Министерство спорта и молодежной политики Республики Бурятия
ГАУ ДПО РБ «Бурятский республиканский институт образовательной политики»
Кафедра воспитания, психологии и дополнительного образования

# УРОКИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБУЧАЮЩИХСЯ СТАРШЕЙ ШКОЛЫ РЕСПУБЛИКИ БУРЯТИЯ (МЕТОДИЧЕСКОЕ ПОСОБИЕ)

Улан-Удэ
2024

**УДК 371.4.485**
**ББК 78.07**
**У-71**

Обсуждено на заседании кафедры воспитания, психологии и дополнительного образования КВПиДО

Одобрено на заседании Научно-методического совета ГАУ ДПО РБ «БРИОП»

**Составитель:**
Сандабкина Т. Б., к.п.н., доцент, зав. кафедрой воспитания, психологии и дополнительного образования ГАУ ДПО РБ «БРИОП»

**Рецензенты:**

Буртонова И. Б., к.п.н., доцент Центра непрерывного повышения профессионального мастерства ГАУ ДПО РБ «БРИОП»

Федоров Н.П., зам.директора МАОУ «Гимназия № 14» г. Улан-Удэ

**Оглавление**

**Пояснительная записка**

Настоящие материалы рекомендованы в помощь в практической деятельности для проведения уроков, классных часов по вопросам информационной безопасности обучающихся школ для администрации общеобразовательных учреждений, специалистам, педагогам, классным руководителям. Разработки уроков ориентированы на проведение уроков по информационной безопасности школьников и безопасному поведению в сети Интернет и отражает актуальные вопросы безопасной работы с персональной информацией, сообщениями и звонками по мобильному телефону, электронной почтой, информационными и коммуникационными ресурсами в сети Интернет, доступа к ресурсам для досуга, поиска новостной, познавательной, учебной информации, общения в социальных сетях, получения и передачи файлов, размещения личной информации в коллективных социальных сервисах.

В основе пособия отражены практические рекомендации и разработки уроков ФГБНУ Институт изучения детства, семьи и воспитания РАО, Центр цифровой трансформации образования ГУ ДПО «ИРО Забайкальского края», МБУ «Центр психолого-педагогической, медицинской и социальной помощи» г. Пермь, Лаборатория знаний.

Данный материал для администрации общеобразовательных учреждений, специалистов, педагогов, классных руководителей - качественный инструмент формирования у детей и подростков культуры безопасного поведения в сети, отвечающий современным требованиям, методическим решениям и проверенной экспертами федерального уровня информацией.

## УЧЕБНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ УРОКОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

### Учебно-тематическое планирование для 10 класса
### Вариант 1[1]

| № | Название | Количество часов |
|---|---|---|
| 1 | «Безопасность в Интернете. Обучение навыкам поведения в Интернете» | 2 |
| 2 | «Безопасность в сети Интернет. Формирование навыков безопасного и ответственного поведения в сети» | 2 |
| 3 | «Безопасный Интернет: опасные угрозы и методы борьбы с ними» | 2 |
| 4 | «Безопасность в сети Интернет» | 2 |
| 5 | «Безопасность в сети Интернет: правила пользования» | 2 |
| 6 | «Чтобы я делал, если б не было сети Интернет» | 2 |
| | Итого | 12 |

### Учебно-тематическое планирование для 11 класса

| № | Название | Количество часов |
|---|---|---|
| 1 | «Безопасность в Интернете» | 2 |
| 2 | «Безопасный Интернет» | 2 |
| 3 | «Урок медиабезопасности. «Предупреждён – значит вооружён» | 2 |
| 4 | «Информационная безопасность» | 2 |
| 5 | «Безопасность в сети Интернет» | 2 |
| 6 | «Безопасность в сети Интернет. Нормы поведения в сети» | 2 |
| 7 | «Моя безопасность в сети» | |
| | Итого | 14 |

## УЧЕБНО-ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ УРОКОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» (вариант 2) [3]

| Модуль | Параграфы в учебном пособии | Всего часов | Теоретические занятия | Практическая работа на компьютере |
|---|---|---|---|---|

| Раздел 1 | | | | |
|---|---|---|---|---|
| Модуль 1. Правовые основы информационной безопасности | Глава 1. Понятия юридической ответственности за правонарушения в области информационной безопасности | 5 | 2 | 3 |
| 1.1. Понятия юридической ответственности за право-нарушения в области информационной безопасности | 2. Основные документы в области информационной безопасности Российской Федерации<br>3. Информация как объект правовых отношений<br>4. Функции, принципы и виды юридической ответственности.<br>5. Субъективная и объективная стороны юридической ответственности | 3 | 2 | 1 |
| 1.2. Контрольное занятие | Подготовка презентации по теме в группах учащихся | 2 | | 2 |
| Модуль 2. Законодательство Российской Федерации о гражданско-правовой ответственности в сфере инфобезопасности | Глава 2. Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации) | 7 | 3 | 4 |
| 2.1.Законодательство Российской Федерации о гражданско-правовой ответственности | 1. Общие положения законодательства Российской Федерации о гражданско-правовой ответственности.<br>2. Порядок привлечения несовершеннолетних к гражданско-правовой ответственности за проступки в области информационной безопасности (защиты информации) | 3 | 2 | 1 |
| 2.2.Гражданско-правовая ответственность несовершеннолетних за проступки в области информационной безопасности (защиты информации) | 1. Ответственность за проступок в области присвоение авторства (плагиат)<br>2. Ответственность за проступок за оскорбления, в том числе в социальных сетях | 3 | 1 | 2 |
| 2.3. Контрольное занятие | Индивидуальный зачет | 1 | | 1 |
| Модуль 3. Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности | Глава 3. Административная ответственность за проступки в области информационной безопасности (защиты информации) | 12 | 6 | 6 |

| | | | | |
|---|---|---|---|---|
| 3.1.Понятие административной ответственности | 1. Административное правонарушение. Основные понятия административного правонарушения.<br>2. Особенности административной ответственности несовершеннолетних. | 2 | 1 | 1 |
| 3.2. Административная ответственность несовершеннолетних граждан за проступки в области информационной безопасности (защиты информации). | 1. Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение<br>2. Ответственность за проступок — за оскорбления, в том числе в социальных сетях<br>3. Ответственность за проступок — ложный вызов экстренных служб<br>4. Ответственность за проступок — пропаганду в Интернете наркотических и психотропных веществ<br>5. Ответственность за проступок — нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные)<br>6. Ответственность за проступок — нарушение правил защиты информации<br>7. Ответственность за проступок — представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство<br>8. Ответственность за проступок — за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт<br>9. Ответственность за проступок — нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации | 9 | 5 | 4 |
| 3.3. Контрольное занятие | Индивидуальный зачет | 1 | | 1 |
| Модуль 4. Законодательство Российской Федерации об уголовной ответственности в сфере инфобезопасности | Глава 4. Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации) | 14 | 7 | 7 |
| 4.1. Понятие уголовной ответственности | 1. Уголовный кодекс Российской Федерации<br>2. Виды наказаний в области уголовной ответственности | 2 | 1 | 1 |

| | | | | |
|---|---|---|---|---|
| 4.2. Уголовная ответственность несовершеннолетних за преступления в области информационной безопасности (защиты информации) | 1. Ответственность за преступления в области компьютерной информации и применения компьютеров<br>2. Ответственность за преступления в области присвоения авторства (плагиат)<br>3. Ответственность за преступления в области нарушения авторских прав на лицензионное программное обеспечение<br>4. Ответственность за преступления в области мошенничества (обмана)<br>5. Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений<br>6. Ответственность за преступления — за проведение скрытой (негласной) аудиозаписи<br>7. Ответственность за преступления — за заведомо ложное сообщение о теракте<br>8. Ответственность за преступления — за неприкосновенности частной жизни (тайна общения и творчества, дневников, личных бумаг)<br>9. Ответственность за преступления — за мошенничество в сфере компьютерной информации<br>10. Ответственность за преступления — за незаконное распространение порнографических материалов<br>11. Ответственность за преступления — за заведомо ложный донос | 11 | 6 | 5 |
| 4.3. Контрольное занятие | Индивидуальный зачет | 1 | | 1 |
| Всего по разделу 1 | Модули 1–4 | 33 | 18 | 15 |
| | | | | Практическая работа на компьютере |
| Часы самостоятельной работы | Самостоятельная работа для индивидуальных зачетов и подготовки презентаций (предоставляется в компьютерной форме) | 5 | | 5 |
| Итого | Раздел 1 | 38 | 18 | 20 |
| Раздел 2 | | | | |
| Модуль 5. Практика применения правил и норм информационной безопасности | Глава 5. Проектные задания | 28 | 6 | 22 |

| | | | | |
|---|---|---|---|---|
| 5.1. Проектная работа. Нормативные основы лицензионных соглашений | 1. Лицензионное соглашение свободного ПО Линукс.<br>2. Как купить лицензию на платную антивирусную программу.<br>3. Что такое СС лицензия.<br>4. Обзор свободного антивирусного ПО и его возможности по антиспаму и шлюзованию | 3 | 2 | 2 |
| 5.2. Проектная работа. Практика соблюдения норм инфобезопасности в личном информационном пространстве | 1. Как задавать безопасный пароль. Настройки телефона, планшета для защиты от несанкционированного доступа.<br>2. Защита персональных данных. Обзор. Личный контент в облаке и система его защиты | 3 | 2 | 2 |
| 5.3. Самостоятельная дистанционная работа | Онлайн-курс «Основы информационной безопасности» | 15 | | 15 |
| 5.4 Контрольное занятие | Тест по онлайн курсу | 1 | | 1 |
| Всего по разделу 2 | Модуль 5 | 24 | 4 | 20 |
| Резерв к разделу 2 | | 4 | 2 | 2 |
| Итого | Раздел 2 | 28 | 6 | 22 |
| Всего часов по курсу (разделы 1 и 2) | За два года обучения (1 час в неделю) За один год обучения (2 часа в неделю) | 66 | 24 | 42 |

**МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ**
**ДЛЯ УРОКОВ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»**
**РАЗРАБОТКИ УРОКОВ ДЛЯ ОБУЧАЮЩИХСЯ 10-Х КЛАССОВ** [1]

**Урок № 1 «Безопасность в сети Интернет. Обучение навыкам поведения в Интернете»**

Цель: обучение навыкам поведения в Интернет сети, навыкам уверенного поведения (умение сказать: «Нет!»), развитие способности к стрессоустойчивости, поиск и использование внутренних ресурсов.
Задача: защитить детей от информации, распространяемой в сети Интернет, причиняющей вред их здоровью, физическому, психическому, духовному и нравственному развитию.
Вступительное слово ведущего (1 минута).
Мы живем в век информационных технологий, достаточно много времени проводим в сети в поисках информации, готовясь к занятиям, или просто отдыхая. Мы общаемся с друзьями в социальных сетях, участвуем в дискуссиях, обсуждаем новости, оставляем комментарии, выкладываем фотографии. Мы получили доступ к практически любой информации, хранящейся на миллионах компьютерах во всем мире. Но, с другой стороны, миллионы компьютеров получили доступ к вашему компьютеру, а, значит, к каждому из вас. И не сомневайтесь, они пользуются этой возможностью. И никогда-то, а прямо сейчас. Поэтому очень важно научиться правильно вести себя в сети Интернет, знать правила безопасности и этичного поведения. Сегодня мы с вами об этом и поговорим.
Ведущий задает участникам вопрос: «Как вы считаете подвергаетесь ли вы опасности, когда пользуетесь интернетом? Если да, то какой?»
Ответы фиксируются на доске. Резюме.
Упражнение № 1 «Игра «Весы».
Работа в мини группах по 3-5 чел.
Участникам группы необходимо, привести по 7-10 примеров положительных и отрицательных возможностей интернета.
Выступления групп, резюме, рефлексия.
Интернет – это безграничный мир информации. Он дал людям много положительных возможностей:
- главное преимущество этого ресурса – огромные возможности поиска разнообразной информации.
- коммуникативные возможности (расстояние между людьми сегодня резко сократилось, появилось больше возможностей для общения, быстрого обмена информацией);
- развлекательные (игры, видео и т.д.).
Однако, кроме хорошего, в виртуальном мире присутствует много негативного.
- Мошенничество (доступ к паролям, конфиденциальной информации и т.д.)
- Появление интернет-зависимости (интернет-сёрфинг, пристрастие к виртуальному общению и к виртуальным знакомствам)
- Так же существует риск Вовлечение в деструктивные группы (экстремистские, сектантсткие, аутоагрессивные, антироссийский антисемейные)
- Негативные интернет-явления (кибербуллинг, троллинг и др.)
Упражнение 2. «Что такое аффирмация»

Для выполнения задания ведущий объясняет ребятам понятие «аффирмация», «мотиватор», «демотиватор».

Аффирмация (от лат. affirmatio — подтверждение) — краткая фраза, содержащая вербальную формулу, которая при многократном повторении закрепляет требуемый образ или установку в подсознании человека, способствуя улучшению\ухудшению его психоэмоционального фона и стимулируя положительные\отрицательные перемены в жизни.

Мотиватор - то, что мотивирует, побуждает человека к определённому поведению

Демотива́тор (демотивационный постер) — разновидность настенного плаката. Демотиватор пародирует мотиваторы (плакаты, предназначенные для создания рабочего настроения), используя схожие с мотиваторами изображения, но с подписями, формально направленными на создание атмосферы обречённости и бессмысленности человеческих усилий.

Формат демотиватора включает базовое изображение в рамке, обрамлённое относительно широкими, чаще всего чёрными, полями и снабжённое по нижнему более широкому полю лозунгом, выполненным крупным белым или жёлтым шрифтом. Помимо слогана многие демотивационные постеры содержат текст-пояснение, выполненное мелким шрифтом, так или иначе оттеняющее смысловое наполнение изображения и/или слогана.

Ведущий показывает картинки «демотиваторы» и предлагает преобразовать их в мотиваторы

Например:

| Демотиватор | Мотиватор |
|---|---|
|  |  |
| - *Во всем виновато осень…* | - *Какая классная все-таки весна!*<br>- *Ты что! У всех осень.* |
| | - *Мне все-равно, что у всех. Весна,*<br>*говорю, классная* |

Упражнение 3. «Создай свой мотиватор»

Для выполнения задания ведущий вводит понятие «самопомощь».

Далее ведущий предлагает, воспользовавшись своими телефонами, планшетами, выбрать фотографию, которая служит напоминанием о самом счастливом моменте жизни (можно предложить нарисовать на листе бумаги предмет, сюжет, явление природы и т.п.). Ребята вспоминают когда было сделано это фото, почему именно этот сюжет напоминает о счастье, насколько сильными были эмоции в тот момент. Затем участникам предлагается придумать фразу (вспомнить цитату), которая бы отражала это эмоциональное состояние.

В конце упражнения ведущий дает домашнее задание: оформить на компьютере свой мотиватор и разместить его на своей социальной страничке.

Упражнение 4. «Придумай предложение»

Предлагалось выполнить еще одно упражнение, которое помогает переключить свои эмоции с негативных на позитивные.

Учащимся предлагается несколько цепочек слов: «учеба — желание — успех», «ссора — решение — дружба», «проблема — помощь — родной человек». Им надо придумать как можно больше предложений с этими словами. При составлении предложений слова можно менять местами.

Упражнение 5. «Сейчас у меня нет…»

Участникам тренинга предлагается написать список того, чего на данный момент в их жизни нет. На выполнение дается пять минут.

В списке у ребят оказались желанные, но недоступные им сейчас вещи: компьютер, модный телефон, своя комната, собака и т.д.

Затем ведущий предлагает посмотреть на свою жизнь с другой стороны, задавая вопрос «Вы сейчас здоровы? Значит, чего еще у вас нет? (болезни). Ребятам предлагается продолжить список с данной точки зрения: чего нет плохого (ссоры с другом, пустого холодильника, грязной одежды, школы за 10 км. от дома, платного обучения, жестоких родителей и т.д.). Желательно, чтобы список-продолжение был длиннее, чем составленный на первом этапе.

Упражнение 6. «Предложи альтернативу».

Ведущий акцентирует внимание детей на том, почему не стоит обсуждать со сверстниками игры и сайты деструктивного характера, подводит к выводу о том, что «запретный плод – сладок».

Ведущий ставит перед участниками тренинга вопросы: Что делать, если ты узнал, что твой сверстник ведет себя деструктивно (играет в «плохие» игры, начал курить, принимать алкоголь или ПАВ, связался с «дурной» компанией)? Что делать, если твой сверстник предлагает тебе подобное?

В ходе обсуждения ребята вспоминают правила «Как сказать: «Нет!» и отрабатывают навыки ведения диалога без отрицания.

Например:

Вместо «Это плохая игра. Не играй в нее!», предложи альтернативу «Давай поиграем в футбол».

Вместо «Не кури! Это вредно», предложи альтернативу «Я занимаюсь в бассейне, пойдем со мной».

## Урок № 2 «Безопасность в Интернете. Формирование навыков безопасного и ответственного поведения в сети»

Цель урока: способствовать формированию у обучающихся навыков безопасного и ответственного поведения в современной информационно-телекоммуникационной среде.

Задачи:

образовательные:

- сформировать правила безопасной работы учащихся в Интернете;
- учить ориентироваться в современном информационном пространстве;
- заложить основы правовых знаний работы в Интернете.

