



Электронная библиотека
«Формирование основ
информационной
безопасности в картинках»



**ПОЛИЦИЯ
ПРЕДУПРЕЖДАЕТ!**

ВНИМАНИЕ **телефонные** **МОШЕННИКИ** **ВЫ ПОЛУЧИЛИ СМС?**

**ПРОЯВЛЯЙТЕ
БДИТЕЛЬНОСТЬ! НЕ ОТВЕЧАЙТЕ!**

выигрыш

Поздравляем! Вы выиграли автомобиль.
Подробности по телефону
+7 000 000 0000

**вирусная
атака**

Вам пришла открытка. Для
получения пройдите по
ссылке <http://000.000.000.ru>

**просьба
о помощи**

Мама у меня беда! Срочно
положи мне на этот номер
денег, потом позвоню.
Помоги!

**карта
заблокирована**

Ваша карта заблокирована.
Позвоните по номеру
+7 000 000 0000

**просьба
перечислить
деньги**

Зачислено 200,00 руб
пополняй баланс за 0%

НЕ **ОТПРАВЛЯЙТЕ ПРЕДОПЛАТУ ПО ОБЪЯВЛЕНИЯМ С САЙТОВ!**
НЕ **СООБЩАЙТЕ ПИН-КОД!**
НЕ **ПЕРЕВОДИТЕ ДЕНЬГИ!**

Извините я вам деньги
ошибочно попожила, вас не
затруднит вернуть

ВО ВСЕХ ПОДОЗРИТЕЛЬНЫХ СЛУЧАЯХ ЗВОНИТЕ - 02

ПОЛИЦИЯ ПРЕДУПРЕЖДАЕТ:

МОШЕННИКИ ИСПОЛЬЗУЮТ РАЗЛИЧНЫЕ СПОСОБЫ ОБМАНА

ЗВОНИТЕ!

К ВАМ ПРИШЛИ
НЕЗНАКОМЫЕ ЛЮДИ



НЕ ОТКРЫВАЙТЕ дверь даже если они представляются работниками пенсионного фонда, газовой и социальной служб, поликлиники, ЖКХ и т.п.

02
102



ПОСТУПИЛ ТЕЛЕФОННЫЙ ЗВОНОК или СМС-СООБЩЕНИЕ, что НУЖНЫ ДЕНЬГИ, чтобы спасти попавшего в БЕДУ родственника (попал в ДТП, подрался, забрали в полицию и т.п.)



Вас обманывают!
Звоните в ПОЛИЦИЮ
02

ИНТЕРНЕТ-МАГАЗИН
БОЛЬШИЕ СКИДКИ %



НИКАКИХ ПРЕДОПЛАТ!
Оплачивая что-либо в сети Интернет, Вы не имеете никаких гарантий

Вы выиграли ПРИЗ!!!



Вас обманывают!
ПРИЗ Вы НЕ получите и ДЕНЬГИ Вам НЕ вернут!

Если Вы или Ваши близкие стали жертвами мошенников, или Вы подозреваете, что в отношении Вас планируются противоправные действия — **незамедлительно обращайтесь в полицию!**

102
с мобильного

02

(4852) 73-10-50
телефон доверия

Вам обязательно помогут!

76.мвд.рф

УМВД России по Ярославской области

ПРЕДУПРЕЖДАЕТ



ОСТОРОЖНО: МОШЕННИКИ!

НЕ ДАЙТЕ СЕБЯ ОБМАНУТЬ!

ИНТЕРНЕТ-МОШЕННИКИ

ОБЪЯВЛЕНИЕ О ПРОДАЖЕ



Мошенники-продавцы просят перечислить деньги за товар, который впоследствии жертва не получает.

ОБЪЯВЛЕНИЕ О ПОКУПКЕ

Мошенники-покупатели спрашивают реквизиты банковской карты и (или) смс-код якобы для перечисления денег за товар, после чего похищают деньги с банковского счета.



ТЕЛЕФОННЫЕ МОШЕННИКИ

ЗВОНОК О НЕСЧАСТНОМ СЛУЧАЕ



Мошенники звонят жертве от лица близкого человека или от представителя власти и выманивают деньги.

Мама, я попал в аварию!



БЛОКИРОВКА БАНКОВСКОЙ КАРТЫ

Сообщение о блокировании банковской карты с номером, по которому нужно позвонить. Цель — узнать личный код банковской карты.

ПОЛУЧЕНИЕ ВЫГРЫША (компенсации за потерянный вклад)

Мошенники сообщают о выигрыше приза, возможности получения компенсации за потерянный вклад в «финансовую пирамиду» и т.п. Жертве можно забрать его, заплатив налог или плату якобы «за сохранность денег».



ВИРУС В ТЕЛЕФОНЕ

Мошенники запускают вирус в телефон, предлагая пройти по «зараженной ссылке» (в том числе и от имени друзей). С помощью вируса получают доступ к банковской карте, привязанной к телефону. Установите антивирус и не переходите по сомнительным ссылкам.



СООБЩЕНИЯ ОТ ДРУЗЕЙ



Мошенник пользуется чужой страничкой в социальной сети в Интернете, и под видом друга (родственника) просит перечислить ему деньги или сообщить данные Вашей карты якобы для перечисления Вам денег под различными предлогами.

УМВД России по Ярославской области
ПРЕДУПРЕЖДАЕТ! ОСТОРОЖНО!
Мошенничество с банковскими картами

Вам поступил звонок,
в том числе с номера телефона банка:
«Ваша банковская карта заблокирована»
с просьбой сообщить данные карты.
ПОМНИТЕ! Ни одна организация, включая банк,
не вправе требовать реквизиты карты!



Необходимо прервать разговор.
Проверьте информацию, позвонив в клиентскую
службу поддержки банка. Велика вероятность того, что
вы общались с мошенником. Никогда не сообщайте
данные своих банковских карт: срок действия, CVC-код,
СМС-коды, одноразовые пароли, кодовые слова.

Звоните в полицию: 02, 102

УМВД России по Ярославской области
ПРЕДУПРЕЖДАЕТ!



НЕ ОТКРЫВАЙТЕ дверь незнакомым
людям, даже если они представляются
работниками социальных, газовых,
электроснабжающих служб, полиции,
поликлиники, ЖКО и т.д.
Перезвоните и уточните, направляли ли
к Вам этого специалиста!

НЕ ДОВЕРЯЙТЕ, если Вам звонят с
сообщением, что Ваш родственник или
знакомый попал в аварию, за решетку, в
больницу или совершил ДТП, и теперь за
него нужно внести залог, штраф, взятку,
выкупить дорогие лекарства - в общем
откупиться. **НЕ ВЕРЬТЕ! ЭТО ОБМАН!**



Незнакомка представляется соцработ-
ником или представителем органов
власти, сообщая о надбавке к пенсии,
перерасчете квартплаты, срочном
обмене денег на дому или предлагая
приобрести товары по неправдоподоб-
ным низким "льготным" ценам?
НЕ ВЕРЬТЕ - ЭТО МОШЕННИЦА!

ЗВОНИТЕ В ПОЛИЦИЮ

02/102

ТЕЛЕФОН ДОВЕРИЯ УМВД: (4852) 73-10-50



УМВД России по Ярославской области ПРЕДУПРЕЖДАЕТ: **ВНИМАНИЕ! МОШЕННИКИ!**

Представляются:

- работником газовой службы
- оператором сотовой связи
- представителем банка
- покупателем товаров онлайн

Могут НАЗЫВАТЬ ваши персональные данные (ФИО, паспортные данные, адрес проживания), а также вашу последнюю операцию по карте

КАК ДЕЙСТВУЮТ МОШЕННИКИ

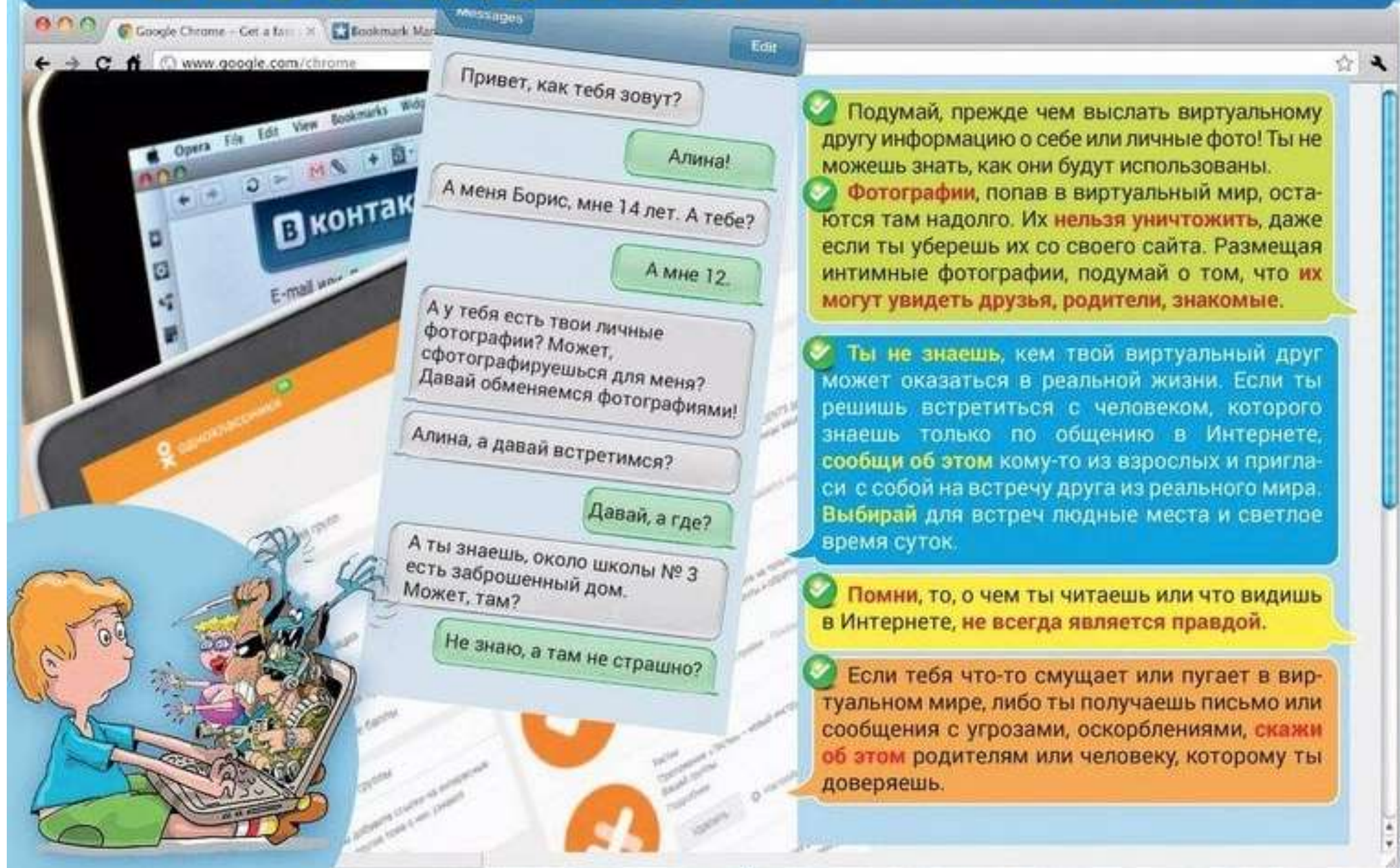
Просят продиктовать реквизиты карты, СМС КОД для списания ваших денежных средств

**ДЕЙСТВУЙТЕ
ТАК!!!**

Отвечайте следующими фразами: «Мне некогда», «Мне это не интересно». «Представьтесь, из какой вы организации», «Ваши имя и фамилия?», «Я Вам перезвоню».

О подозрительном звонке или визите сразу сообщите родственникам, в отдел полиции (с мобильного - 102), в отделение вашего банка.

БЕЗОПАСНЫЙ ИНТЕРНЕТ



Привет, как тебя зовут?

Алина!

А меня Борис, мне 14 лет. А тебе?

А мне 12.

А у тебя есть твои личные фотографии? Может, сфотографируешься для меня? Давай обменяемся фотографиями!

Алина, а давай встретимся?

Давай, а где?

