Косарина, И.И. Планета «Интернет»: выбор взрослых, выбор детей / И.И. Косарина // Современная библиотека. – 2010. – № 3. – С. 78.
18. Косенко, В. П. «Вебландия»: [ежегодная акция «Неделя безопасного Интернета»] / В. П. Косенко, В. П. Чудинова // Современная библиотека. – 2013. – № 2. – С. 24 – 27.
19. Косолапова, Е.В. Социальные медиа как среда обитания современных детей и подростков: мнимые угрозы и реальные риски / Е. В. Косолапова // Школьная библиотека. – 2017. – № 10. – С. 38 – 48.
20. Крамер, Е. А. Прививка от киберзависимости : [анкетирование родителей и учащихся об информационных угрозах] / Е. А. Крамер // Начальная школа. – 2015. – № 4. – С. 32 – 35.
21. Куликова, Е. Игра по правилам : [прогулки по виртуальным джунглям: Неделя безопасного Рунета в Тамбовской областной детской библиотеке] / Е. Куликова // Библиотечное дело. – 2015. – № 8. – С. 32 – 33 : ил.
22. Лазеева, Л. П. Библиотека за чистый Интернет : [информационная безопасность] / Л. П. Лазеева // Школьная библиотека. – 2014. – № 3-4. – С. 137 – 141 : фото.
23. Лебедева, О. Компьютерная грамотность и безопасность подростков в сетевом режиме : [опыт работы в Рязанской ОНБ] / О. Лебедева // Библиотека. – 2014. – № 4. – С. 29 – 30.
24. Медиаграмотность: [роль библиотек в формировании медиаграмотности и информационной культуры у детей и подростков – тематический выпуск] // Библиотечное дело. – 2015. – № 8. – С. 2-44.

25. Поговорите с ребёнком об интернете : методическое пособие // Дети в информационном обществе. – 2017. – № 26. – С. 48 – 60 : ил.
26. Серёгина, Е. «Дети в Интернете»: уроки безопасности от МТС / Е. Серёгина, Т. Герасименко // Дети в информационном обществе. – 2017. – № 26. – С. 38 – 41 : фот.
27. Сокоерина, Е. Н. Родительский контроль, фильтры, советы и запреты : [о деятельности Национальной детской библиотеки Республики Коми им. С. Я. Маршак по защите детей от киберопасностей] / Е. Н. Сокоерина // Библиотечное дело. – 2017. – № 15. – С. 25 – 27 : фот.
28. Суслова, И. Радуга Рунета. Путешествия по Интернетландии : [Неделя безопасного Рунета в Липецкой областной детской библиотеке] / Ирина Суслова // Библиотечное дело. – 2015. – № 8. – С. 37 – 38 : ил. 1
29. Трушина, И. А. ФЭ-436 : чтение с остановками. : [пролемы применения ФЗ № 436 «О защите детей от информации, причиняющей вред их здоровью и развитию» в библиотеках и рекомендации РБА по его применению] / И.А. Трушина // Библиотека в школе. – 2013. – № 9. – С. 13 – 17.
30. Ухова, С. Кибератаки : предупредить и обезвредить : [о безопасности интернет-ресурсов ; DDoS-атаки и борьба с ними] / С. Ухова // Деловое обозрение. – 2017. – № 6. – С. 44 – 45 : ил., фот.
31. Учим детей отличать правду от лжи : [интернет-безопасность: чем опасны фейки и как защититься от фейковых новостей] // Библиотека в школе. – 2017. – № 9 – 10. – С. 4 – 6.
32. Фалалеев, М. Домушники живут в Интернете : [квартирные воры пользуются Сетью для наводки] / М. Фалалеев // Российская газета. – 2017. – 18 янв. – С. 7.
33. Чернова, Т. «Ну погоди!» ничего не угрожает : [для родителей напишут инструкцию, как оградить ребёнка от опасностей в медиaproстранстве] / Т. Чернова // Российская газета. – 2014. – 16 – 22 янв. – С. 8.
34. Чудинова, В. П. Наши дети в интернете : обеспечение безопасности и продвижение позитивного контента : [безопасность детей онлайн, проблемы развития позитивного контента, стратегия действия дет.библиотек по безопасному интернету] / В. П. Чудинова // Библиотечное дело. – 2015. – № 8. – С. 5 – 12.



35. Шадрина, Т. Ничего тайного : [Наталья Касперская: Интернет вещей – катастрофическая штука с точки зрения информационной безопасности] / Т. Шадрина // Российская газета. – 2017. – 20 июня (№ 132). – С. 8 : ил.
36. Шаталина, И. А. Интернешка : [занятия по правилам безопасного пользования Интернетом для 2-6 классов] / И. А. Шаталина // Игровая библиотека. – 2012. – № 3. – С. 24 – 31.
37. Шершнев, Л. Виды безопасности : [о важнейших видах безопасности] / Л. Шершнев // ОБЖ. – 2011. – № 12. – С. 20 – 30.