развивающие:

- формировать информационную культуру учащихся;

- развивать умение самостоятельно находить нужную информацию пользуясь web-ресурсами;
- развивать критическое мышление.
воспитательные:
- воспитывать ответственность и дисциплинированность учащихся при работе в сети.
Оборудование: компьютерный класс, ПК, мультимедийный проектор.
Ход урока Активизация внимания
Учитель.
Сегодня у нас очень важная тема, те проблемы, о которых мы будем говорить, касаются абсолютно каждого из вас. Посмотрев, на рисунки и попробуйте определить тему нашего урока.
Интернет вошел в нашу жизнь. Интернет наш помощник – помогает нам работать, путешествовать, отдыхать, общаться с друзьями. Интернет наш учитель – помогает получать новые знания, своевременную информацию.
Но путешествие в Интернет похоже на поход неопытного человека в лес. В лесу можно заблудиться, попасть в болото, собрать ядовитые грибы или ягоды, попасть в лапы диких зверей. Но, если человек знает лес, знает, кто в нем обитает, знает растения, которые в нем растут, то поход в лес ничего кроме пользы и удовольствия не принесет.
Так и в Интернете много полезного, нужного и интересного, но на каждой web – странице вас могут поджидать информация, опасная для вашего кошелька, физического или психического здоровья и даже жизни.
Задача нашего урока оценить эти опасности и выработать стратегию поведения в каждом конкретном случае.
Новый материал
Группа 1
Вирусы
1. Что делают вирусы на нашем компьютере? (виды вирусов, пути распространения, деструктивные действия)
2. Антивирусные программы (назначение, возможности, советы по безопасности)
Группа 2:
Мошенники в Интернете
1. Сайты – двойники
2. Интернет – шантаж
3. Предложение работы на дому и не только
4. «Лохотрон» на проверке безопасности
5. Инвестиционные проекты и финансовые пирамиды.
Демонстрируется видеоролик «Безопасность и развлечения в Интернете»
Группа 3:
Информация в интернете
1.. Безопасное общение. Что такое «скам»?
2. Интернет – зависимость
3. Какие сайты не следует посещать никогда.
Демонстрируется видеоролик «Безопасность в Интернете»
Группа 4
Этика и право в Интернете

1. Этические нормы Интернета
2. «Крэкерские» сайты и «ломаные» программы
3. Защита интеллектуальной собственности в России
Просмотр видеоролика «Я и Интернет» (http://kvestsetevichok.ru/index.php/2015-09-17-14-45-01/videourok)
Правила безопасного поведения в сети Интернет
Просмотр видеоролика, подготовленный пресс-службой Совета Федерации Федерального Собрания Российской Федерации, о проведении 30 октября во всех школах страны Единого урока безопасности в сети Интернет (http://kvestsetevichok.ru/index.php/rolik-soveta-federatsii).
Закрепление материала
Учитель.
Давайте проверим, насколько хорошо вы усвоили сегодняшний урок, выполнив тест на компьютере. (Индивидуальная работа учащихся на ПК)
Итог урока
Домашнее задание (по выбору учащихся)
1. Запишите в тетрадь основные правила безопасного поведения в сети Интернет
2. Придумать сказку для учащихся младших классов об осторожности в Интернете
Рефлексия

**Урок № 3 «Безопасность в сети Интернет. Опасные угрозы и методы борьбы с ними»**

Цель урока: изучение опасных угроз сети Интернет и методы борьбы с ними; предотвращение возможных негативных последствий использования Интернета.
Задачи:
1. ознакомление с возможными угрозами сети Интернет;
2. приобретение навыка выявления мошеннических манипуляций над пользователем;
3. выработка тактики безопасного поведения пользователя в сети;
4. обучение ответственному использованию online-технологий;
5. воспитание дисциплинированности при работе в сети.
Тип урока: урок изучения нового материала.
План урока:
- Организационный момент (1-2 мин.);
- Актуализация знаний (7 мин.);
- Объяснение нового материала (30-35 мин.);
- Самостоятельная работа (7-10 мин.);
- Итог урока (2-3 мин.);
Ход урока:
Организационный момент, 1-2 мин.:
- сообщение темы урока (занесение темы в тетрадь), его целей и задач;
- краткий план деятельности.
Актуализация знаний (7-10 мин)
- Что такое Интернет?
- Какова польза от сети Интернет?

- Как вы думаете, опасен ли Интернет? Если да, то какой вред от использования Интернета?

Сегодня наш урок посвящен теме «Безопасность в сети Интернет».

Интернет – это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов.

Рассматривая возможности Интернета, следует выделить его положительное влияние (формирование социализации, обучение решению жизненно важных проблем, предоставления выбора «виртуального» социального окружения («виртуальных» сообществ) и пр.). Но на ряду с этим, существуют риски негативного влияния: воздействие на состояние физического и психического здоровья пользователя (например, прямое влияние на зрение и опосредованное – на формирование психологической Интернет-зависимости, нарушение осанки, малоподвижный образ жизни, замкнутость поведения).

Вообще в настоящее время использование Интернета порождает гораздо больше проблем, нежели радужных перспектив.

Одна из проблем – обеспечение информационной безопасности в сети. На сегодняшний день практический каждый человек, так или иначе, пользуется сетью Интернет. Возможности Интернет безграничны: учеба, поиск необходимой информации, перевод денежных средств, отдых и многое другое. Однако, многие пользователи даже не задумываются о том, какая опасность поджидает нас во всемирной паутине.

Игра «за или против».

Учитель предлагает игру «за или против». На слайде – несколько высказываний.

Попробуйте привести аргументы, отражающие противоположную точку зрения.

1. Интернет имеет неограниченные возможности дистанционного образования. И это хорошо!
2. Интернет – это глобальный рекламный ресурс. И это хорошо!
3. Общение в интернете – это плохо, потому что очень часто подменяет реальное общение виртуальному.
4. Интернет является мощным антидепрессантом.
5. В интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Учитель предлагает ученикам ответить на вопросы «Какие опасности подстерегают нас?», «Какие виртуальные грабли лежат у нас на пути?». Давайте подумаем и вспомним, какие угрозы вы уже встречали во время работы за компьютером, а может, о каких-то угрозах, вы слышали от своих друзей? (ответы учащихся)

Объяснение нового материала (25-30 мин.):

А теперь давайте обратимся к статистике в сети Интернет. Рейтинг самых опасных угроз распределяется следующим образом:

- Вредоносные программы
- Кража информации
- Халатность сотрудников
- Хакерские атаки
- Финансовое мошенничество
- Спам
- Аппаратные и программные сбои

Как вы видите, угроз достаточно много и все они связаны между собой, например, из-за халатности сотрудников может произойти кража информации, а кража информации в свою очередь, может быть связана с финансовым мошенничеством.

Поэтому сегодня я расскажу вам о том, как обезопасить себя, свих друзей, свой личный или рабочий компьютер, чтобы не стать жертвой сетевых угроз.

Итак, как же бороться с сетевыми угрозами?

Опасности в сети Интернет, пути их преодоления

| Проблема | Способы преодоления |
|---|---|
| Вирусы. Компьютерный вирус разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация). | - Установка антивирусной программы. Сегодня актуальны так называемые «комплексные системы защиты», предназначенные для полной защиты вашего компьютера<br>- Новые вирусы появляются ежедневно, поэтому необходимо регулярно обновлять базы сигнатур, лучше всего настроить программу на автоматическое обновление<br>- Осуществлять веб – серфинг по проверенным сайтам<br>- Блокировать всплывающие окна |
| | - Внимательно проверять доменное имя сайта<br>- Обращать внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.<br>- Проверять сохраняемые файлы, скачанные в Интернете<br>- Установить запрет открытия вложений электронной почты от неизвестных и подозрительных адресатов, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения. |
| Спам, мошеннические письма | - Сообщать свой основной адрес электронной почты только хорошим знакомым<br>- Использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки и никому их не сообщать.<br>- Никогда не отвечать на спам, не переходить по содержащимся в нем ссылкам, не отписываться от спама и тем более не пересылать его по цепочке.<br>- Установить программу анти-спам<br>- Не передавать учетные данные логины и пароли по незащищенным каналам связи |
| Фальшивые Интернет - магазины | - Перед покупкой услуги или товара на незнакомом сайте обязательно нужно проверять отзывы о нём в Интернете<br>- Не доверять объявлениям о подозрительно дешевых товарах<br>- Старайтесь делать покупки в известных и проверенных интернет- магазинах. |
| Бесплатное скачивание файлов с подпиской | - Не указывать свой мобильный номер на незнакомых сайтах.<br>- Если подписка уже оформлена, позвонить в |

| | |
|---|---|
| | службу поддержки оператора и попросить отключить её. |
| Безопасность при оплате картами в сети | - Заведите отдельную карту для покупок в Интернете.<br>- Используйте для покупок в Интернете только личный компьютер.<br>- Перед подтверждением оплаты убедитесь, что в адресе платежной страницы в браузере указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.<br>- Подключите в банке услугу SMS-уведомлений, чтобы получать сведения о всех совершаемых платежах.<br>- Сохраняйте отчеты об оплате и доставке товаров, которые вы получаете по электронной почте.<br>- Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам. |

Опасности общения в социальных сетях

| Проблема | Способы преодоления |
|---|---|
| Проблема конфиденциальности | - Размещая информацию о себе в социальных сетях, необходимо помнить, что ее может увидеть большое количество людей, в том числе родителей, работодателей и др. В итоге, личная жизнь становится достоянием общественности. |
| Взлом страницы мошенниками и злоумышленниками | - Использовать сложные логин и пароль и никому их не сообщать |
| Страницы-фэйки, страницы – двойники | - Необходимо ограниченно сообщать личную информацию о себе (не указывать домашний адрес, номер телефона, номер паспорта, и др.), чтобы злоумышленники несмогли воспользоваться ею в своих целях. |
| Интернет – зависимость | - Планировать время, проводимое в Интернете, и строго следовать этому, соблюдать санитарные нормы |
| Зависть и агрессия | Делиться успехами с самыми близкими: теми, кто искренне за вас порадуется. |

Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников.

Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.

Соблюдая несложные правила, вы сможете избежать популярных сетевых угроз. (Слайд 40).