А ты знаешь, около школы № 3 есть заброшенный дом. Может, там?

Не знаю, а там не страшно?

✓ Подумай, прежде чем выслать виртуальному другу информацию о себе или личные фото! Ты не можешь знать, как они будут использованы.

✓ **Фотографии**, попав в виртуальный мир, остаются там надолго. Их **нельзя уничтожить**, даже если ты уберешь их со своего сайта. Размещая интимные фотографии, подумай о том, что **их могут увидеть друзья, родители, знакомые**.

✓ Ты не знаешь, кем твой виртуальный друг может оказаться в реальной жизни. Если ты решишь встретиться с человеком, которого знаешь только по общению в Интернете, **сообщи об этом** кому-то из взрослых и пригласи с собой на встречу друга из реального мира. **Выбирай** для встреч людные места и светлое время суток.

✓ Помни, то, о чем ты читаешь или что видишь в Интернете, **не всегда является правдой**.

✓ Если тебя что-то смущает или пугает в виртуальном мире, либо ты получаешь письмо или сообщения с угрозами, оскорблениями, **скажи об этом** родителям или человеку, которому ты доверяешь.



ПОМНИТЕ!

ИНТЕРНЕТ может быть
прекрасным и полезным
средством для обучения,
отдыха или общения с друзьями.

Но – как и реальный мир –
Сеть тоже может быть опасна!

Как проявляется кибербуллинг

Электронные письма или мгновенные сообщения с оскорблениями или угрозами.

Оскорбления во время онлайн-игр в сети.

Умышленное применение функции «Пожаловаться» только для того, чтобы пользователя забанили на сайте.

Создание поддельных профилей, сайтов - кто-то запускает страницу от твоего имени и наполняет ее постыдной информацией.

Использование твоих данных для регистрации на различных сайтах.

Использование твоего никнейма (или слегка видоизмененного) для создания ложного аккаунта, чтобы оскорблять других людей якобы от твоего имени.

Копирование в публичном доступе личных переписок.

Создание опросов (например, «Ваня – тормоз или ботан?»), предназначенных для того, чтобы смутить или унизить тебя.



Составление оскорбительных рейтингов с участием знакомых: «Кто самый толстый?», «Кто самый глупый?» и т.п.

Публикация списка твоих контактов.

Порождение слухов, которые приведут к киберпреследованию со стороны других детей – к примеру, о том, что ребенок якобы высмеивает за спиной своего друга.

Использование твоего пароля для изменения учетной записи: добавления фото, статусов, записей от твоего имени.

Блокировку твоего аккаунта путем смены пароля.

Рассылки оскорбительных фото или картинок на почту и в социальные сети.

Размещение твоего фото в сети (его могут украсть у тебя с телефона, вырезать из видео или взять на твоей страничке в социальной сети и растиражировать).

Публикация личной информации о тебе (когда кто-то, воспользовавшись твоим доверием, рассказывает всему интернету твои секреты).

ИНТЕРНЕТ – ЭТО БЕЗГРАНИЧНЫЙ

МИР ИНФОРМАЦИИ. ЗДЕСЬ ТЫ

НАЙДЕШЬ МНОГО ИНТЕРЕСНОГО И ПО-

ЛЕЗНОГО ДЛЯ УЧЁБЫ. В ИНТЕРНЕТЕ

МОЖНО ОБЩАТЬСЯ СО ЗНАКОМЫМИ И

ДАЖЕ ЗАВОДИТЬ ДРУЗЕЙ.



НО КРОМЕ ХОРОШЕГО, В ВИРТУАЛЬ-

НОМ МИРЕ ЕСТЬ И ПЛОХОЕ. НЕПРА-

ВИЛЬНОЕ ПОВЕДЕНИЕ В ИНТЕРНЕТЕ

МОЖЕТ ПРИНЕСТИ ВРЕД НЕ ТОЛЬКО

ТЕБЕ, НО ТАКЖЕ ТВОИМ РОДНЫМ

И БЛИЗКИМ.



ЧТОБЫ ОБЕЗОПАСИТЬ СЕБЯ В ИН-

ТЕРНЕТЕ, ДОСТАТОЧНО СОБЛЮДАТЬ

ПРАВИЛА, КОТОРЫЕ СОДЕРЖАТСЯ В

ЭТОЙ ПАМЯТКЕ. В ЭТИХ ПРАВИЛАХ

НЕТ НИЧЕГО ТРУДНОГО. ОТНЕСИСЬ К

НИМ ВНИМАТЕЛЬНО – И РАССКАЖИ

О НИХ СВОИМ ДРУЗЬЯМ!



ТЕСТ НА ЗНАНИЕ ПРАВИЛ ПОВЕДЕНИЯ В ИНТЕРНЕТЕ

1) Новый друг, в чьих данных указан тот же возраст, что и у тебя, предлагает тебе обменяться фотографиями.

А Попрошу его фото, и потом отправлю своё.

В Посоветуюсь с родителями.

2) В чате тебя обозвали очень грубыми словами.

А Скажу в ответ: «Сам дурак».

В Прекращу разговор с этим человеком.

3) Знакомый предложил разослать телефон и адрес «плохой девочки», чтобы все знали о ней.

А Потребую доказательств, что она плохая.

В Сразу откажусь.

4) Пришло сообщение с заголовком «От провайдера» – запрашивают твой логин и пароль для входа в Интернет.

А Вышлю только пароль: они сами должны знать логин.

В Отмечу письмо как Спам.

ПОСЧИТАЙ, СКОЛЬКО ПОЛУЧИЛОСЬ
ОТВЕТОВ «А» И СКОЛЬКО «В».



4 «А»

Тебе ещё многому надо научиться.



3 «А» и 1 «В»

Внимательно прочитай эту памятку.



2 «А» и 2 «В»

Неплохо, но ты защищён лишь наполовину.



1 «А» и 3 «В»

Ты почти справился, но есть слабые места.



4 «В»

Молодец! К Интернету готов!



Министерство
внутренних дел
Российской
Федерации

Управление «Н»



БЕЗОПАСНЫЙ ИНТЕРНЕТ – ДЕТЯМ!

Полезные
советы
для тебя
и твоих
друзей



ОСТОРОЖНО:

ВИРУСЫ И ДРУГИЕ

ЧЕРН. ТРОЯНЫ

ВРЕДОНОСНЫЕ ПРОГРАММЫ

В Интернет ты заходишь через компьютер. Это может быть школьный или библиотечный компьютер, твой личный или тот, которым пользуется вся семья.

Любому компьютеру могут повредить вирусы, их еще иногда называют вредоносными программами. Они могут уничтожить важную информацию или украсть деньги через Интернет.

- Для защиты компьютера на нём установлены специальные защитные программы и фильтры. Не меняй ничего в их настройках!
- Не сохраняй подозрительные файлы и не открывай их.
- Если антивирусная защита компьютера не рекомендует, не заходи на сайт, который считается «подозрительным».
- Никому не сообщай свой логин с паролем и не выкладывай их в Интернете – относись к ним так же бережно, как к ключам от квартиры.



ВИРТУАЛЬНЫЕ МОШЕННИКИ (ЗЕЛЫ) И ДРУГИЕ ПРЕСТУПНИКИ ИНТЕРНЕТА

Ты знаешь, что вне дома и школы есть вероятность столкнуться с людьми, которые могут причинить тебе вред или ограбить. В Интернете также есть злоумышленники – ты должен помнить об этом и вести себя так же осторожно, как и на улице или в незнакомых местах.

- Не сообщай свой адрес или телефон незнакомым людям и никогда не выкладывай в Интернете. Никогда не высылай свои фотографии без родительского разрешения. Помни, что преступники могут использовать эту информацию против тебя или твоих родных.
- Если ты хочешь поучаствовать в каком-нибудь конкурсе, где нужно указывать свои данные, посоветуйся с родителями.
- Никогда не соглашайся прийти в гости к человеку, с которым ты познакомился в Интернете. Если назначается встреча, она должна проходить в людном месте и желательно с присутствием родителей. Помни, что под маской твоего ровесника может скрываться взрослый человек с преступными намерениями.



ГРУБИЯНЫ И ХУЛИГАНЫ ТРОЛЬ, ПРОВОКАТОР В ИНТЕРНЕТЕ: КАК СЕБЯ ВЕСТИ?

Кроме преступников в Интернете есть просто злые и невоспитанные люди. Ради собственного развлечения они могут обидеть тебя, прислать неприятную картинку или устроить травлю. Ты можешь столкнуться с такими людьми на самых разных сайтах, форумах и чатах.

- Помни: ты не виноват, если получил оскорбительное сообщение. Не нужно реагировать на грубых людей – просто прекрати общение.
- Если тебе угрожают по Интернету, не стесняйся сообщить об этом родителям. Помни, что цель угроз – испугать тебя и обидеть. Но подобные люди боятся ответственности.
- Коллективное преследование – это крайнее проявление жестокости. Жертву забрасывают оскорблениями и угрозами, его фотографию искажают и все данные публикуют. Никогда не участвуй в травле и не общайся с людьми, которые обижают других.
- Всегда советуйся с родителями во всех указанных случаях.



Как обезопасить себя и близких:

- **Не рассказывайте** в социальных сетях подробности о себе и своих близких, избегайте откровенностей в открытых чатах, пубliках, форумах;
- **Не пересылайте** бездумно информацию в соцсетях;
- **Ограничьте доступ** к своим аккаунтам, а также фото- и видеозаписям кругом друзей, которых вы лично знаете;
- Не соглашайтесь на сомнительные предложения подзаработать. Помните: сомнительные — **зачастую противоправные**;
- **Подвергайте сомнению** любую информацию от незнакомцев.



Незамедлительно прервите общение с незнакомцем, если он:

- **Просит прислать персональные данные**, сообщить место жительства или информацию о банковских картах;
- Настойчиво **навязывает** свою **помощь**;
- Навязчиво и беспричинно **пытается войти** к вам **в доверие**;
- Обещает **решить все проблемы**, если вы выполните его условия;
- **Угрожает** в случае вашего отказа.



Наш адрес:
г. Ярославль, ул. Пионерская, д. 19.
Тел.: 68-14-29

E-mail: moucentredoverie@mail.ru
<http://centr-doverie.edu.yar.ru>



Проезд до остановки «Ул. Пионерская»
троллейбусом № 2, 7, 8;
автобусом № 8, 10, 11, 25;
маршрутным такси № 46, 51, 71, 78, 80,
83, 87, 88, 90, 91, 97
Буклет разработала: Н.В. Хабарова

ПОЛЕЗНЫЕ КОНТАКТЫ

(обращение в случае
Интернет-угрозы):

- «Горячая линия» Центра безопасного интернета в России (круглосуточно): [8-800-200-24-00](tel:8-800-200-24-00);
- Линия помощи «Дети онлайн»: [8-800-250-00-15](tel:8-800-250-00-15) (с 9 до 18 по рабочим дням, время московское, звонки по России бесплатные);
- «Детский телефон Доверия» (обратиться за психологической помощью): [8-800-2000-122](tel:8-800-2000-122)
- Через «Интернет»: nedopusti.ru и saferunet.org (нажав на красную кнопку «Горячая линия»).
- Написав обращение по электронной почте: helpline@detionline.com;
- На сайте www.detionline.com



Муниципальное учреждение
Центр психолого-педагогической,
медицинской и социальной помощи
«Доверие»

Информация для родителей

Безопасный Интернет



Ярославль
2020



ПОЛЕЗНЫЕ КОНТАКТЫ

(обращение в
случае

Интернет-угрозы)

«Горячая линия» Центра безопасного интернета
в России (круглосуточно): 8-800-200-24-00;

Линия помощи «Дети онлайн»:

8-800-250-00-15 (с 9 до 18 по рабочим дням, время
московское, звонки по России бесплатные);

«Детский телефон Доверия» (обратиться за
психологической помощью): 8-800-2000-122

Через «Интернет»: nedopusti.ru и saferunet.org (нажав
на красную кнопку «Горячая линия»)

Написав обращение по электронной почте:
helpline@detionline.com;

На сайте www.detionline.com

**Календарь мероприятий по информационной безопасности
в рамках инновационного проекта
«Академия культуры информационной безопасности участников
образовательных отношений»**

№	Наименование	Дата	участники	Организаторы	формат
1.	Комплексное образовательное событие «День безопасной информации»	март	5-7 кл 8-11 кл	классные руководители, педагоги-организаторы	офлайн
2.	Тематические лектории для родительской общности по теме «Развитие культуры информационной безопасности»	март, сентябрь, декабрь	родители 1-11 классов	администрация, педагог-психолог, классные руководители	офлайн + онлайн
3.	Электронная библиотека «Формирование основ информационной безопасности в картинках»	в течение года	педагоги, родители	библиотекарь администратор сайта, паблика	офлайн + онлайн
4.	Семинар классных руководителей «Безопасная среда как условие личностного развития подростков»	ноябрь	учителя-предметники, классные руководители, воспитатели	педагог-психолог, администрация	офлайн



Муниципальное образовательное учреждение
средняя общеобразовательная школа
«Образовательный комплекс имени Б.Н. Богачева»



Центр образования лицей № 2

Круглый стол-дискуссия
**«Виртуальное предложение – реальные последствия:
Действия виртуальные, ответственность - реальная»**
(о недопустимости взаимодействия с аккаунтами,
предлагающими нарушать правопорядок)

Рыбинск, 2025 год
Круглый стол-дискуссия

**«Виртуальное предложение – реальные последствия:
Действия виртуальные, ответственность - реальная»**
(о недопустимости взаимодействия с аккаунтами,
предлагающими нарушать правопорядок)

Вступление (спикер)

Здравствуйте! Сегодня мы поднимаем важную тему безопасности в сети, и то, как виртуальные знакомства могут обернуться реальными последствиями.