ССЫЛКИ НА ИНТЕРНЕТ-РЕСУРСЫ:

1. Азбука безопасности [Электронный ресурс]. – Режим доступа: <http://azbez.com/> (24.01.2018).
2. Безопасный Интернет для детей : законодательство, советы, мнения, международный опыт. – Режим доступа: <http://deti.org/> (24.01.2018).
3. Дети России Онлайн [Электронный ресурс]. – Режим доступа: <http://detionline.com/> (24.01.2018). (Подробное руководство, обеспечивающее безопасную работу детей в Интернете)
4. Единый урок по безопасности в сети «Интернет» [Электронный ресурс] // Единый урок. Календарь, методики, материалы. – Режим доступа : <https://www.единыйурок.rf/index.php/kalendar-edinykh-urokov/item/7-edinyj-urok-ro-bezopasnosti-v-seti-internet> (24.01.2018).
5. Интернет-зависимое поведение. Критерии и методы диагностики : учебное пособие. – Москва: МГМСУ, 2011. – 32 с. ; То же [Электронный ресурс]. – Режим доступа: <http://medpsy.com/library/library135.pdf> (24.01.2018).
6. Научи хорошему – за возрождение нравственности в СМИ [Электронный ресурс]. – Режим доступа: <https://whatisgood.ru/> (24.01.2018).



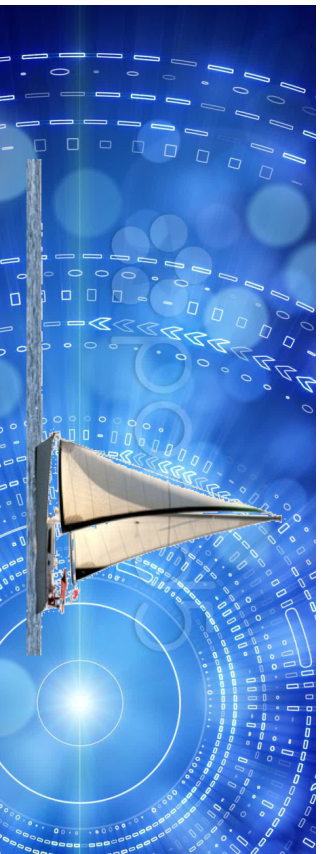
СОДЕРЖАНИЕ

7. Москвитина, О. А. Основные характеристики младшего подросткового возраста [Электронный ресурс] / О. А. Москвитина // Superinf.ru. Информационная помощь студентам. – Режим доступа : https://superinf.ru/view_hehrstud.php?id=5608. (24.01.2018).
8. Основы детской безопасности [Электронный ресурс] // Google. Центр безопасности. – Режим доступа:<http://www.google.ru/safelycenter/families/start/basics/> (24.01.2018).
9. Персональные данные Дети [Электронный ресурс] : сайт. – Режим доступа <http://персональныеданные.дети/> (24.01.2018). (База материалов в виде правил, презентаций, тестов и игр, объясняющих детям о важности личной информации при использовании цифровых технологий.)

10. Права и дети в Интернете [Электронный ресурс] // Школьный сектор Ассоциации РЕПАРН. – Режим доступа: <http://school-sector.relarn.ru/prava/index.html> (24.01.2018).

11. Фонд развития Интернет [Электронный ресурс] – Режим доступа: <http://www.fid.su/> (24.01.2018).

12. Чемпионат по кибер-грамотности : [в 2016 году состоялся V Всероссийский онлайн-чемпионат «Изучи Интернет – управляй им!»] // Дети в информационном обществе. – 2017. – №26. – С. 76-77 ; То же [Электронный ресурс] : – Режим доступа : <http://school-sector.relarn.ru/wrs/?r=4722> (24.01.2018). (Социально-образовательный проект для школьников, который позволяет получить базовые знания об устройстве и возможностях сети Интернет)



От составителей	3
Методические рекомендации	5
Сценарий квеста	7
Правила квеста	8
1 площадка	
Секретные материалы The X-Files	9
2 площадка	
Украденное время (компьютерная зависимость)	12
3 площадка	
Побег из Паутины	15

Вторая часть игровой познавательной программы 19

4 площадка	
«Виртуальные помощники или Программы, атакующие вирусы» или «Агенты 007 – Борцы с вирусами»	20
5 площадка	
«Великие и независимые. Узнайте их...»	25
6 Площадка	
В лабиринтах обмана (мошенничество)	30

Приложения 35

1 Пример карты-маршрута	35
2 Ключ	36
3 Послания	35
4 Полезные ссылки, которые можно рекомендовать детям после квеста, оформив закладки, рекламные памятки	38
Горячие линии и службы поддержки по вопросам безопасности в Интернете	39
Линии помощи и телефоны доверия	40
Список рекомендуемой литературы	41
Ссылки на интернет-ресурсы	45