Самостоятельная работа (7-10 мин.);

Тест:

1. Закончите предложение: Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно…

A. Административному кодексу
B. Трудовому кодексу
C. Уголовному кодексу
D. Гражданскому кодексу

2. Какой из приведенных паролей является более надежным
A. 123456789
B. qwerty
C. annaivanova
D. 13u91A_Ivanova

3. Для того, чтобы антивирусные программы обеспечивали наилучшую безопасность вашего ПК, необходимо:
A. Установить несколько антивирусных программ
B. Удалить все файлы, загруженные из сети Интернет
C. Своевременно обновлять антивирусные базы
D. Отключить компьютер от сети Интернет

4. Какие действия не рекомендуется делать при работе с электронной почтой?
A. Отправлять электронные письма
B. Добавлять в свои электронные письма фотографии
C. Открывать вложения неизвестной электронной почты
D. Оставлять электронные письма в папке Отправленные

5. Что необходимо сделать, если на экране появилось окно с просьбой отправить SMS для дальнейшей работы?
A. Отправить SMS сообщение
B. Выполнить форматирование жесткого диска
C. Перезагрузить компьютер
D. Не отправлять SMS сообщение

6. Зачем необходимо делать резервные копии?
A. Чтобы информация могла быть доступна всем желающим
B. Чтобы не потерять важную информацию
C. Чтобы можно было выполнить операцию восстановления системы
D. Чтобы была возможность распечатать документы

7. А что для вас является "безопасным интернетом?

_____

_____

Итог урока (2-3 мин.):

Домашнее задание.

И 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!

Использованы материалы:

1. Мельников В.П. Информационная безопасность и защита информации: учеб.пособие для студентов высших учебных заведений; 3-е изд., стер.-М.: Издательский центр «Академия», 2008. – 336 с.
2. Википедия – свободная энциклопедия http://ru.wikipedia.org/wiki/Компьютерный_вирус
3. Социальная сеть работников образования http://nsportal.ru/
4. База образовательных ресурсов http://obrazbase.ru/inform/uroki-i- meropriyatiya
5. Интернет СМИ «ваш личный интернет» http://content-filtering.ru

## Урок № 4 «Безопасный Интернет»

Цель проведения занятия – повышение информационной грамотности учащихся, обеспечение ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Содержание

1. Введение.
2. Проблемы современной жизни в киберпространстве.
3. Наиболее злободневные вопросы.
4. Основные выводы для обеспечения безопасного и полезного пребывания в сети Интернет.

Введение

Современное общество и виртуальная реальность тесно связаны друг с другом. Подростки проводят большую часть времени в Интернет и не мыслят себя без него. Массу преимуществ и колоссальные возможности даёт возможность пользоваться Интернетом, но, как и в реальной жизни, жизнь в киберпространстве сопряжена с целым рядом рисков.

Проблема безопасного интернета становится всё более актуальной проблемой, так как год от года возрастает количество киберпреступлений.

Проблемы современной жизни в киберпространстве

Какие опасности могут подстерегать пользователей Интернета?

В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Для этого они могут использовать вирусное программное обеспечение (или «вирусы»), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и на почтовых сервисах, смс-мошенничество.

Мошенникам удаётся достичь своих целей, так как они манипулируют такими человеческими качествами как доверчивость, невнимательность и неосведомлённость. Осведомлён – значит вооружён! Надо знать о возможных действиях мошенников, быть готовым не поддаваться провокации с их стороны и в случае атаки дать отпор, действовать грамотно.

Наиболее злободневные вопросы

Множество вопросов возникает у пользователей сети Интернет, когда они сталкиваются с проблемами. И есть много ресурсов, посвящённых безопасности в сети. Наиболее часто возникающие вопросы по разрешению проблем, возникающих у подростков, разработчики сайта «Сетевичок» собрали в раздел «Быстропомощь» (http://xn--b1afankxqj2c.xn-- p1ai/vopros/elektronnaya-all )

На этом ресурсе отдельно рассматриваются общие вопросы безопасности, вопросы, посвящённые Интернету, компьютеру, электронной почте и мобильной связи.

Здесь же можно задать свой вопрос, если ответ на страницах сайта не найден. Для этого существует форма обратной связи, и все операторы находятся офлайн. Можно оставить сообщение и получить ответ на него в ближайшее время.

Памятка для пользователей

Как уберечь компьютер от заражения вирусом

• Используйте антивирусное программное обеспечение с обновленными базами вирусных сигнатур.
• Не открывайте вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства связи, не удостоверившись, что файл или ссылка не содержит вирус.
• Внимательно проверяйте доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).
• Обращайте внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.
• Не подключайте к своему компьютеру непроверенные съемные носители.
• Не поддавайтесь на провокации злоумышленников, например, требования перевести деньги или отправить смс, чтобы снять блокировку компьютера.

Как защитить свои личные данные
• Используйте сложные пароли (они состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).
• Никому не сообщайте свой пароль.
• Для восстановления пароля используйте привязанный к аккаунту мобильный номер, а несекретный вопрос или электронную почту.
• Не передавайте учетные данные — логины и пароли — по незащищенным каналам связи (не защищены, как правило, открытые и общедоступные wi-fi сети).
• Внимательно проверяйте доменные имена сайтов, на которых вводите учетные данные.
• Не вводите пароли от важных учётных записей, когда подключены к общественной Wi-Fi-сети.
Как не попасться на удочку смс-мошенников
• Не отправляйте смс на незнакомые телефонные номера, за оправку таких смс могут взимать плату.
• Переводите деньги только на известные телефонные номера.
• Не вводите телефонный номер на незнакомых сайтах. Как избежать мошенничества при платежах
• Помните, что банки и платежные сервисы никогда не просят сообщать — ни по почте, ни по телефону — пароль, пин-код или код из смс.
• Никому не сообщайте пароли, пин-коды и коды из смс от своего кошелька или банковской карты.
• Храните банковскую карту в надежном месте.
• Не держите записанные пароли и коды рядом с картой.
• Заведите отдельную карту для покупок в интернете.
• Используйте для покупок в интернете только личный компьютер.
• Регулярно обновляйте антивирусную защиту компьютера.
• Старайтесь делать покупки в известных и проверенных интернет- магазинах.
• Перед подтверждением оплаты убедитесь, что в адресной строке браузера указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.

• Подключите в банке услугу уведомлений по смс, чтобы оперативно получать сведения о совершенных транзакциях.
• Сохраняйте документы об оплате услуг и доставке товаров, полученные по электронной почте.
• Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.
Основные выводы для обеспечения безопасного и полезного пребывания в сети Интернет
Пользователи должны научиться грамотно пользоваться Интернетом и электронными устройствами:
• критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет;
• отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
• избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
• распознавать признаки злоупотребления их доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
• критически относиться к информационной продукции;
• применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.
Будь внимателен! Стань грамотным потребителем цифровой эпохи!

## Урок 5 «Безопасность в сети Интернет»

Цель урока: изучить опасные угрозы сети Интернет и методы борьбы с ними;
Задачи:
- Образовательная: познакомитьсяс понятием «Интернет», «Вирус», изучить приемы безопасности при работе в сети Интернет;
- Развивающая: развитие интереса к предмету, информационной культуры; формирование приёмов логического мышления; развитие способность анализировать и обобщать, делать выводы;
- Воспитательная: воспитание аккуратности, точности, самостоятельности, привитие навыки групповой работы, сотрудничества;
- Здоровьесберегающая: соблюдение санитарных норм при работе с компьютером, соблюдение правил техники безопасности, оптимальное сочетание форм и методов, применяемых на уроке;
Предварительная подготовка учителя: изучение материала урока, написание конспекта, создание презентации, создание теста, подготовка видеофрагмента;
Дидактические основы урока:
Методы обучения: словесные, наглядные, практические.
Тип урока: объяснение нового материала;
Формы учебной работы учащихся: фронтальная, индивидуальная работа.
Оборудование: ПК, проектор, интерактивная доска (или экран), 12 компьютеров, тетради, презентация «Безопасность в сети Интернет».

План урока:
1. Организационный момент (1-2 мин.);
2. Введение в тему (3-5 мин.);
3. Объяснение нового материала (30-35 мин.);
4. Физкультминутка (1 мин.);
5. Самостоятельная работа (7-10 мин.);
6. Итог урока (2-3 мин.);
Ход урока:
1. Организационный момент, 1-2 мин.:
- сообщение темы урока (занесение темы в тетрадь), его целей и задач;
- краткий план деятельности.
2. Введение в тему, 3-5 мин.:
- подготовить детей к восприятию темы;
- нацелить на продуктивную работу.
Сегодня наш урок посвящен теме «Безопасность в сети Интернет». (Слайд 1)
Примечание. Учащиеся записывают в тетрадь основные определения самостоятельно по ходу лекции.
(Слайд 2) Интернет – это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно- вычислительных ресурсов.
На сегодняшний день практический каждый человек, так или иначе, пользуется сетью Интернет. Возможности Интернет безграничны: учеба, поиск необходимой информации, перевод денежных средств, отдых и многое другое. Однако, многие пользователи даже не задумываются о том, какая опасность поджидает нас во всемирной паутине.
Давайте подумаем и вспомним, какие угрозы вы уже встречали во время работы за компьютером, а может, о каких-то угрозах, вы слышали от своих друзей? (ответ учащихся)
Молодцы!
3. Объяснение нового материала (27-30 мин.):
А теперь давайте обратимся к статистике в сети Интернет. Рейтинг самых опасных угроз распределяется следующим образом (Слайд 3):
1. Вредоносные программы
2. Кража информации
3. Халатность сотрудников
4. Хакерские атаки
5. Финансовое мошенничество
6. Спам
7. Аппаратные и программные сбои
Как вы видите, угроз достаточно много и все они связаны между собой, например, из- за халатности сотрудников может произойти кража информации, а кража информации в свою очередь, может быть связана с финансовым мошенничеством.
Но, конечно же, лидером среди угроз являются вирусы. Давайте посмотрим, что такое вирусы, и какими они бывают. (Слайд 4)

Компьютерный вирус — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация).