Начну с вопроса: что объединяет три критических случая, в каждом из которых виновные получили реальные тюремные сроки:

2 апреля 2023 года – взрыв в Санкт-Петербурге (1 жертва, около 70 пострадавших)

15-17 марта 2024 года – нарушение правопорядка (порча бюллетеней) на избирательных участках;

22 марта 2024 года – террористический акт в Крокус Сити Холле (более 130 жертв и еще более 160 пострадавших).

Ответ: *С исполнителями связывались по телефону или другим средствам связи и обещали достойное вознаграждение за нарушение правопорядка.*

Часть 1. Последствия для исполнителей:

Сколько получили исполнители за то, что согласились на сделку?

- 27 лет колонии;
- до 5 лет лишения свободы;
- пожизненное заключение.

Последствия для остальных: погибшие люди, которые не увидели свои семьи и не смогли сделать мир лучше; пострадавшие люди с пост травматическим синдромом на некоторый отрезок жизни.

Часть 2. Почему это важно сейчас?

Ежедневно сотни подростков России получают предложения принять участие в нарушении порядка: что-то украсть, разрушить, вплоть до того, чтобы лишить других жизни. В обмен предлагают деньги или другие привилегии.

Это очень серьезное испытание для каждого из нас, и я хочу, чтобы мы вместе обсудили, как мы можем предотвратить подобные ситуации и сохранить свою неприкосновенность.

Часть 3. Законы и правила

Законы созданы для того, чтобы обеспечить порядок и безопасность каждого гражданина. Нарушение законов может повлечь за собой серьезные последствия. Например, в России существует Уголовный кодекс, который определяет, что является преступлением, и предусматривает наказания за его совершение. Поговорим о том, какие действия могут быть незаконными и какие могут быть последствия их нарушения.

Часть 3.1. Немного статистики и сухих фактов.

В первой половине 2023 года в России осудили 6503 несовершеннолетних. Россияне младше 18 лет совершают 2,4% от общего количества уголовных преступлений.

До 14 лет дети не несут уголовной ответственности, поэтому за них перед судом отвечают родители или законные представители. После достижения этого возраста подростков могут судить за отдельные тяжкие преступления: например, за убийство, причинение тяжкого вреда здоровью, грабеж, разбой, изнасилование. С 16 лет наступает полная уголовная ответственность — то есть несовершеннолетние могут оказаться на скамье подсудимых за любое преступление.

Часть 4. Почему кто-то идет на такие нарушения?

Теперь давайте обсудим причины. Как вы думаете, почему кто-то решается нарушать закон?

- Давление сверстников и стремление быть принятым в «круг избранных»;
- Трудности в семье или школе;
- Недостаток информации о последствиях.
- и т.к. (обсудить, почему их друзья идут на это).

Часть 5. Как правильно действовать, если предлагают нарушить закон?

Теперь давайте поработаем над развитием навыков принятия решений, которые помогут вам избегать вовлечения в незаконные ситуации. Важно научиться анализировать ситуации, в которые вы попадаете, и принимать обдуманные решения. Для этого можно использовать методику 'СТОП-думай-делай'. Сначала остановитесь и подумайте о возможных последствиях вашего действия. Затем внимательно проанализируйте ситуацию и возможные

варианты действий. И только после этого сделайте осознанный выбор, который не противоречит закону и вашим моральным убеждениям. Помните, что у вас всегда есть выбор, и ваши действия могут повлиять не только на вас самих, но и на окружающих.

Давайте рассмотрим несколько конкретных ситуаций.

(Здесь лучшие разбиться на команды по партам).

Каждой команде задаю вопрос (или можно раздать), вы совещаетесь минуту, а затем зачитываете вопрос и отвечаете на него. Остальные могут дополнить. Приведенные примеры ответов – не жёсткие. Можно руководствоваться здравым смыслом.

1. Предложение принять участие в курении или употреблении алкоголя на вечеринке. *Вежливо отказаться от употребления алкоголя или курения и, если возможно, покинуть вечеринку. Обратиться к родителям или другим взрослым за помощью в случае давления.*
2. Запрос на участие в буллинге или запугивании одноклассника в школе. *Отказаться от участия в запугивании и обратиться за помощью к учителю, школьному психологу или родителям. Поддержать жертву буллинга и сообщить об инциденте ответственным лицам.*
3. Приглашение присоединиться к группе, занимающейся уличным граффити или вандализмом. *Отказаться от участия в вандализме и предложить альтернативные способы проведения времени с друзьями, не связанные с нарушениями закона. Обратиться к родителям или другим взрослым за поддержкой. Либо предложить друзьям принять участия в специализированных фестивалях граффити или организовать свой фестиваль (предварительно согласовав территории).*
4. Предложение принять участие в драке или конфликте с другой группой подростков. *Попытаться разрешить конфликт мирным путем или уйти из опасной ситуации. Обратиться за помощью к взрослым или правоохранительным органам при угрозе физического насилия.*
5. Запрос на участие в краже или мелком воровстве из магазина или школы. *Отказаться от участия в краже и уведомить об этом сотрудников магазина или учителей. Обратиться к родителям за помощью в разрешении ситуации.*
6. Приглашение распространить чужую личную информацию с целью манипуляции и запугивания. *Отказаться от участия в распространении личной информации и предупредить человека, чья информация может быть распространена.*

Обратиться к родителям, учителю или правоохранительным органам за помощью.

7. В социальных сетях/мессенджерах некий аккаунт предлагает совершить нападение на мирных людей в торговом центре, обещая 500 000 рублей. *Заблокировать аккаунт, сообщить родителям/учителю, а также обратиться в соответствующие органы.*

8. Приглашение участвовать в опасных экстремальных забавах или вызовах, таких как "челленджи" в социальных сетях.

Отказаться от участия в опасных активностях и предложить альтернативные способы проведения времени, безопасные для здоровья и жизни. Предупредить родителей или взрослых о возможной опасности.

9. Предложение присоединиться к группе, занимающейся незаконным оборотом наркотиков или алкоголя.

Отказаться от участия в незаконных действиях и, если необходимо, сообщить органам правопорядка о подобных предложениях. Обратиться за помощью к взрослым или специалистам по борьбе с наркоманией.

Часть 6. Семья и общество.

Семья играет важную роль в формировании моральных ценностей и навыков у детей. Родители должны обучать своих детей правильным принципам поведения и объяснять им последствия нарушения законов, а общество создавало условия для развития положительных интересов у детей и поддерживало их в трудных ситуациях.

Расскажите, чем вы занимаетесь в свободное время?

(Дети могут рассказать о своих увлечениях)

Слово представителя полиции

Заключение (спикер)

Помните, что каждый из вас имеет силу сделать правильный выбор и соблюдать законы общества. Надеюсь, наше занятие помогло вам лучше понять последствия нарушений закона и развить навыки принятия осознанных решений. Важно использовать эти знания и навыки в повседневной жизни, чтобы стать ответственными гражданами и избежать неприятных последствий.



Муниципальное образовательное учреждение
средняя общеобразовательная школа
«Образовательный комплекс имени Б.Н. Богачева»



Центр образования лицей № 2

**Сценарий игровой программы
«На просторах интернета»
для учащихся 5-6 классов**

Рыбинск, 2025

Игра "На просторах Интернета" – это викторина, адаптированная для детей, в которой вопросы касаются различных аспектов работы и безопасности в интернете. Игра проводится в форме карусели, где дети по очереди отвечают на вопросы, а правильные ответы приносят им очки. В конце игры подводятся итоги, и определяется победитель.

Цель игры: формирование навыков безопасного использования интернета, распознавание и реагирование на интернет-угрозы.

Задачи игры:

- Систематизировать знания детей в области интернет-безопасности по направлениям:
 - раскрытие персональных данных;
 - мошенничества, в т.ч. мобильные, заражение компьютера и мобильных устройств;
 - общение в сети;
 - общая компьютерная грамотность.
- Формировать навыки безопасного использования интернета на основании имеющегося у них опыта, учить связывать навыки повседневного использования интернета и электронных устройств с правилами безопасности.
- Повышать уровень осведомленности детей о наиболее актуальных интернет-угрозах (с учетом возраста аудитории, региона, других факторов), формировать умения противодействовать интернет-угрозам.
- Воспитывать этическую культуру в цифровой среде.

1. Подготовка:

- Подготовить вопросы, касающиеся безопасного поведения в интернете, правил этикета, защиты личной информации, умения распознавать фейки и т.д.
- Разделить детей на команды или предоставить возможность играть индивидуально.
- Подготовить необходимое оборудование:
 - Карточки с вопросами.
 - Таблица для записи результатов.

- Призы для победителей (например, небольшие сувениры, наклейки, связанные с интернетом).
- Придумать название для каждой команды (например, "Браузеры", "Файерволлы", "Социальные сети").
- Подготовить место для проведения игры, чтобы дети могли свободно перемещаться по кругу.

2. Правила игры:

- Игра проводится в виде карусели, то есть дети перемещаются по кругу, отвечая на вопросы.
- Ведущий задает вопрос, а участники по очереди на него отвечают.
- За каждый правильный ответ команде начисляются очки.
- Можно установить лимит времени на обдумывание ответа.
- Если команда не знает ответа, можно передать право ответа следующей команде или использовать подсказку.
- В конце игры подводятся итоги, и определяется команда-победитель.

3. Вариации игры:

- Можно использовать карточки с картинками, связанными с интернетом, и просить детей угадывать, что на них изображено.
- Можно добавить элементы соревнования, например, кто быстрее ответит на вопрос.
- Можно устроить "сражение" между командами, где каждая команда будет защищать свой ответ.

5. Завершение игры:

Подведение итогов, Награждение победителей.

Ход игры:

Здравствуйте ребята, сегодня в нашей школе проходят Единые уроки безопасности в сети «Интернет». В нашем сегодняшнем мероприятии – игре-карусели вспомним все правила безопасности нахождения в интернете через интересные задания. Вы согласны? Тогда начнем. Команды – группы передвигаются по кольцевой системе от волонтера к волонтеру, отвечая на вопросы викторины.