Классификация (Слайд 5)

В настоящее время не существует единой системы классификации и именования вирусов. Принято разделять вирусы на следующие группы.

По поражаемым объектам (Слайд 6-11)

Файловые вирусы. Это вирусы-паразиты, которые при распространении своих копий обязательно изменяют содержимое исполняемых файлов, при этом файлы, атакованные вирусом, в большинстве случаев полностью или частично теряют работоспособность)

Загрузочные вирусы. Это компьютерные вирусы, записывающиеся в первый сектор гибкого или жесткого диска и выполняющиеся при загрузке компьютера.

Скриптовые вирусы. Требуют наличия одного из скриптовых языков (Javascript, VBScript) для самостоятельного проникновения в неинфицированные скрипты.

Макровирусы. Это разновидность компьютерных вирусов разработанных намакроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office.

Вирусы, поражающие исходный код. Вирусы данного типа поражают или исходный код программы, либо её компоненты (OBJ-, LIB-, DCU- файлы) а также VCL и ActiveX компоненты.

По поражаемым операционным системам и платформам (Слайд 12-13)

- DOS
- Microsoft Windows
- Unix
- Linux

По технологиям, используемым вирусом (Слайд 14-17)

Полиморфные вирусы. Вирус, который при заражении новых файлов и системных областей диска шифрует собственный код.

Стелс-вирусы. Вирус, полностью или частично скрывающий свое присутствие в системе, путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т. д.)

Руткит. Программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

По языку, на котором написан вирус (Слайд 18-19)

- ассемблер
- высокоуровневый язык программирования
- скриптовый язык и др.

По дополнительной вредоносной функциональности (Слайд 20-24)

Бэкдоры. Программы, которые устанавливает взломщик на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе

Шпионы. Spyware — программное обеспечение, осуществляющее деятельность по сбору информации о конфигурации компьютера, деятельности пользователя и любой другой конфиденциальной информации без согласия самого пользователя.

Ботнеты. Это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.

(Слайд 25-26) Каждый день появляются все новые и новые вирусы. Вам необходимо знать, что создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному кодексу РФ (глава 28, статья 273).

(Слайд 27) Также в нашей стране существует доктрина информационной безопасности РФ, согласно которой в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами, детскими порносайтами и обеспечению информационной безопасности в сетях ЭВМ.

Поэтому сегодня я расскажу вам о том, как обезопасить себя, свих друзей, свой личный или рабочий компьютер, чтобы не стать жертвой сетевых угроз.

4. Физкультминутка (1 мин)

Но сначала, мы немножко отдохнем и проведем физкультминутку. (Слайд 28)

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

Итак, как же бороться с сетевыми угрозами? (Слайд 29)

1. Установите комплексную систему защиты. (Слайд 30)

Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление.

2. Будьте осторожны с электронной почтой (Слайд 31)

Не стоит передавать какую-либо важную информацию через электронную почту. Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения. Программы Microsoft Outlook и Windows Mail помогают блокировать потенциально опасные вложения.

3. Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari. (Слайд 32)

Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera. В рейтинге популярности лидирует IE, но лишь потому, что он встроен в Windows. Браузер Opera очень популярен в России из-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.

4. Обновляйте операционную систему Windows. (Слайд 33) Постоянно обновляйте операционную систему Windows. Корпорация Microsoft периодически выпускает

специальные обновления безопасности, которые могут помочь защитить компьютер. Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки входа.

5. Не отправляйте SMS-сообщения. (Слайд 34)

Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.

При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.

Поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.

6. Пользуйтесь лицензионным ПО. (Слайд 35)

Если вы скачиваете пиратские версии программ или свеженький взломщик программы, запускаете его и сознательно игнорируете предупреждение антивируса, будьте готовы к тому, что можете поселить вирус на свой компьютер. Причем, чем программа популярнее, тем выше такая вероятность.

Лицензионные программы избавят Вас от подобной угрозы!

7. Используйте брандмауэр. (Слайд 36)

Используйте брандмауэр Windows или другой брандмауэр оповещают о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру. Он также позволяет запретить вирусам, червям и хакерам загружать потенциально опасные программы на компьютер.

8. Используйте сложные пароли. (Слайд 37)

Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но, чтобы взломать семисимвольный пароль, потребуется два-четыре года.

Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

9. Делайте резервные копии. (Слайд 38)

При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена. Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве – флеш-карте, оптическом диске, переносном жестком диске.

10. Функция «Родительский контроль» обезопасит вас. (Слайд 39)

Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников.

Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.

Соблюдая эти не сложные правила, вы сможете избежать популярных сетевых угроз. (Слайд 40).

5. Самостоятельная работа (7-10 мин.);

Закрепление материала - компьютерное тестирование.

А теперь, давайте проверим, насколько внимательно вы сегодня слушали данный материал.

- Займите места за компьютером.
- Загрузите программу My Test Student.
- Выберите файл «Безопасность в сети Интернет»

Тест содержит 10 вопросов, в каждом вопросе есть только один правильный ответ.

По результатам теста, вы увидите окно со своим результатам. Оценка, которую поставит вам компьютер, и будет вашей оценкой за сегодняшний урок.

Тест:

1. Закончите предложение: Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно…

A. Административному кодексу
B. Трудовому кодексу
C. Уголовному кодексу
D. Гражданскому кодексу

2. Какой классификации вирусов на сегодняшний день не существует?

A. По поражаемым объектам
B. По поражаемым операционным системам и платформам
C. По количеству поражаемых файлов
D. По дополнительной вредоносной функциональности

3. Какой из приведенных паролей является более надежным

A. 123456789
H. qwerty
I. annaivanova
J. 13u91A_Ivanova

4. Для того, чтобы антивирусные программы обеспечивали наилучшую безопасность вашего ПК, необходимо:

A. Установить несколько антивирусных программ
B. Удалить все файлы, загруженные из сети Интернет
C. Своевременно обновлять антивирусные базы
D. Отключить компьютер от сети Интернет

5. Какой из браузеров считается менее безопасным, чем остальные:

A. Mozilla Firefox
B. Internet Explorer
C. Google Chrome
D. Opera

6. Какие действия не рекомендуется делать при работе с электронной почтой?

A. Отправлять электронные письма
B. Добавлять в свои электронные письма фотографии
C. Открывать вложения неизвестной электронной почты
D. Оставлять электронные письма в папке Отправленные

7. Что необходимо сделать, если на экране появилось окно с просьбой отправить SMS для дальнейшей работы?

A. Отправить SMS сообщение
B. Выполнить форматирование жесткого диска
C. Перезагрузить компьютер
D. Не отправлять SMS сообщение

8. Согласно какому документу в России проводится правой ликбез по вопросам защиты информации в ЭВМ?
A. Трудовому кодексу РФ
B. Доктрине информационной безопасности РФ
C. Стратегии развития информационного общества РФ
D. Конвенции о правах ребенка

9. Зачем необходимо делать резервные копии?
A. Чтобы информация могла быть доступна всем желающим
B. Чтобы не потерять важную информацию
C. Чтобы можно было выполнить операцию восстановления системы
D. Чтобы была возможность распечатать документы

10. Что необходимо сделать, если на сайте в Интернет, вдруг появилось сообщение о быстрой проверке ПК с просьбой перезагрузки компьютера?
A. Перезагрузить компьютер
B. Отформатировать жесткий диск
C. Закрыть сайт и выполнить проверку ПК
D. Выключить компьютер.

6. Итог урока (2-3 мин.);

Домашнее задание.

Ребята, домашнее задние у вас будет тоже связано с нашей темой. Разделимся на группы – вы сидите за компьютерами и по номеру компьютера мы и определим, какая группа будет готовить материал:

1. Учащиеся за компьютерами №1-№4 – Вам необходимо найти информацию о праздниках, связанных с информацией и сетью Интернет, которые отмечаются в нашей стране.
2. Учащиеся за компьютерами №5-№8 – Вам необходимо найти правила общения в сети, которые называются «Сетевым этикетом»
3. Учащиеся за компьютерами №9-№12 – Вам необходимо найти информацию об антивирусных программах – их виды и краткую характеристику популярных антивирусов.

## Урок № 6 «Безопасность в сети Интернет. Правила пользования»

Цель: знакомство с правилами безопасной работы в сети Интернет.