Вопросы для викторины:

- Какие данные не следует публиковать в социальных сетях? (Ответ: номер телефона, домашний адрес, пароли)
- Как узнать, что сайт безопасный? (Ответ: наличие замка в адресной строке, <https://> в начале адреса)
- Что такое "фишинг"? (Ответ: вид мошенничества в интернете, когда злоумышленники пытаются выманить личные данные)
- Как защитить свой аккаунт в социальной сети? (Ответ: придумать сложный пароль, не делиться им ни с кем, включить двухфакторную аутентификацию)
- Что делать, если вам пришло сообщение от незнакомого человека? (Ответ: не отвечать, сообщить о подозрительном сообщении)
- Какие сайты могут быть опасны для детей? (Ответ: сайты с нежелательным контентом, сайты для взрослых)
- Как распознать фейковую новость? (Ответ: проверить источник информации, поискать информацию на других сайтах)
- Что такое "кибербуллинг"? (Ответ: травля в интернете)
- Как вести себя в интернете, чтобы не обидеть других? (Ответ: быть вежливым, уважать чужое мнение)
- Какие правила поведения в интернете вы знаете? (Ответ: не грубить, не обманывать, не распространять слухи)

После завершения выполнения заданий, подсчитываются результаты, во время подведения итогов командам предлагается посмотреть серию «Game Over» из мультфильма «Маша и Медведь».

(Просмотр мультфильма)

Подведение итогов. Объявление результатов. Обмен мнениями. Вручение памяток из «Электронной библиотеки «Информационная безопасность в картинках».



Муниципальное образовательное учреждение
средняя общеобразовательная школа
«Образовательный комплекс имени Б.Н. Богачева»



Центр образования лицей № 2

**Сценарий игровой программы
«Прогулка через ИнтерНетЛес»
для учащихся 7-8 классов**

Рыбинск, 2025

Игра "Прогулка через ИнтерНетЛес" – это квест-игра, предназначенная для школьников 7-10 классов, задания, предлагаемые участникам касаются различных аспектов работы и безопасности в цифровом пространстве.

Цель игры: развитие навыков безопасного использования интернета, распознавание и реагирование на интернет-угрозы.

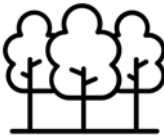
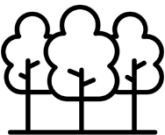
Задачи игры:

- Развивать навыки безопасного использования интернета на основании имеющегося у них опыта, учить связывать навыки повседневного использования интернета и электронных устройств с правилами безопасности.
- Повышать уровень осведомленности детей о наиболее актуальных интернет-угрозах (с учетом возраста аудитории, региона, других факторов), формировать умения противодействовать интернет-угрозам.
- Воспитывать этическую культуру в цифровой среде.

Правила игры:

Участникам предлагается за определенное время пройти 6 дистанций. На каждую дистанцию дается 3 минуты. Команды двигаются в соответствии с маршрутным листом. После успешного выполнения каждого задания участники получают по одной букве из слова, которое мы составим в конце игры.

Маршрутный лист квест «Прогулка через ИнтерНетЛес»

	1	2	3	4	5	6
А	Дистанция «Правила безопасности в сети «Интернет»	Дистанция «Волшебный квадрат» 	Дистанция «Ситуационное задание»	Дистанция «Ребусы» 	Дистанция «Последствия вируса»	Дистанция «Верю – не верю» 
Б	Дистанция «Волшебный квадрат» 	Дистанция «Ситуационное задание»	Дистанция «Ребусы» 	Дистанция «Последствия вируса»	Дистанция «Верю – не верю» 	Дистанция «Правила безопасности в сети «Интернет»
В	Дистанция «Ситуационн ое задание»	Дистанция «Ребусы» 	Дистанция «Последствия вируса»	Дистанция «Верю – не верю» 	Дистанция «Правила безопасности в сети «Интернет»	Дистанция «Волшебный квадрат» 

Задания игры:

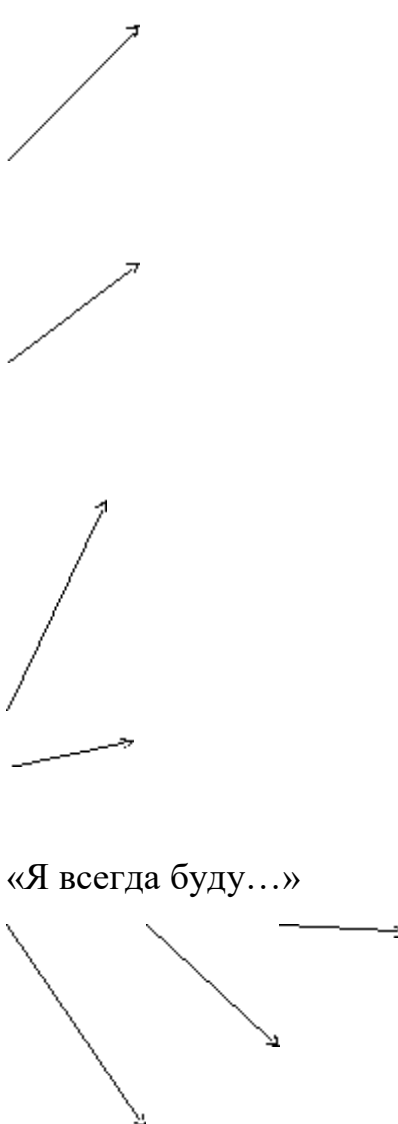
Дистанция «Правила безопасности в сети «Интернет»

Задание. Сопоставьте две колонки при помощи стрелок «Правила безопасности пользования интернетом»

«Я всегда буду...»	Скрывать информацию о себе Обновлять антивирусную программу Выставлять свое настоящее имя, адрес, телефон Покидать нехорошие веб-сайты Хранить свой пароль в тайне Открывать и пересылать «письма счастья» Открывать подозрительные сообщения Вести себя в соцсетях вежливо Общаться в сеть с незнакомыми людьми
--------------------	---

«Я никогда не буду...»	Рассказывать родителям о проблемах в сеть Участвовать в платных играх, конкурсах, лотереях Обижать других людей в соцсетях
-------------------------------	---

Ответ:

 «Я всегда буду...»	Скрывать информацию о себе Обновлять антивирусную программу Выставлять свое настоящее имя, адрес, телефон Покидать нехорошие веб-сайты Хранить свой пароль в тайне Открывать и пересылать «письма счастья»
--	--

 «Я никогда не буду...»	Открывать подозрительные сообщения Вести себя в соцсетях вежливо Общаться в сеть с незнакомыми людьми Рассказывать родителям о проблемах в сеть Участвовать в платных играх, конкурсах, лотереях Обижать других людей в соцсетях
---	--

Дистанция «Волшебный квадрат»

Задание. Найдите в каждой строчке по одному слову, связанное с компьютером, интернетом и обведите овалом.

а	п	к	о	р	у	с	е	т	ь	д	л	о	м	и
к	с	п	а	м	а	в	т	у	к	е	б	ш	г	о
о	з	о	н	и	н	т	е	р	н	е	т	с	м	и
ф	а	й	л	в	о	р	о	н	к	а	т	и	у	р
г	о	л	о	л	е	д	ж	м	в	и	р	у	с	а

а	в	а	б	р	а	у	з	е	р	а	к	е	т	а
а	ц	а	п	л	к	о	м	п	ь	ю	т	е	р	ч
в	б	е	з	о	п	а	с	н	о	с	т	ь	м	и
о	р	е	х	п	о	п	р	о	г	р	а	м	м	а
к	а	д	и	с	к	е	т	а	р	е	л	к	а	т
у	в	о	к	л	а	в	и	а	т	у	р	а	и	ж
н	з	а	в	и	с	и	м	о	с	т	ь	ю	ж	з
н	о	с	о	к	о	т	р	а	с	с	ы	л	к	а

Ответ:

						с	е	т	ь					
	с	п	а	м										
				и	н	т	е	р	н	е	т			
ф	а	й	л											
									в	и	р	у	с	
			б	р	а	у	з	е	р					
					к	о	м	п	ь	ю	т	е	р	
	б	е	з	о	п	а	с	н	о	с	т	ь		
						п	р	о	г	р	а	м	м	а
		д	и	с	к	е	т	а						
			к	л	а	в	и	а	т	у	р	а		
	з	а	в	и	с	и	м	о	с	т	ь			
							р	а	с	с	ы	л	к	а

Дистанция «Ситуационное задание»

Задание. Прочитав ситуацию, дайте письменно правильный ответ.

Ты общаешься в социальной сети со своими друзьями, и тебе приходит сообщение от незнакомого человека: «Привет, классные фото! Только у меня все равно круче! Жми сюда!». Предлагается перейти по ссылке для просмотра фотографий. Как поступить в данной ситуации?

Ответ: _____

Ответ: не переходить по незнакомым подозрительным ссылкам.

Дистанция «Ребусы»

Задание. Разгадайте ребусы и запишите ответ.



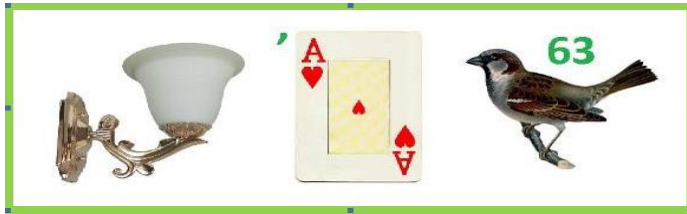
Ответ: ВИРУС



Ответ: ХАКЕР



Ответ: МОДЕМ



Ответ: БРАУЗЕР

Дистанция «Последствия вируса»

Задание. Восстановите из поврежденных слов термины, относящиеся к информатике и компьютеру:

1. КАДСИТЕ -
2. ТИРНРЕП -
3. СЙЖКОТДИ -
4. РАВЛУАТИКА -
5. НОЛИКОК -

Ответы: 1. Дискета, 2. Принтер, 3. Джойстик, 4. Клавиатура, 5. Колонки.

Дистанция «Верю – не верю»

Задание. Прочитайте текст, определите его правдивость.

Поставьте «+», если считаете, что написанное - правда, «-» - ложь.

1. Комедийный театр в Барселоне внедрил новую систему оплаты за смех. В спинки кресел в зрительном зале вмонтированы планшеты с установленной программой по распознаванию мимики. Каждая зафиксированная улыбка стоит 30 евроцентов, а максимальная

стоимость представления установлена в 24 €, то есть после 80-й улыбки можно смеяться бесплатно. Система понравилась как зрителям, количество которых увеличилось, так и администрации театра, чьи доходы выросли.

Ответ: _____

Ответ: ПРАВДА (+)

1. На самом первом логотипе Apple был изображён сэр Исаак Ньютон и яблоня, с которой вот-вот ему на голову упадёт яблоко. Этой эмблемы не было на корпусе компьютера Apple I, только в инструкции к нему. Общая композиция логотипа была сильно перегружена деталями, поэтому менее чем через год его сменил привычный нам надкушенный фрукт.

Ответ: _____

Ответ: ПРАВДА (+)

1. Windows 98 содержит 8 миллионов строк кода.

Ответ: _____

Ответ: ЛОЖЬ (18 миллионов)(-)

1. В Microsoft работает общей сложностью 72 тысячи сотрудников (из них 95% мужчин, и всего 5% женщин), годовой оборот компании только от сетевых проектов составляет 44 миллиарда долларов.

Ответ: _____

Ответ: ЛОЖЬ (75 мужчин и 25 женщин)(-)

1. Все домены, состоящие из любых трех букв, уже зарегистрированы.

Ответ: _____

Ответ: ПРАВДА (+)

1. Специалисты утверждают, что в 2016 году количество сетевых пользователей возможно перевалит за миллиард.

Ответ: _____

Ответ: ЛОЖЬ (в 2005 году перевалило за миллиард)(-)

Подведение итогов игры. Рефлексия, определение победителя.



Муниципальное образовательное учреждение
средняя общеобразовательная школа
«Образовательный комплекс имени Б.Н. Богачева»



Центр образования лицей № 2

**Методические рекомендации
по диагностике компьютерной зависимости у детей и подростков
(по материалам регионального семинара «Безопасная среда как условие
личностного развития подростков» от 26.10.2019 г.г.)**

Рыбинск, 2025

Методические рекомендации для педагогов-психологов по диагностике компьютерной зависимости у детей и подростков

1. Понятие компьютерной зависимости

Зависимость – подчинение другим (другому) при отсутствии самостоятельности, свободы, навязчивое влечение, переходящее в манию (С.И. Ожегов).

Компьютерная зависимость понимается нами как нерациональное интенсивное использование компьютера и электронных гаджетов (смартфон, планшет и др.). Два вида компьютерной зависимости: интернет-зависимость (сетеголизм) и зависимость от компьютерных игр (геймерство).

Интернет-зависимость (сетеголизм) проявляется следующим образом:

информационная перегрузка, «электронное бродяжничество», т.е. компульсивная длительная (многочасовая) навигация по сети без конкретной цели; источником удовольствия служит факт пребывания в сети. Неконтролируемое желание поиска, чтения информации различного рода в сети, просмотра видео, прослушивания музыки. Пользователь получает мультимедийные формы поощрения и стимуляции либо узнавание чего-то нового;

компульсивное применение Интернета, т.е. патологическая привязанность к опосредствованным Интернетом азартным играм, онлайн-аукционам и биржам или электронным покупкам;

сверхпотребность в виртуальном общении (чаты, форумы, социальные сети), зависимость от «кибер-отношений» и возможного установления в ходе общения дружеских отношений или «флирта»;

зависимость от «киберсекса», т.е. от порнографических сайтов в Интернете, от обсуждения сексуальной тематики в чатах или специальных телеконференциях «для взрослых».

Геймерство - зависимость от компьютерных он-лайн и офф-лайн игр.

Понятия компьютерной зависимости нет в Международной классификации болезней – МКБ-10, Руководстве по диагностике и статистике психических расстройств DSM-IV.

Возможные варианты наблюдаемой компьютерной зависимости (по В.Л. Малыгину):

1. Патологическая увлеченность компьютером как одна из форм зависимого поведения - доболезненное расстройство в рамках девиантного (отклоняющегося) поведения.

2. Синдром компьютерной зависимости, за которым скрывается множество других личностных и/или психических расстройств, имеющих определенную принадлежность к тому или иному заболеванию.

3. Компьютерная зависимость (сетеголизм или кибераддикция) как самостоятельное болезненное пристрастие, обусловленное взаимным патогенным влиянием характерологических черт и интернет-среды.

2. Этапы формирования зависимости (по С.В. Молчанову):

1. Этап первых проб к способу действия, улучшающему психическое состояние при фрустрации и сильных негативных переживаниях.
2. Этап систематического обращения к способу.
3. Этап формирования зависимости.
4. Этап личностной деструкции (личностные изменения, изменения образа жизни, десоциализация).

3. Диагностические критерии компьютерной зависимости

Диагностика компьютерной зависимости как расстройства в настоящее время затруднена тем, что до сих пор не существует единой системы критериев, включенных в DSM-IV. Из всех диагнозов, представленных в DSM-IV, наиболее соответствующей сути компьютерной зависимости оказалась игромания.

И. Голдберг - Internet Addiction Disorder (IAD) – расстройство зависимости от интернета, 1995 г. (основа - диагностические критерии для патологии азартных игр). Интернет-зависимость диагностировалась при наличии 3 или более пунктов, выявленных в течение последних 12 месяцев:

1. Толерантность.
 - 1.1. Количество времени, которое нужно провести в Интернет, чтобы достичь удовлетворения, со временем заметно возрастает.
 - 1.2. Если человек не увеличивает количество времени, которое он проводит в Интернет, то эффект заметно снижается.

2. Абстиненция («синдром отмены»).

Наличие двух или более симптомов, которые возникают в период от нескольких дней до одного месяца после прекращения или уменьшения длительности работы в сети:

- психомоторное возбуждение;
- тревога;
- навязчивые мысли об Интернете;
- фантазии или мечты о сети;
- произвольные или непроизвольные «печатающие» движения пальцев рук.

Симптомы, перечисленные в пункте 2, вызывают снижение или нарушение социальной, профессиональной или другой деятельности. Использование Интернета позволяет избежать симптомов «синдрома отмены».

3. Интернет часто используется в течение большего количества времени или чаще, чем было задумано.

4. Существуют постоянное желание или безуспешные попытки прекратить или начать контролировать использование Интернет.

5. Огромное количество времени тратится на деятельность, связанную с использованием Интернета (поиск новых источников информации, организация найденных в Интернете файлов).

6. Значимая социальная, профессиональная деятельность, отдых прекращаются или редуцируются в связи с использованием Интернета.

7. Использование сети продолжается, несмотря на очевидные и осознаваемые социальные и психологические проблемы, связанные с работой в Интернете (депривация сна, проблемы в семье, опоздания в школу, пренебрежение учебой и т.п.).

Концепция И. Голдберга критиковалась за отсутствие подтверждения клиническими данными.

К. Янг, 1996 г. (основа - диагностические критерии для патологического гемблинга), зависимость диагностируется при наличии 5 и более признаков:

1. Чувство охваченности Интернетом («думаете ли Вы о предыдущих он-лайн сеансах и предвкушаете ли последующие»).

2. Потребность постоянно увеличивать время нахождения в сети для получения чувства удовлетворения.

3. Постоянные безуспешные попытки контролировать, урезать или прекращать использование Интернета.

4. Чувство беспокойства, депрессии, раздражительности при попытке сократить или прекратить использование Интернета.

5. Нахождение в сети дольше, чем планировалось.

6. Риск потери значимых отношений, образования из-за нахождения в сети.

7. Ложь членам семьи или другим людям, чтобы скрыть степень вовлеченности в Интернет-активность.

8. Использование Интернета как способа ухода от своих проблем или освобождения от негативных эмоциональных состояний (например, чувства беспомощности, вины, тревоги, депрессии).

В настоящее время надёжность исследований, проведённых К. Янг, ставится под сомнение - по самым усреднённым данным 80% пользователей, из участвовавших в исследовании, диагностировались как зависимые, что свидетельствует о явной гипердиагностике указанного расстройства (по данным Gray & Gray, 2006).

Критерии диагностики компьютерной зависимости М. Орзак (Maressa Hecht Orzack, PhD, 1999):

1. Получение удовольствия, волнения или облегчения за компьютером.

2. Увеличение времени, проводимого за компьютером, и возрастание денежных расходов на компьютерную деятельность.

3. Покупка нового программного и аппаратного обеспечения для компьютера.

4. Изменения настроения вне компьютера/Интернета.

5. Появление тревоги, злости и депрессии вне компьютера/Интернета.

6. Ощущение потери контроля и подавленности вне компьютера/Интернета.

7. Постоянные мысли о компьютере или Интернете вне компьютера/Интернета.

8. Неудачные попытки контролировать время, проводимое за компьютером.

9. Использование компьютера с целью ухода от текущих проблем.

10. Игнорирование своих обязанностей вследствие использования компьютера.

11. Потеря весомых взаимоотношений вследствие использования компьютера.

12. Ложь о количестве времени, проводимом за компьютером/в Интернете.

13. Ложь о деятельности, проводимой за компьютером/в Интернете.

14. Возникновение финансовых трудностей, возникших в результате злоупотребления компьютером / Интернетом.

15. Проблемы на работе или в учебе вследствие компьютерной деятельности.

16. Проблемы со здоровьем вследствие компьютерной деятельности.

Наличие как минимум пяти перечисленных симптомов свидетельствует о наличии компьютерной зависимости.

Критерии интернет-зависимости по А.Е. Войскунскому, 2017 г.:

1. неспособность и нежелание отвлечься от Интернета даже на короткое время;

2. досада и раздражение при невозможности использовать Интернет, навязчивые мысли о возобновлении использования;

3. тенденция к увеличению времени, проводимому в сети;

4. почти навязчивое стремление получать свежую информацию о новинках в Интернете;

5. готовность тратить на обеспечение работы Интернета все большее количество средств, часто в ущерб другим важным покупкам;

6. ложь о количестве времени, проводимом в сети;

7. склонность забывать о других важных делах (работа, учеба, домашние дела, встречи и т.д.);

8. злоупотребление кофе, другими тонизирующими средствами;

9. нежелание принимать критику своего образа жизни от других людей;

10. готовность мириться с разрушением значимых отношений в семье, с друзьями из-за чрезмерного применения Интернета;

11. сокращение или избегание физической активности, оправдывая это необходимостью работы в Интернете;

12. пренебрежение личной гигиеной из-за стремления провести в сети как можно больше времени;

13. драйв (специфический подъем настроения и забывание о доводах в пользу прекращения работы в Интернете).

Близкие принципы, соответствующие общепринятым диагностическим критериям МКБ 10 (Международная классификация болезней) были предложены К. Бэрд, Е. Вульф в 2001 г.:

А. Неадекватная озабоченность использованием Интернета, включающая в себя хотя бы один из следующих пунктов:

1. Охваченность использованием Интернета, которая переживается как непреодолимое состояние;

2. Чрезмерное использование Интернета по длительности превышающее запланированное время.

В. Использование Интернета или озабоченность им вызывает клинически значимое состояние дистресса или нарушения в социальной, профессиональной или других значимых областях жизни.

С. Чрезмерное использование Интернета появляется не только в периоды гипомании или мании и не подходит под описание заболеваний, категоризированных в первой оси.

Последний пункт является попыткой очертить, сузить круг проявлений, специфичных для истинной зависимости от Интернета. Данный критерий предполагает исключение из категории пользователей, которые используют ресурсы Интернета для игры или шоппинга, а также тех, кто демонстрирует проблемное пользование Интернетом в рамках эпизода мании.

Психологические критерии геймерства (С.А. Кулаков, С.А. Фридман):

☐ пассивное взаимоотношение с действительностью, поверхностное восприятие происходящего только на основе внешних признаков; игнорирование сути явлений, цели поступков;

☐ предпочтение искусственной реальности, замена ею всех других ценностей, событий, явлений жизни, которые игнорируются. Использование бегства в искусственную реальность как основного метода решения проблем;

☐ безуспешные попытки сократить пребывание в искусственной реальности, сопровождающееся чувством вины;

☐ поглощение зависимостью всех сил, всей информации от жизни, что приводит к невозможности делать нечто, не связанное с зависимостью;

☐ распад прежних отношений и связей, скрытность, лживость. Смена значимого окружения на новое, взаимодействие с которым осуществляется только для обеспечения выхода в искусственную реальность (массовые ролевые онлайн игры);

☐ в процессе игры настроение существенно улучшается (радость, состояние эйфории), также подростки испытывают положительные эмоции в ситуации «предвкушения» компьютерной игры;

☐ отсутствие контроля над временем, проводимым за играми;

☐ появление чувства гнева, фрустрации при отсутствии возможности поиграть или попытка окружающих прервать игру («синдром отмены»);

□ после игры настроение ухудшается, быстро возвращаясь на исходный уровень, оставаясь на нем до следующего «вхождения» в виртуальный мир.

Обобщая все проявления, характерные для компьютерной зависимости, можно выделить ее *основные признаки*:

невозможность субъективного контроля за использованием компьютера и Интернета и дезадаптация, которая отражает отрицательное влияние его использования на межличностные отношения, здоровье, работу, учёбу, эмоциональное, психологическое состояние, финансовый статус, и др., характерные, впрочем, для любого зависимого поведения.

данный вид деятельности носит *контрпродуктивный (непродуктивный, бесполезный) характер*. В противном случае к зависимым от компьютера следует отнести значительное количество людей, по многу часов в сутки использующих компьютер и Интернет как профессиональный инструмент.

Компьютерная зависимость как болезненное расстройство включает *шесть компонентов, универсальных для всех вариантов аддикций* (R. Brown, 1993; M. Griffiths, 1996):

- 1- особенность, «сверхценность» (salience),
- 2- изменения настроения (mood changes),
- 3- рост толерантности (tolerance),
- 4- симптомы отмены (withdrawal symptoms),
- 5- конфликт с окружающими и самим собой (conflict),
- 6- рецидив (relapse).

4. Обзор методик психодиагностики компьютерной зависимости

В нашей стране наиболее часто используемым тестом для диагностики интернет-зависимого поведения, является тест К. Янг в адаптации В. Лоскутовой.

1. Тест Кимберли Янг на интернет-зависимость, в оригинале – «Internet Addiction Test» - тест на интернет-аддикцию (приложение 1).

Данная тестовая методика разработана и апробирована в 1994 году доктором Кимберли Янг (Kimberley S. Young), профессором психологии Питсбургского университета в Брэтфорде. Тест представляет собой инструмент самодиагностики патологического пристрастия к интернету (вне зависимости от формы этого пристрастия).