Задачи:

• изучить информированность пользователей о безопасной работе в сети Интернет; познакомить с правилами безопасной работы в Интернете; учить ориентироваться в информационном пространстве; способствовать ответственному использованию online-технологий;

• формировать информационную культуру учащихся; умение самостоятельно находить нужную информацию пользуясь web-ресурсами;

• развивать критическое мышление;
• воспитывать дисциплинированность при работе в сети.
Учащиеся должны знать:
• перечень информационных услуг сети Интернет;
• опасности глобальной компьютерной сети.
Учащиеся должны уметь:
• работать с Web-браузером;
• пользоваться информационными ресурсами;
• искать информацию в сети Интернет;
• ответственно относиться к использованию online- технологий.
Тип урока: урок изучения нового материала
Методы и формы обучения: словесный (дискуссия, рассказ), видеометод, наглядный (демонстрация), практический; частично- поисковый, проблемный, метод мотивации интереса; интерактивная форма обучения (обмен мнениями, информацией).
Программно-дидактическое обеспечение: презентация «Безопасный Интернет.pptx», видеофайлы «Дети и Интернет.flv», «Учите детей общаться.flv», тест, информационные плакаты, карточки с адресами Web-ресурсов.
Этапы урока:
1. Организация начала урока. Постановка цели урока. Просмотр видеоролика. Постановка темы и главного вопроса урока.
2. Изучение нового материала. Дискуссия в группе. Теоретическое освещение вопроса (сообщения учащихся).
3. Практическая работа. Поиск информации в сети Интернет. Дискуссия по найденному материалу.
4. Закрепление изученного материала. Рекомендации по правилам безопасной работы. Тестирование.
5. Подведение итогов урока. Оценка работы группы. Просмотр видеоролика. Информация о домашнем задании.
Ход урока
1.Организация начала урока. Постановка цели урока (3 мин).
Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь у вас появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире. Но, с другой стороны, миллионы компьютеров получи доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И не когда-то, а прямо сейчас.
- Внимание, видеоролик!
(Просмотр видеоролика «Дети и Интернет» – 1 мин.)
- Как не стать жертвой сети Интернет? Тема нашего урока - «Безопасный Интернет». Главный вопрос урока: Как сделать работу в сети безопасной?
2. Изучение нового материала (18 мин).
Игра «За или против» (5 мин.).
Для начала, предлагаю поиграть в игру «За или против». Вы увидите несколько высказываний. Попробуйте привести аргументы, отражающие противоположную точку зрения.

• Интернет имеет неограниченные возможности дистанционного образования. И это хорошо!
• Интернет – это глобальный рекламный ресурс. И это хорошо!
• Общение в Интернете – это плохо, потому что очень часто подменяет реальноеобщение виртуальному.
• Интернет-магазины – это плохо, потому что это наиболее популярный вид жульничества в Интернете.
• В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!
Виртуальные грабли (8 мин.)
- Какие опасности подстерегают нас? Какие виртуальные грабли лежат у нас на пути? Посмотрим, что на это скажет Таня, которая подробно познакомилась с этой проблемой дома (сообщение учащегося по темам: «Интернет-зависимость», «Вредоносные и нежелательные программы», «Онлайновое пиратство»).
- Как уберечься от недостоверной информации? Кто такие интернет-мошенники? Расскажет Владимир (сообщение учащегося по темам: «Как уберечься от недостоверной информации?», «Материалы нежелательного содержания», «Интернет-мошенники»).
- Общение в Интернете. Какое оно? Послушаем Мариям (сообщение учащегося по теме «Преступники в Интернете», «Интернет-дневники»).
Физ. минутка «Собери рукопожатия» (2 мин.).
Участникам предлагается в течении 10 секунд пожать руки как можно большего числа других людей.
Обсуждение.
- Кому сколько человек удалось поприветствовать? У кого-то возник психологический дискомфорт? Чем он был вызван?
Аналогия с работой в Интернет.
Общаясь в Интернете, мы очень часто добавляем незнакомых людей в свои социальные сети и общаемся с ними. Мы не знаем про них ничего, только их Ники. Как много информации про человека мы можем узнать от Ника или рукопожатия?
- Ответим на главный вопрос урока – «Как сделать работу в сети безопасной?»
3. Практическая работа (7 мин.).
- Что можно? Что нельзя? К чему надо относиться осторожно?
Давайте посмотрим, что об этом можно прочитать на web-страницах и попробуем сформулировать правила безопасной работы.
- У вас на столах лежат карточки с адресами web-страниц, которые я предлагаю вам сегодня посетить. Данный ресурс добавлен в закладки браузера Opera в папку «Безопасный Интернет». Познакомьтесь с информацией ресурса и сформулируйте правила безопасной работы в сети.
Резюмируем (обсуждение найденной информации). Какие правила безопасной работы вы выбрали, посещая web-сайты?
4. Закрепление изученного материала (12 мин).
- Я тоже для вас приготовила несколько советов.
Интернет – это новая среда взаимодействия людей. В ней новое звучание приобретают многие правила и закономерности, известные людям с давних времен. Попробую сформулировать некоторые простые рекомендации, используя хорошо известные образы.

Повернись, избушка, ко мне передом, а к лесу задом!
Современный Интернет – это не только обширная, но и настраиваемая среда обитания! В нем хорошо тому, кто может обустроить в нем собственное пространство и научиться управлять им. Записывайте свои впечатления в блог, создавайте галереи своих фотографий и видео, включайте в друзья людей, которым вы доверяете. Тогда вместо бессмысленного блуждания по сети ваше Интернет общение будет приносить пользу.
Не пей из колодца!
Даже когда мы испытываем жажду, мы не будем пить из грязной лужи. Также и в среде Интернет, случайно оказавшись в месте, которое производит отталкивающее впечатление агрессивного и замусоренного, лучше покинуть его, переборов чувство любопытства. Это защитит вас от негативных эмоций, а ваш компьютер – от вредоносного программного обеспечения.
Волку дверь не открывайте!
У интернет-мошенников ничего не получится, если только мы сами не откроем им дверь – не сообщим им наши пароли, не загрузим на свой компьютер сомнительные файлы или не дадим возможность пользоваться нашей сетью незнакомым людям.
5. Подведение итогов урока (5 мин.).
Я рада, что вы не остались равнодушны к теме безопасного интернета. Спасибо за активное участие (оценка работы группы).
Каждый год, проходит День безопасного Интернета. Его цель – способствовать безопасному и более ответственному использованию онлайн-технологий и мобильных телефонов среди детей и молодежи по всему миру. Впервые он проводился в 2004 году, и с тех пор число его участников постоянно растет. Для его проведения был образован Российский Оргкомитет, в состав которого вошли представители практически всех ведущих общественных, некоммерческих и других организаций, деятельность которых связана с развитием Интернета. В рамках проведения Дня безопасного Интернета прошел конкурс на лучший видеоролик. Ролик, занявший 1 место, вы видели в начале урока.
- В завершении нашего урока предлагаю посмотреть еще одну интересную конкурсную работу (просмотр видеоролика «Учите детей общаться.pptx» - 0, 35 сек.).

## Урок № 7«Чтобы я делал, если бы не было сети Интернет»

Цель: сформировать представления об альтернативных способах проведения досуга вне сети интернет.
Форма проведения: фотокросс.
Используемые термины:
Фотокросс – это творческие соревнования в условиях временных, тематических и инструментальных ограничений.
Кросс – это объект для съемки (вещь, чувство, ситуация, процесс, сюжет или какой-либо другой объект материальной или нематериальной природы).
Процедура проведения
Подготовительный этап. В ходе подготовительного этапа все участники делятся на команды, в каждой команде не менее 5 человек, количество команд не более 5. Организаторам необходимо убедиться в технической оснащенности участников (наличие

устройств с функцией фотографирования). На данном этапе озвучиваются правила участия в фотокроссе, ограничения по времени проведения.

Правила участия в фотокроссе общее время прохождения всех этапов – не более часа; команда не должна покидать территории образовательной организации; каждую команду в ходе выполнения заданий фотокросса сопровождает педагогический работник; фотографировать разрешается все, что, на взгляд участников, соответствует тематике кросса, задания; в каждой команде должен быть выбран капитан из числа обучающихся, который будет отвечать за взаимодействие с организаторами фотокросса и координировать деятельность всей команды.

Основной этап. Обучающимся необходимо передвигаться по кабинетам (в маршрутных листах каждой команды указана информация о месте старта). Команды необходимо направлять таким образом, чтобы они находились на разных локациях, в разное время.

В каждом кабинет, ответственный за организацию, выдает капитану задание:

Задание локации № 1

Предполагаемая локация организована в спортзале или кабинете со спортивным инвентарем. Тема фотографии: «Наши Олимпийские игры!» Текст задания: «Сделайте интересные групповые фотографии на спортивную тематику. На фотографии должен быть запечатлен момент занятия спортом. Оригинальность и нестандартный подход приветствуется».

Задание локации № 2

Тема фотографии: «Весна – время ловить улыбки!» Текст задания: «Сделайте фотографию так, чтобы на ней не было людей, но была весна и повод для улыбки».

Задание локации № 3

Тема фотографии: «Я – ты – мы!» Текст задания: «При помощи фотографии надо показать друзей, или запечатлеть момент, который воплощает дружбу».

Задание локации № 4.

Предполагаемая локация в библиотеке или в кабинете литературы. Тема фотографии: «Селфи с книгой» Текст задания: «Сделайте креативное фото с интересной книгой, а может вам удастся изобразить героев или передать основную мысль произведения?»

Задание локации № 5.

Тема фотографии: «Вне сети» Текст задания: «Сделайте самую креативную фотографию, где вы отобразите мир без интернета». На финише участники должны сдать свои работы (фотографии) в электронном виде. Вместе с кадрами участники сдают маршрутные листы с подписанными наименованиями файлов с фотографиями по каждому заданию.

Подведение итогов. Подведение итогов фотокросса проводит жюри из числа педагогических работников, принявших участие в организации и проведении мероприятия. При подведении итогов учитывается скорость выполнения, мастерство и оригинальность.

Критерии оценок фотографий:

– соответствие снимка теме задания;

– оригинальность идеи;

– качество выполненных заданий.

Общая оценка за Фотокросс выставляется команде путем сложения оценок за все конкурсные снимки.

Жюри вправе исключить из зачета кадры, грубо нарушающие правила или общепринятые этические нормы.
При равном количестве баллов лучшее место присуждается участнику, пришедшему на финиш раньше.
После того, как победители будут объявлены и награждены, обучающимся предлагается завершить фотокросс флешмобом «Сделай свой выбор в пользу разнообразной и насыщенной жизни!» (Групповое фото с шарами и иным реквизитом).