Первоначально тест состоял из 8 вопросов на которые нужно было отвечать по принципу Да/Нет. В случае пяти и более положительных ответов респондент считался интернет-зависимым. В настоящее время полная версия опросника состоит из 40 пунктов. На каждый вопрос испытуемый должен дать ответ в соответствии с 5-балльной Шкалой Ликкерта. Баллы по всем вопросам суммируются, определяя итоговое значение. Адаптация опросника для русского языка была произведена В. Лоскутовой.

2. Скрининговая диагностика компьютерной зависимости по методике Л.Н. Юрьевой и Т.Ю. Ботьбот (приложение 2).

При разработке методики авторы руководствовались общими представлениями о зависимом поведении и накопленным опытом диагностики и лечения киберзависимостей. В частности, авторы опирались на критерии диагностики интернет-зависимости И. Голдберга, М. Орзак, описанные выше.

Авторы справедливо указывают на то, что недостатком данных диагностических подходов является их ориентированность на социальную ситуацию США, дихотомичность как ответов (да-нет), так и диагностических суждений (есть зависимость-нет зависимости), снижающих эффективность применения методик.

Авторами была поставлена задача выявления не только сформированной зависимости (II стадия аддикции), но и начальной зависимости (I стадия), и формирующейся (предзависимость, аттачмент).

На основании этого был разработан скрининговый способ диагностики интернет-зависимости. На способ получен патент.

Опросник состоит из 11 утверждений относительно проявлений эмоционального состояния личности за компьютером или в Интернете.

Косвенным образом результаты тестирования позволяют выделить «группу риска» с признаками компьютерной зависимости с целью применения эффективных профилактических программ, которые направлены на предупреждение развития психических и поведенческих расстройств.

Использование данного способа поможет провести скрининг-диагностику компьютерной зависимости, а также одновременно оценить эмоциональное состояние личности, ее волевые свойства, способности к самоконтролю поведения, физическое и психологическое состояние.

3. Тест Г.В. Лозовой на наличие зависимостей.

Тест позволяет диагностировать общую склонность к следующим видам зависимостей: алкогольной, интернет и компьютерной зависимостям, любовной, наркотической, игровой, никотиновой, пищевой, зависимости от межполовых отношений, трудоголизма, телевизионной, религиозной, зависимости от здорового образа жизни, лекарственной, а также общей склонности человека к зависимостям.

На основании результатов тестирования клинический диагноз нельзя поставить, поэтому методика является скорее ориентировочной и показывает общую склонность к той или иной зависимости. Кроме того, в литературе отсутствуют данные о валидации и стандартизации данного теста. Для диагностики некоторых видов зависимости приводится по 3 вопроса, что, на наш взгляд, недостаточно для формулирования каких-либо диагностических предположений. Вызывает сомнение шкала «лекарственная зависимость», баллы по которой начисляются даже за утверждения «в моем доме много медикаментов» или «когда я очень сильно нервничаю, я принимаю успокоительное». Некоторые вопросы сформулированы так, что могут вызвать интерес к наркотикам или алкоголю, ранний интерес к сексуальной

стороне межличностных отношений, показать, что это норма. Например: «По интенсивности ощущений наркотик не может сравниться ни с чем», «Межполовые отношения – это самое большое удовольствие в жизни», «Бывает, что я чуть-чуть перебираю, когда выпиваю».

Мы не приводим в приложении данный опросник, так как считаем, что его использование не только неэффективно, но и чревато негативными последствиями в виде интереса к девиантному поведению.

4. Тест на интернет-зависимость Кулакова С.А. (приложение 3).

Тест состоит из 20 утверждений, представляющих собой модификацию теста К. Янг применительно к детскому и подростковому возрасту. Сведения о валидизации и стандартизации отсутствуют.

5. Тест Такера для экспресс-диагностики игромании, модифицированный и адаптированный для несовершеннолетних Коньгиной И.А. (приложение 4).

Модифицированный тест Такера подходит для взрослых и несовершеннолетних испытуемых. Он может служить инструментом скрининга для выявления группы лиц со склонностью к игромании. Отвечая на опросник, нужно иметь в виду, что информативными по событиям являются только данные последнего года.

Сведения о валидизации и стандартизации отсутствуют.

Чем выше результаты теста, тем сильнее человек увлечен игровым процессом и серьезнее могут быть проблемы. Если испытуемый набрал много баллов и входит в группу риска по игровой зависимости, важно не оставлять этот факт без внимания. Важно помнить, что любое тестирование, в том числе тест Такера, — это только начальный ориентировочный этап выявления лиц со склонностью к зависимому поведению - по нему не ставят диагнозы.

6. Шкала интернет-зависимости Чена - шкала CIAS (приложение 5).

По своим диагностическим критериям тест интернет-зависимости Чена наиболее близок к известным шести диагностическим компонентам, универсальным для всех вариантов аддикций, R. Brown, 1993; M. Griffiths, 1996 (сверхценность, изменения настроения, рост толерантности, симптомы отмены, конфликт с окружающими и самим собой, рецидив. Тест позволяет параллельно измерять специфические симптомы зависимости среди которых: толерантность, симптом отмены, компульсивности и в то же время еще и исключительно психологические аспекты, такие как: способность управлять собственным временем и наличие внутриличностных проблем. Шкала интернет зависимости Чена. Разработчик: S.-H. Chen, 2003 год, Китай:

Тест включает в себя 5 оценочных шкал:

1 Шкала компульсивных симптомов

2 Шкала симптомов отмены

3 Шкала толерантности

4 Шкала внутриличностных проблем и проблем связанных со здоровьем

5 Шкала управления временем

Помимо пошкальной оценки существуют 2 типа надшкальных критериев. Интегральные (ключевые) симптомы непосредственно самой Интернет-зависимости, включающие в себя первые 3 шкалы и критерий негативных последствий использования интернета (последние 2 шкалы). Сумма всех шкал является интегральным показателем –общим показателем наличия интернет зависимого поведения. Таким образом, имея пятиосевую модель, можно не просто диагностировать предполагаемое наличие/отсутствие интернет-зависимого поведения в дихотомическом делении на да/нет, но и качественно определить выраженность тех или иных симптомов характеризующих паттерн зависимого поведения. Особым достоинством теста Чена является его многогранность, способность измерять с нескольких точек единый континуум поведения, связанного с интернет-ресурсами. Сотрудниками факультета клинической психологии МГМСУ Росздрава в 2011 году была произведена апробация данной методики. По результатам авторы сделали заключение о высокой степени надежности и валидности теста.

ВЫВОДЫ

Подводя итог обзору современных диагностических методик, следует отметить их небольшое число, при этом отсутствие данных по стандартизации и валидации для большинства. Поэтому необходимо тщательно ознакомиться с теоретической базой опросника, характеристиками его целевой аудитории. Наиболее валидными представляются методика Чена, методика Л.Н. Юрьевой и Т.Ю. Больбот. Обязательно самостоятельное выполнение методики «на себе» прежде проведения индивидуального или массового тестирования. Важно сказать, что ни одна из представленных методик не снабжена шкалой лжи, поэтому для получения надежных результатов необходим высокий уровень доверительности в общении между психологом-диагностом и тестируемым ребенком, убежденность ребенка в конфиденциальности общения с психологом.

Приведенные методики можно использовать и в работе с родителями, предлагая дать «взгляд на ребенка со стороны».

Также рекомендуется активно использовать метод наблюдения (самостоятельного наблюдения психолога, наблюдения классных руководителей и родителей по заданию психолога) с опорой на описанные в настоящих методических рекомендациях диагностические критерии.



Муниципальное образовательное учреждение
средняя общеобразовательная школа
«Образовательный комплекс имени Б.Н. Богачева»



Центр образования лицей № 2

**Материалы информационных лекториев
для родительской общественности по теме
«Развитие культуры информационной безопасности»
в рамках инновационного проекта
«Академия культуры информационной безопасности участников
образовательных отношений»**

Рыбинск, 2025 год

Лекторий №1 Культура информационной безопасности (март)

Развитие культуры информационной безопасности для родителей включает в себя обучение, выработку правил и совместную работу с детьми по защите их цифровой жизни. Родители должны быть в курсе онлайн-активности детей, обучать их безопасному поведению в интернете и использовать инструменты родительского контроля.

Вот некоторые ключевые аспекты:

Обучение и информирование:

- **Разъяснение рисков:**

Объясните детям, какие опасности подстерегают их в интернете: мошенничество, фишинг, буллинг, нежелательный контент, контакты с незнакомцами.

- **Правила безопасного поведения:**

Научите детей не делиться личной информацией (адресом, номером телефона, фотографиями), не отвечать на сообщения от незнакомцев, не переходить по подозрительным ссылкам, не загружать неизвестные файлы.

- **Создание списка правил:**

Разработайте с детьми список правил поведения в интернете и следите за их соблюдением.

- **Безопасный поиск:**

Объясните, как пользоваться поисковыми системами и как отличать надежные сайты от подозрительных.

- **Парольная безопасность:**

Научите детей создавать надежные пароли и не использовать один пароль для разных аккаунтов.

- **Общение с незнакомцами:**

Объясните, что не стоит доверять незнакомым людям, которые пытаются завязать общение в интернете, и ни в коем случае не встречаться с ними в реальной жизни.

Инструменты и технологии:

- **Родительский контроль:**

Используйте программное обеспечение для родительского контроля, которое позволяет фильтровать контент, ограничивать время, проводимое в интернете, и отслеживать активность ребенка.

- **Антивирусные программы:**

Установите антивирусное программное обеспечение на все устройства, которыми пользуются дети.

- **Блокировка нежелательного контента:**

Используйте средства блокировки нежелательного контента, чтобы ограничить доступ к определенным сайтам.

- **Регулярные обновления:**

Обеспечьте регулярное обновление программного обеспечения на всех устройствах, чтобы устранить уязвимости.

Взаимодействие и поддержка:

- **Открытое общение:**

Создайте атмосферу доверия, чтобы дети могли свободно рассказывать вам о своих проблемах и опасениях в интернете.

- **Участие в жизни ребенка:**

Интересуйтесь онлайн-активностью ребенка, его друзьями в интернете, обсуждайте с ним проблемы, которые он может встретить.

- **Позитивный пример:**

Показывайте детям пример безопасного поведения в интернете.

- **Поддержка и понимание:**

В случае, если ребенок столкнулся с какой-либо проблемой, поддержите его и помогите найти решение.

Помните, что культура информационной безопасности формируется постепенно и требует постоянного внимания и участия родителей.

Лекторий №2 Развитие навыков цифровой гигиены (сентябрь)

Определение термина «информационная безопасность детей» содержится в Федеральном законе № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», регулирующим отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию. Согласно данному закону «информационная безопасность детей» – это состояние защищенности, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию.

В силу Федерального закона № 436-ФЗ информацией, причиняющей вред здоровью и (или) развитию детей, является:

1. информация, запрещенная для распространения среди детей;
2. информация, распространение которой ограничено среди детей определенных возрастных категорий.

К информации, запрещенной для распространения среди детей, относится:

1. информация, побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в т.ч. причинению вреда своему здоровью, самоубийству;
2. способность 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;
3. обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям и животным;
4. отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;
5. оправдывающая противоправное поведение;
6. содержащая нецензурную брань;
7. содержащая информацию порнографического характера.

К информации, распространение которой ограничено среди детей определенного возраста, относится:

1. информация, представляемая в виде изображения или описания жестокости, физического и (или) психического насилия, преступления или иного антиобщественного действия;
2. вызывающая у детей страх, ужас или панику, в т.ч. представляемая в виде изображения или описания в унижающей человеческое достоинство форме ненасильственной смерти, заболевания, самоубийства, несчастного случая, аварии или катастрофы и (или) их последствий;
3. представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;
4. содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

С учетом этого Вам предлагаются правила работы в сети Интернет для различных возрастных категорий, соблюдение которых позволит обеспечить информационную безопасность ваших детей.

Общие правила для родителей

1. Независимо от возраста ребенка используйте программное обеспечение, помогающее фильтровать и контролировать

информацию, но не полагайтесь полностью на него. Ваше внимание к ребенку – главный метод защиты.

2. Если Ваш ребенок имеет аккаунт на одном из социальных сервисов (LiveJournal, blogs.mail.ru, vkontakte.ru и т.п.), внимательно изучите, какую информацию помещают его участники в своих профилях и блогах, включая фотографии и видео.
3. Проверьте, с какими другими сайтами связан социальный сервис Вашего ребенка. Странички Вашего ребенка могут быть безопасными, но могут и содержать ссылки на нежелательные и опасные сайты (например, порносайт, или сайт, на котором друг упоминает номер сотового телефона Вашего ребенка или Ваш домашний адрес)
4. Поощряйте Ваших детей сообщать обо всем странном или отталкивающим и не слишком остро реагируйте, когда они это делают (из-за опасения потерять доступ к Интернету дети не говорят родителям о проблемах, а также могут начать использовать Интернет вне дома и школы).
5. Будьте в курсе сетевой жизни Вашего ребенка. Интересуйтесь, кто их друзья в Интернет так же, как интересуетесь реальными друзьями.

Возраст от 7 до 8 лет

В Интернете ребенок старается посетить те или иные сайты, а возможно и чаты, разрешение на посещение которых он не получил бы от родителей. Поэтому родителям особенно полезны будут те отчеты, которые предоставляются программами по ограничению использования Интернета, т. е. Родительский контроль или то, что вы сможете увидеть во временных файлах. В результате, у ребенка не будет ощущения, что за ним ведется постоянный контроль, однако, родители будут по-прежнему знать, какие сайты посещает их ребенок. Дети в данном возрасте обладают сильным чувством семьи, они доверчивы и не сомневаются в авторитетах. Они любят играть в сетевые игры и путешествовать по Интернету, используя электронную почту, заходить на сайты и чаты, не рекомендованные родителями.

Советы по безопасности в сети Интернет для детей 7-8 лет

1. Создайте список домашних правил посещения Интернета при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения временных норм нахождения за компьютером. Покажите ребенку, что Вы наблюдаете за ним не потому что Вам это хочется, а потому что Вы беспокоитесь о его безопасности и всегда готовы ему помочь.
3. Компьютер с подключением к Интернету должен находиться в общей комнате под присмотром родителей.
4. Используйте специальные детские поисковые машины.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Создайте семейный электронный ящик, чтобы не позволить детям иметь собственные адреса.
7. Блокируйте доступ к сайтам с бесплатными почтовыми ящиками с помощью соответствующего программного обеспечения.
8. Приучите детей советоваться с Вами перед опубликованием какой-либо информации средствами электронной почты, чатов, регистрационных форм и профилей.
9. Научите детей не загружать файлы, программы или музыку без вашего согласия.
10. Не разрешайте детям использовать службы мгновенного обмена сообщениями.
11. В «белый» список сайтов, разрешенных для посещения, вносите только сайты с хорошей репутацией.
12. Не забывайте беседовать с детьми об их друзьях в Интернете, как если бы речь шла о друзьях в реальной жизни.
13. Не делайте «табу» из вопросов половой жизни, так как в Интернете дети могут легко наткнуться на порнографию или сайты «для взрослых».
14. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Оставайтесь спокойными и напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.

Возраст детей от 9 до 12 лет

В данном возрасте дети, как правило, уже слышаны о том, какая информация существует в Интернете. Совершенно нормально, что они хотят это увидеть, прочесть, услышать. При этом нужно помнить, что доступ к нежелательным материалам можно легко заблокировать при помощи средств Родительского контроля.

Советы по безопасности для детей от 9 до 12 лет

1. Создайте список домашних правил посещения Интернет при участии детей и требуйте его выполнения.
2. Требуйте от Вашего ребенка соблюдения норм нахождения за компьютером.
3. Наблюдайте за ребенком при работе за компьютером, покажите ему, что Вы беспокоитесь о его безопасности и всегда готовы оказать ему помощь.
4. Компьютер с подключением в Интернет должен находиться в общей комнате под присмотром родителей.

5. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
6. Не забывайте принимать непосредственное участие в жизни ребенка беседовать с детьми об их друзьях в Интернете.
7. Настаивайте, чтобы дети никогда не соглашались на личные встречи с друзьями по Интернету.
8. Позволяйте детям заходить только на сайты из «белого» списка, который создайте вместе с ними.
9. Приучите детей никогда не выдавать личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
10. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
11. Создайте Вашему ребенку ограниченную учетную запись для работы на компьютере.
12. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам о своих тревогах и опасениях.
13. Расскажите детям о порнографии в Интернете.
14. Настаивайте на том, чтобы дети предоставляли вам доступ к своей электронной почте, чтобы вы убедились, что они не общаются с незнакомцами.
15. Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз.

Возраст детей от 13 до 17 лет

В этом возрасте подростки активно используют поисковые машины, пользуются электронной почтой, службами мгновенного обмена сообщениями, скачивают музыку и фильмы. Мальчикам в этом возрасте больше по нраву сметать все ограничения, они жаждут грубого юмора, азартных игр, картинок «для взрослых». Девочки предпочитают общаться в чатах, при этом они гораздо более чувствительны к сексуальным домогательствам в Интернете. Зачастую в данном возрасте родителям уже весьма сложно контролировать своих детей, так как об Интернете они уже знают значительно больше своих родителей. Тем не менее, не отпускайте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка в Интернете.

Важно по-прежнему строго соблюдать правила Интернет-безопасности – соглашение между родителями и детьми. Кроме того, необходимо как можно чаще просматривать отчеты о деятельности детей в Интернете. Следует обратить внимание на необходимость содержания родительских паролей

(паролей администраторов) в строгом секрете и обратить внимание на строгость этих паролей.

Советы по безопасности в этом возрасте от 13 до 17 лет

1. Создайте список домашних правил посещения Интернета при участии подростков и требуйте безусловного его выполнения. Обговорите с ребенком список запрещенных сайтов («черный список»), часы работы в Интернете, руководство по общению в Интернете (в том числе в чатах).
2. Компьютер с подключением к сети Интернет должен находиться в общей комнате.
3. Не забывайте беседовать с детьми об их друзьях в Интернете, о том, чем они заняты таким образом, будто речь идет о друзьях в реальной жизни. Спрашивайте о людях, с которыми дети общаются посредством служб мгновенного обмена сообщениями, чтобы убедиться, что эти люди им знакомы.
4. Используйте средства блокирования нежелательного контента как дополнение к стандартному Родительскому контролю.
5. Необходимо знать, какими чатами пользуются Ваши дети. Поощряйте использование модерлируемых чатов и настаивайте, чтобы дети не общались в приватном режиме.
6. Настаивайте на том, чтобы дети никогда не встречались лично с друзьями из сети Интернет.
7. Приучите детей не выдавать свою личную информацию средствами электронной почты, чатов, систем мгновенного обмена сообщениями, регистрационных форм, личных профилей и при регистрации на конкурсы в Интернете.
8. Приучите детей не загружать программы без Вашего разрешения. Объясните им, что они могут случайно загрузить вирусы или другое нежелательное программное обеспечение.
9. Приучите Вашего ребенка сообщать вам о любых угрозах или тревогах, связанных с Интернетом. Напомните детям, что они в безопасности, если сами рассказали вам, о своих угрозах или тревогах. Похвалите их и посоветуйте подойти еще раз в подобных случаях.
10. Расскажите детям о порнографии в Интернете. Помогите им защититься от спама. Научите подростков не выдавать в Интернете своего реального электронного адреса, не отвечать на нежелательные письма и использовать специальные почтовые фильтры.
11. Приучите себя знакомиться с сайтами, которые посещают подростки.
12. Научите детей уважать других в интернете. Убедитесь, что они знают о том, что правила хорошего поведения действуют везде — даже в виртуальном мире.
13. Объясните детям, что ни в коем случае нельзя использовать Сеть для хулиганства, распространения сплетен или угроз другим людям.

14. Обсудите с подростками проблемы сетевых азартных игр и их возможный риск. Напомните, что дети не могут играть в эти игры согласно закону.

Постоянно контролируйте использование Интернета Вашим ребенком! Это не нарушение его личного пространства, а мера предосторожности и проявление Вашей родительской ответственности и заботы.

Лекторий № 3 Как уберечься от недостоверной информации (декабрь)

Данные рекомендации экспертов – это практическая информация для родителей, которая поможет предупредить угрозы и сделать работу детей в Интернете полезной.

Интернет предлагает колоссальное количество возможностей для обучения, но есть и большая доля информации, которую никак нельзя назвать ни полезной, ни надежной. Пользователи Сети должны мыслить критически, чтобы оценить точность материалов; поскольку абсолютно любой может опубликовать информацию в Интернете. Это относится и к детям, которые склонны думать: «Раз в Интернете – значит, правильно». У газет или журналов есть проверяющие люди: корректор и редактор. Но Интернет не сможет проверить, насколько правдива размещенная информация. Неверно представление о том, что где-то существует безопасный Интернет. Надо помнить, что большинство ресурсов создается с коммерческой целью, и здесь реализуются чьи-то цели.

Правило 1. Внимательно относитесь к действиям ваших детей в «мировой паутине»: Не отправляйте детей в «свободное плавание» по Интернету. Старайтесь активно участвовать в общении ребенка с Интернет, особенно на этапе освоения. Беседуйте с ребенком о том, что нового для себя он узнает с помощью Интернет, чтобы вовремя предупредить угрозу.

Правило 2. Информировать ребенка о возможностях и опасностях, которые несет в себе сеть: Объясните ребенку, что в Интернете как в жизни встречаются и «хорошие», и «плохие» люди. Объясните, что если ребенок столкнулся с негативом или насилием от другого пользователя Интернет, ему нужно сообщить об этом близким людям. Научите ребенка искать нужную ему информацию и проверять ее, в том числе с вашей помощью. Научите ребенка внимательно относиться к скачиванию платной информации и получению платных услуг из Интернет, особенно путем отправки sms, – во избежание потери денег. Сформируйте список полезных, интересных, безопасных ресурсов, которыми может пользоваться ваш ребенок, и посоветуйте их использовать.

Правило 3. Выберите удобную форму контроля пребывания вашего ребенка в Сети: Установите на ваш компьютер необходимое программное

обеспечение – решение родительского контроля и антивирус. Если ваш ребенок остается часто дома один, ограничьте время пребывания вашего ребенка в Интернете. Если компьютер используется всеми членами семьи, установите его в месте, доступном для всех членов семьи, а не в комнате ребенка. Создавайте разные учетные записи на вашем компьютере для взрослых и детей. Это поможет не только обезопасить ребенка, но и сохранить ваши личные данные. Регулярно отслеживайте ресурсы, которые посещает ваш ребенок. Простые настройки компьютера позволят вам быть в курсе того, какую информацию просматривал Ваш ребенок.

Правило 4. Регулярно повышайте уровень компьютерной грамотности, чтобы знать, как обеспечить безопасность детей: Используйте удобные возможности повышения уровня компьютерной и Интернет грамотности, например, посещение курсов, чтение специальной литературы, консультации с экспертами.

Об информационной безопасности подростков

Для обеспечения безопасности в интернете подросткам следует соблюдать ряд правил. Нельзя делиться личной информацией (имя, адрес, номер телефона, пароли) с незнакомыми людьми, а также нужно быть осторожным с размещением фотографий и видео. Важно помнить, что не все, что видишь в интернете, является правдой, и нужно критически относиться к информации. Нельзя отвечать на спам и открывать файлы от неизвестных отправителей. Необходимо избегать общения с навязчивыми незнакомцами и не встречаться с виртуальными друзьями без сопровождения взрослых. Следует использовать сложные пароли и не сообщать их никому, а также не использовать один пароль для разных аккаунтов. В случае возникновения проблем, угроз или неприятных ситуаций, необходимо сообщить об этом взрослым.

Вот более подробные правила:

1. Защита личной информации:

- Нельзя размещать в интернете персональную информацию, такую как имя, адрес, номер телефона, адрес электронной почты, фотографии и другую личную информацию.
- Нельзя делиться личной информацией со случайными или незнакомыми людьми в интернете.

- Нельзя публиковать фотографии и видео, которые могут быть использованы против вас.
- Всегда будьте осторожны с тем, что вы публикуете в социальных сетях и на других платформах.

2. Осторожность в общении:

- Нельзя отвечать на спам и открывать файлы от незнакомых отправителей.
- Нельзя добавлять в друзья или общаться в чатах с незнакомыми людьми, не проверив их личность.
- Нельзя встречаться с виртуальными друзьями в реальной жизни без сопровождения взрослых.
- Если вас кто-то беспокоит или угрожает в интернете, немедленно сообщите об этом взрослым.