## РАЗРАБОТКИ УРОКОВ ДЛЯ ОБЧАЮЩИХСЯ 11-Х КЛАССОВ

### Урок № 1 «Безопасность в Интернете»

Цель урока: способствовать формированию у обучающихся навыков безопасного и ответственного поведения в современной информационно-телекоммуникационной среде.
Задачи:
образовательные:
- сформировать правила безопасной работы учащихся в Интернете;
- учить ориентироваться в современном информационном пространстве;
- заложить основы правовых знаний работы в Интернете.
развивающие:
- формировать информационную культуру учащихся;
- развивать умение самостоятельно находить нужную информацию пользуясь web-ресурсами;
- развивать критическое мышление.
воспитательные:
- воспитывать ответственность и дисциплинированность учащихся при работе в сети.
Оборудование: компьютерный класс, ПК, мультимедийный проектор.
Ход урока
I. Оргмомент
II. Активизация внимания
Учитель.
Сегодня у нас очень важная тема, те проблемы, о которых мы будем говорить, касаются абсолютно каждого из вас. Посмотрев, на рисунки и попробуйте определить тему нашего урока.
Интернет вошел в нашу жизнь. Интернет наш помощник – помогает нам работать, путешествовать, отдыхать, общаться с друзьями. Интернет наш учитель – помогает получать новые знания, своевременную информацию.
Но путешествие в Интернет похоже на поход неопытного человека в лес. В лесу можно заблудиться, попасть в болото, собрать ядовитые грибы или ягоды, попасть в лапы диких зверей. Но, если человек знает лес, знает, кто в нем обитает, знает растения, которые в нем растут, то поход в лес ничего кроме пользы и удовольствия не принесет.
Так и в Интернете много полезного, нужного и интересного, но на каждой web – странице вас могут поджидать информация, опасная для вашего кошелька, физического или психического здоровья и даже жизни.

Задача нашего урока оценить эти опасности и выработать стратегию поведения в каждом конкретном случае.

III. Новый материал

Группа 1

Вирусы

1. Что делают вирусы на нашем компьютере? (виды вирусов, пути распространения, деструктивные действия)
2. Антивирусные программы (назначение, возможности, советы по безопасности)

Группа 2:

Мошенники в Интернете

1. Сайты – двойники
2. Интернет – шантаж
3. Предложение работы на дому и не только
4. «Лохотрон» на проверке безопасности
5. Инвестиционные проекты и финансовые пирамиды.

Демонстрируется видеоролик «Безопасность и развлечения в Интернете»

Группа 3:

Информация в интернете

1.. Безопасное общение. Что такое «скам»?
2. Интернет – зависимость
3. Какие сайты не следует посещать никогда.

Демонстрируется видеоролик «Безопасность в Интернете»

Группа 4

Этика и право в Интернете

1. Этические нормы Интернета
2. «Крэкерские» сайты и «ломаные» программы
3. Защита интеллектуальной собственности в России

Просмотр видеоролика «Я и Интернет» (http://kvestsetevichok.ru/index.php/2015-09-17-14-45-01/videourok)

Правила безопасного поведения в сети Интернет

Просмотр видеоролика, подготовленный пресс-службой Совета Федерации Федерального Собрания Российской Федерации, о проведении 30 октября во всех школах страны Единого урока безопасности в сети Интернет (http://kvestsetevichok.ru/index.php/rolik-soveta-federatsii).

IV. Закрепление материала

Учитель.

Давайте проверим, насколько хорошо вы усвоили сегодняшний урок, выполнив тест на компьютере. (Индивидуальная работа учащихся на ПК)

V. Итог урока

VI. Домашнее задание (по выбору учащихся)

1. Запишите в тетрадь основные правила безопасного поведения в сети Интернет
2. Придумать сказку для учащихся младших классов об осторожности в Интернете

VII. Рефлексия

## Урок № 2 «Безопасный интернет»

Цель проведения занятия – повышение информационной грамотности учащихся, обеспечение ответственного и безопасного поведения в современной информационно-телекоммуникационной среде.

Содержание

1. Введение.
2. Проблемы современной жизни в киберпространстве.
3. Наиболее злободневные вопросы.
4. Основные выводы для обеспечения безопасного и полезного пребывания в сети Интернет.

Введение

Современное общество и виртуальная реальность тесно связаны друг с другом. Подростки проводят большую часть времени в Интернет и не мыслят себя без него. Массу преимуществ и колоссальные возможности даёт возможность пользоваться Интернетом, но, как и в реальной жизни, жизнь в киберпространстве сопряжена с целым рядом рисков.

Проблема безопасного интернета становится всё более актуальной проблемой, так как год от года возрастает количество киберпреступлений.

Проблемы современной жизни в киберпространстве

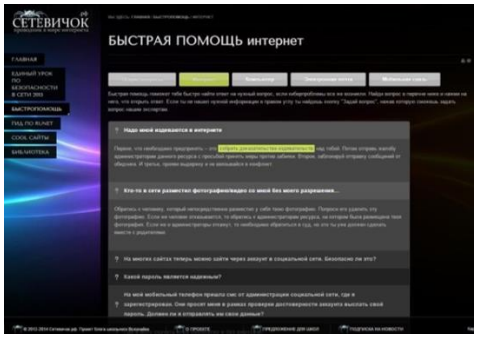
Какие опасности могут подстерегать пользователей Интернета?

В первую очередь это действия мошенников, которые хотят получить финансовую или иную выгоду. Для этого они могут использовать вирусное программное обеспечение (или «вирусы»), поддельные сайты, мошеннические письма, перехват и подбор паролей к учетным записям в социальных сетях и на почтовых сервисах, смс-мошенничество.

Мошенникам удаётся достичь своих целей, так как они манипулируют такими человеческими качествами как доверчивость, невнимательность и неосведомлённость. Осведомлён – значит вооружён! Надо знать о возможных действиях мошенников, быть готовым не поддаваться провокации с их стороны и в случае атаки дать отпор, действовать грамотно.

Наиболее злободневные вопросы

Множество вопросов возникает у пользователей сети Интернет, когда они сталкиваются с проблемами. И есть много ресурсов, посвящённых безопасности в сети. Наиболее часто возникающие вопросы по разрешению проблем, возникающих у подростков, разработчики сайта «Сетевичок» собрали в раздел «Быстропомощь» (http://xn--b1afankxqj2c.xn-- p1ai/vopros/elektronnaya-all )




На этом ресурсе отдельно рассматриваются общие вопросы безопасности, вопросы, посвящённые Интернету, компьютеру, электронной почте и мобильной связи.

Здесь же можно задать свой вопрос, если ответ на страницах сайта не найден. Для этого существует форма обратной связи, и все операторы находятся офлайн. Можно оставить сообщение и получить ответ на него в ближайшее время.

Памятка для пользователей

Как уберечь компьютер от заражения вирусом

• Используйте антивирусное программное обеспечение с обновленными базами вирусных сигнатур.

• Не открывайте вложенные файлы или ссылки, полученные по электронной почте, через социальную сеть или другие средства связи, не удостоверившись, что файл или ссылка не содержит вирус.

• Внимательно проверяйте доменное имя сайта (например, www.yandex.ru), так как злоумышленники часто используют похожие имена сайтов, чтобы ввести жертву в заблуждение (например, www.yadndex.ru).

• Обращайте внимание на предупреждения браузера или поисковой машины о том, что сайт может угрожать безопасности компьютера.

• Не подключайте к своему компьютеру непроверенные съемные носители.

• Не поддавайтесь на провокации злоумышленников, например, требования перевести деньги или отправить смс, чтобы снять блокировку компьютера.

Как защитить свои личные данные

• Используйте сложные пароли (они состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем).

• Никому не сообщайте свой пароль.

• Для восстановления пароля используйте привязанный к аккаунту мобильный номер, а несекретный вопрос или электронную почту.

• Не передавайте учетные данные — логины и пароли — по незащищенным каналам связи (не защищены, как правило, открытые и общедоступные wi-fi сети).

• Внимательно проверяйте доменные имена сайтов, на которых вводите учетные данные.

• Не вводите пароли от важных учётных записей, когда подключены к общественной Wi-Fi-сети.

Как не попасться на удочку смс-мошенников

• Не отправляйте смс на незнакомые телефонные номера, за оправку таких смс могут взимать плату.

• Переводите деньги только на известные телефонные номера.

• Не вводите телефонный номер на незнакомых сайтах. Как избежать мошенничества при платежах

• Помните, что банки и платежные сервисы никогда не просят сообщать — ни по почте, ни по телефону — пароль, пин-код или код из смс.

• Никому не сообщайте пароли, пин-коды и коды из смс от своего кошелька или банковской карты.

• Храните банковскую карту в надежном месте.

• Не держите записанные пароли и коды рядом с картой.

• Заведите отдельную карту для покупок в интернете.