3. Критическое отношение к информации:

- Не все, что вы видите в интернете, является правдой.
- Нужно критически относиться к информации и перепроверять ее на других источниках.
- Нельзя доверять всей рекламе и акциям, которые вы видите в интернете.

4. Безопасность паролей и устройств:

- Используйте сложные пароли, состоящие из букв, цифр и символов, и не используйте один и тот же пароль для разных аккаунтов.
- Нельзя сообщать свои пароли никому, даже друзьям и родственникам.
- Обновляйте программное обеспечение и антивирусные программы на своих устройствах.
- Не скачивайте файлы и программы с непроверенных сайтов.

5. Правила поведения в социальных сетях:

- Нельзя оскорблять других пользователей и участвовать в травле.

- Нельзя публиковать чужие фотографии без разрешения.
- Нельзя использовать нецензурную лексику и грубить.
- Нужно соблюдать правила этикета в интернете, как и в реальной жизни.

6. Обращение за помощью:

- Если у вас возникли проблемы или вопросы, обратитесь за помощью к взрослым (родителям, учителям, другим доверенным лицам).
- Не бойтесь рассказывать взрослым о своих проблемах в интернете, они помогут вам.

Безопасность ребенка в Интернете. Памятка родителям.



Полезные цифровые ресурсы для родителей по теме «Развитие культуры информационной безопасности»

Интернет – ресурсы:

- http://www.symantec.com/ru/ru/norton/clubsymantec/library/article.jsp?aid=c_s_teach_kids – Club Symantec единый источник сведений о безопасности в Интернете. Статья для родителей «Расскажите детям о безопасности в Интернете». Информация о средствах родительского контроля.
- <http://www.oszone.net/6213/> – OS.zone.net: Компьютерный информационный портал. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль».

Информационные материалы:

[ПАМЯТКА № 1 Для родителей об информационной безопасности для детей](#)

[ПАМЯТКА № 2 Общие правила для родителей](#)

[«Безопасность детей в Интернете»](#) – компания Microsoft. Информация для родителей: памятки, советы, рекомендации.

[«Безопасно и просто: родительский контроль»](#). Буклет.

[Дети в Интернете. Советы и рекомендации родителям](#). Брошюра МТС.

[Глобальная сеть: правила пользования](#) Как защитить ребенка от столкновения с вредоносной информацией в сети? Как научить его справляться с последствиями таких встреч? Рекомендации для родителей. МТС.

Онлайн –урок [Советы по безопасности в сети интернет](#) Учи.ру для родителей
https://vk.com/video-61888001_456239698



Муниципальное образовательное учреждение
средняя общеобразовательная школа
«Образовательный комплекс имени Б.Н. Богачева»



Центр образования лицей № 2

**Комплексное образовательное событие
«День безопасной информации»**

Рыбинск, 2025 год

Комплексное образовательное событие по организации информационной безопасности «День безопасной информации» – это тематическая неделя, направленная на повышение осведомленности учащихся разного возраста, родителей и педагогов о правилах безопасного поведения в сети Интернет и защиты личных данных.

Все мероприятия тематической недели формируют у участников культуру информационной безопасности.

Культура информационной безопасности — это совокупность знаний, навыков, принципов и ценностей, которые формируют безопасное поведение людей в информационном пространстве.

Комплексное образовательное событие «День безопасной информации» проводится ежегодно и является ключевым событием III четверти (2-3-я декада марта месяца) учебного года.

Целевая аудитория: обучающиеся 1-11 классов лицея, педагоги, выпускники, родители, социальные партнеры.

Цель образовательного события: повышение осведомленности учащихся, родителей и педагогов о правилах безопасного поведения в сети Интернет и защиты личных данных, сохранение лицейских традиций.

Задачи:

1. способствовать формированию культуры ответственного, этичного и безопасного использования информационных технологий;
2. способствовать повышению уровня осведомленности о рисках и угрозах в информационной среде;
3. создавать условия для формирования навыков критического мышления при работе с информацией;
4. содействовать повышению самооценки и созданию ситуаций успеха в рамках публичных выступлений школьников.
5. расширять возможности знакомства обучающихся с позитивным контентом в сети Интернет, в том числе, способствующим их развитию и образованию ответственного поведения в сети Интернет.

Основные направления Комплексного образовательного события:

- **Ознакомление с правилами безопасного поведения в сети:**

Учащиеся узнают о видах угроз в интернете, таких как фишинг, мошенничество, кибербуллинг, а также о способах защиты от них.

- **Формирование навыков критического мышления при работе с информацией:**

Учащиеся учатся анализировать информацию, отличать фейки от правдивых новостей, оценивать достоверность источников.

- **Обучение основам информационной безопасности:**

В рамках недели проводятся тренинги и мастер-классы по настройке паролей, использованию антивирусного ПО, резервному копированию данных.

Реализация события проводится по следующему плану: программа Комплексного образовательного события «День безопасной информации» включает мероприятия разного формата: уроки безопасности, классные часы, радиолинейки, лекции с социальными партнерами, квесты, информационные десанты, выставки творческих работ.

Формы организации:

- **Классные часы:**

Обсуждение правил безопасности в интернете, разбор конкретных ситуаций, просмотр видеороликов и презентаций.

- **Уроки безопасности:**

Занятия, направленные на изучение основных понятий информационной безопасности и практическое применение полученных знаний.

- **Родительские собрания:**

Обсуждение вопросов безопасности детей в интернете, обмен опытом и рекомендациями.

- **Конкурсы и викторины:**

Творческие задания, направленные на закрепление знаний по информационной безопасности.

- **Квест-игры:**

Интерактивные игры, в которой учащиеся выполняют задания, связанные с информационной безопасностью.

- **Лекторий для родителей:**

Родители получают информацию о том, как защитить детей от опасностей в интернете, как контролировать их время в сети и какие ресурсы использовать для обучения детей основам информационной безопасности.

Мероприятия Комплексного образовательного события «День безопасной информации»

дата	день недел и	Время и место проведения	Название мероприятия/участники	Организатор	Аннотация
17.03.2025	пн	08.00-8.05 радио лица	Радиолинейка Открытие тематической недели «День безопасной информации»/ 1-11 классы	куратор медиа центра	Освещение событий тематической недели
17.03.2025	пн	по плану класса	Тематическое занятие «Что можно и нельзя в Сети Интернет»/ 5-11 классов	классные руководители 1-11 классов	Тематическое занятие способствует формированию у обучающихся представлений о правилах безопасного поведения в сети
Тематический день: первичного отделения Движения 1					
17.03.2025	пн	17.03.2025 11.50-12.30 – 5 классы 12.30-13.20 – 6 классы	Игра – карусель «На просторах Интернета»/5-6 классы	инициативная группа ПО Движение 1, педагог- организатор	Игра способствует повышению уровня осведомленности о рисках и угрозах в информационной среде
18- 19.03.2025	вт	18.03.2025 13.30-14.30 – 7 классы, 19.03.2025 13.30-14.30 – 8 классы	Квест-игра «Прогулка через ИнтерНетЛес»/7-8 классы	инициативная группа ПО Движение 1, советник по воспитанию	Образовательное событие способствует формированию навыков цифровой гигиены

18.03.2025	вт	10.30-10.50 центр детских инициатив	Консультация «Виртуальная реальность. Как обезопасить себя»	советник по воспитанию	Повышение цифровой культуры несовершеннолетних
19.03.2025	ср	10.30-10.50 центр детских инициатив	Викторина «Что я знаю о безопасной работе в Интернете»	педагог-организатор	Повышение цифровой культуры несовершеннолетних
Тематический день кафедр естественно-научного направления					
19.03.2025	ср	в течение дня	Информационные десанты «Интернет и мое здоровье»/5-7 классы	учителя биологии, инициативная группа	Информационные десанты проводят старшеклассники: простым языком ведется рассказ о правилах работы за компьютером и пользовании смартфоном.
19.03.2025	ср		Урок безопасности: «Интернет – современная среда обитания. Безопасность в среде» /8-11 классы	учителя биологии, географии, инициативная группа	В ходе урока безопасности обсуждаются проблемы информационной безопасности, создаются условия для повышения цифровой культуры обучающихся.
Тематический день кафедры математических дисциплин					
18-20.03.2025	вт-чт	12.30-13.20, каб. информатики	Интерактивная игра «Интернет среди нас»	учитель информатики, инициативная группа обучающихся	Игра-конкурс по медиабезопасности

Тематический день в информационно-библиотечном центре					
17.03.2025	пн	09.50-10.30	Библиотечный урок «Интернет как источник информационных ресурсов»	библиотекарь	Повышение информационной культуры школьников
21.03.2025	ср	в течение дня	Анкетирование учащихся по теме «Безопасность в Интернете»	педагог-психолог	Изучение представлений школьников о сформированных навыках грамотного, безопасного и безопасного поведения в сети Интернет и защиты личных данных
Тематический день кафедр гуманитарного цикла					
19.03.2025	ср	в рамках уроков права /обществознания	Урок безопасности: «Правовая азбука юного интернет-пользователя» /5-7 классы	учителя истории, права и обществознания, обучающиеся 10 классов	В ходе урока безопасности обсуждаются проблемы информационной безопасности, создаются условия для повышения цифровой культуры обучающихся.
20.03.2025	чт	в рамках уроков права /обществознания	Информационные десанты «Безопасный Интернет и социальные сети» 8-10 классы	учителя истории, права и обществознания, обучающиеся 11 классов	Информационные десанты проводят старшеклассники: обсуждаются правила пользования социальными сетями и мессенджерами
Тематический день кафедры художественно-эстетических дисциплин и физического воспитания					
22.03.2025	сб	10.50-11.30	Презентация выставки детского творчества «Социальный	куратор выставки,	Выполнение творческих работ, посвященных правилам

			плакат: Интернет и моя будущая профессия» 5-6 классы	администрация	безопасного поведения в цифровой среде
21.03.2025	пт	в течение дня	Конкурс детского рисунка «Интернет и я – друзья навсегда» (1-4 классы)	учителя ИЗО, кураторы ВУД	Выполнение творческих работ, посвященных правилам безопасного поведения в цифровой среде
20.03.2025	чт	в течение дня	Выставка буклетов «БезОпасный и пОлезный» (7-9 классы)	учитель труда, ИЗО	Выполнение творческих работ, посвященных правилам безопасного поведения в цифровой среде
Тематический день Большого ученического совета					
21.03.2025	пт	08.00-08.40	Круглый стол «Виртуальное предложение – реальные последствия: действия виртуальные, ответственность - реальная»	заместитель директора по ВР, с приглашением сотрудников МУ МВД «Рыбинское»	Информационное просвещение несовершеннолетних о возможностях защиты от информации, причиняющей вред здоровью и развитию детей
Информационное просвещение родителей о возможности защиты детей от информации, причиняющей вред их здоровью и развитию					
17.03.2025	пн	17.00-18.00	Консультация «Профилактика игровой и компьютерной зависимости детей и подростков»	педагог-психолог	Содействие в профилактике игровой и компьютерной зависимости детей и подростков
19.03.2025	чт	17.30-18.30 актовый зал	Родительский лекторий «Профилактика у детей и подростков игровой зависимости и правонарушений	администрация с участием социальных	Повышение грамотности родителей (законных представителей) по проблемам информационной

			с использованием цифровых технологий»	партнеров	безопасности детей и подростков
17-22.03.2025	пн-сб	в течение недели	Публикация материалов по защите детей от противоправного контента в образовательной среде	администратор сайта	Размещение на сайте образовательной организации и на паблике материалов по проблемам информационной безопасности для всех участников образовательного процесса.
22.03.2025	сб	11.30-12.00	Закрытие тематической недели	администрация	Награждение активных участников, победителей, призеров, волонтеров тематической недели

Ожидаемые результаты тематической недели:

- Повышение уровня осведомленности о рисках и угрозах в информационной среде среди участников образовательных отношений.
- Сформирована культура ответственного и безопасного поведения в сети Интернет.
- Приобретены навыки защиты личных данных и конфиденциальной информации.
- Сформированы навыки критического мышления при работе с информацией.