• Используйте для покупок в интернете только личный компьютер.
• Регулярно обновляйте антивирусную защиту компьютера.
• Старайтесь делать покупки в известных и проверенных интернет- магазинах.
• Перед подтверждением оплаты убедитесь, что в адресной строке браузера указан протокол https. Только этот протокол обеспечивает безопасную передачу данных.
• Подключите в банке услугу уведомлений по смс, чтобы оперативно получать сведения о совершенных транзакциях.
• Сохраняйте документы об оплате услуг и доставке товаров, полученные по электронной почте.
• Регулярно просматривайте в интернет-банке историю выполненных операций по вашим картам.
Основные выводы для обеспечения безопасного и полезного пребывания в сети Интернет
Пользователи должны научиться грамотно пользоваться Интернетом и электронными устройствами:
• критически относиться к сообщениям и иной информации, распространяемой в сетях Интернет;
• отличать достоверные сведения от недостоверных, вредную для них информацию от безопасной;
• избегать навязывания им информации, способной причинить вред их здоровью, нравственному и психическому развитию, чести, достоинству и репутации;
• распознавать признаки злоупотребления их доверчивостью, попытки вовлечения их в противоправную и иную антиобщественную деятельность;
• критически относиться к информационной продукции;
• применять эффективные меры самозащиты от нежелательных для них информации и контактов в сетях.
Будь внимателен! Стань грамотным потребителем цифровой эпохи!

## Урок № 3«Безопасность в сети Интернет»

Цель урока: изучить опасные угрозы сети Интернет и методы борьбы с ними;
Задачи:
- Образовательная: познакомитьсяс понятием «Интернет», «Вирус», изучить приемы безопасности при работе в сети Интернет;
- Развивающая: развитие интереса к предмету, информационной культуры; формирование приёмов логического мышления; развитие способность анализировать и обобщать, делать выводы;
- Воспитательная: воспитание аккуратности, точности, самостоятельности, привитие навыки групповой работы, сотрудничества;
- Здоровьесберегающая: соблюдение санитарных норм при работе с компьютером, соблюдение правил техники безопасности, оптимальное сочетание форм и методов, применяемых на уроке;
Предварительная подготовка учащихся: материал, изученный на предыдущих уроках информатики;
Предварительная подготовка учителя: изучение материала урока, написание конспекта, создание презентации, создание теста, подготовка видеофрагмента;

Дидактические основы урока:
Методы обучения: словесные, наглядные, практические.
Тип урока: объяснение нового материала;
Формы учебной работы учащихся: фронтальная, индивидуальная работа.
Оборудование: ПК, проектор, интерактивная доска (или экран), 12 компьютеров, тетради, презентация «Безопасность в сети Интернет».
План урока:
1. Организационный момент (1-2 мин.);
2. Введение в тему (3-5 мин.);
3. Объяснение нового материала (30-35 мин.);
4. Физкультминутка (1 мин.);
5. Самостоятельная работа (7-10 мин.);
6. Итог урока (2-3 мин.);
Ход урока:
1. Организационный момент, 1-2 мин.:
- сообщение темы урока (занесение темы в тетрадь), его целей и задач;
- краткий план деятельности.
2. Введение в тему, 3-5 мин.:
- подготовить детей к восприятию темы;
- нацелить на продуктивную работу.
Сегодня наш урок посвящен теме «Безопасность в сети Интернет». (Слайд 1)
Примечание. Учащиеся записывают в тетрадь основные определения самостоятельно по ходу лекции.
(Слайд 2) Интернет – это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно- вычислительных ресурсов.
На сегодняшний день практический каждый человек, так или иначе, пользуется сетью Интернет. Возможности Интернет безграничны: учеба, поиск необходимой информации, перевод денежных средств, отдых и многое другое. Однако, многие пользователи даже не задумываются о том, какая опасность поджидает нас во всемирной паутине.
Давайте подумаем и вспомним, какие угрозы вы уже встречали во время работы за компьютером, а может, о каких-то угрозах, вы слышали от своих друзей? (ответ учащихся)
Молодцы!
3. Объяснение нового материала (27-30 мин.):
А теперь давайте обратимся к статистике в сети Интернет. Рейтинг самых опасных угроз распределяется следующим образом (Слайд 3):
1. Вредоносные программы
2. Кража информации
3. Халатность сотрудников
4. Хакерские атаки
5. Финансовое мошенничество
6. Спам
7. Аппаратные и программные сбои

Как вы видите, угроз достаточно много и все они связаны между собой, например, из- за халатности сотрудников может произойти кража информации, а кража информации в свою очередь, может быть связана с финансовым мошенничеством.

Но, конечно же, лидером среди угроз являются вирусы. Давайте посмотрим, что такое вирусы, и какими они бывают. (Слайд 4)

Компьютерный вирус — разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является способность к размножению (саморепликация).

Классификация (Слайд 5)

В настоящее время не существует единой системы классификации и именования вирусов. Принято разделять вирусы на следующие группы.

По поражаемым объектам (Слайд 6-11)

Файловые вирусы. Это вирусы-паразиты, которые при распространении своих копий обязательно изменяют содержимое исполняемых файлов, при этом файлы, атакованные вирусом, в большинстве случаев полностью или частично теряют работоспособность)

Загрузочные вирусы. Это компьютерные вирусы, записывающиеся в первый сектор гибкого или жесткого диска и выполняющиеся при загрузке компьютера.

Скриптовые вирусы. Требуют наличия одного из скриптовых языков (Javascript, VBScript) для самостоятельного проникновения в неинфицированные скрипты.

Макровирусы. Это разновидность компьютерных вирусов разработанных намакроязыках, встроенных в такие прикладные пакеты ПО, как Microsoft Office.

Вирусы, поражающие исходный код. Вирусы данного типа поражают или исходный код программы, либо её компоненты (OBJ-, LIB-, DCU- файлы) а также VCL и ActiveX компоненты.

По поражаемым операционным системам и платформам (Слайд 12-13)

- DOS
- Microsoft Windows
- Unix
- Linux

По технологиям, используемым вирусом (Слайд 14-17)

Полиморфные вирусы. Вирус, который при заражении новых файлов и системных областей диска шифрует собственный код.

Стелс-вирусы. Вирус, полностью или частично скрывающий свое присутствие в системе, путем перехвата обращений к операционной системе, осуществляющих чтение, запись, чтение дополнительной информации о зараженных объектах (загрузочных секторах, элементах файловой системы, памяти и т. д.)

Руткит. Программа или набор программ для скрытия следов присутствия злоумышленника или вредоносной программы в системе.

По языку, на котором написан вирус (Слайд 18-19)

- ассемблер
- высокоуровневый язык программирования
- скриптовый язык и др.

По дополнительной вредоносной функциональности (Слайд 20-24)

Бэкдоры. Программы, которые устанавливает взломщик на взломанном им компьютере после получения первоначального доступа с целью повторного получения доступа к системе

Шпионы. Spyware — программное обеспечение, осуществляющее деятельность по сбору информации о конфигурации компьютера, деятельности пользователя и любой другой конфиденциальной информации без согласия самого пользователя.

Ботнеты. Это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами — автономным программным обеспечением. Обычно используются для нелегальной или неодобряемой деятельности — рассылки спама, перебора паролей на удалённой системе, атак на отказ в обслуживании.

(Слайд 25-26) Каждый день появляются все новые и новые вирусы. Вам необходимо знать, что создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно Уголовному кодексу РФ (глава 28, статья 273).

(Слайд 27) Также в нашей стране существует доктрина информационной безопасности РФ, согласно которой в России должен проводиться правовой ликбез в школах и вузах при обучении информатике и компьютерной грамотности по вопросам защиты информации в ЭВМ, борьбы с компьютерными вирусами, детскими порносайтами и обеспечению информационной безопасности в сетях ЭВМ.

Поэтому сегодня я расскажу вам о том, как обезопасить себя, свих друзей, свой личный или рабочий компьютер, чтобы не стать жертвой сетевых угроз.

4. Физкультминутка (1 мин)

Но сначала, мы немножко отдохнем и проведем физкультминутку. (Слайд 28)

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

Итак, как же бороться с сетевыми угрозами? (Слайд 29)

1. Установите комплексную систему защиты. (Слайд 30)

Установка обычного антивируса – вчерашний день. Сегодня актуальны так называемые «комплексные системы защиты», включающие в себя антивирус, файрволл, антиспам-фильтр и еще пару-тройку модулей для полной защиты вашего компьютера. Новые вирусы появляются ежедневно, поэтому не забывайте регулярно обновлять базы сигнатур: лучше всего настроить программу на автоматическое обновление.

2. Будьте осторожны с электронной почтой (Слайд 31)

Не стоит передавать какую-либо важную информацию через электронную почту. Установите запрет открытия вложений электронной почты, поскольку многие вирусы содержатся во вложениях и начинают распространяться сразу после открытия вложения. Программы Microsoft Outlook и Windows Mail помогают блокировать потенциально опасные вложения.

3. Пользуйтесь браузерами Mozilla Firefox, Google Chrome и Apple Safari. (Слайд 32)

Большинство червей и вредоносных скриптов ориентированы под Internet Explorer и Opera. В рейтинге популярности лидирует IE, но лишь потому, что он встроен в Windows. Браузер Opera очень популярен в России из-за ее призрачного удобства и очень большого числа настроек. Уровень безопасности имеет ряд недостатков как у одного, так и у второго браузера, поэтому лучше ими не пользоваться вовсе.

4. Обновляйте операционную систему Windows. (Слайд 33) Постоянно обновляйте операционную систему Windows. Корпорация Microsoft периодически выпускает специальные обновления безопасности, которые могут помочь защитить компьютер. Эти обновления могут предотвратить вирусные и другие атаки на компьютер, закрывая потенциально опасные точки входа.

5. Не отправляйте SMS-сообщения. (Слайд 34)

Сейчас очень популярны сайты, предлагающие доступ к чужим SMS и распечаткам звонков, также очень часто при скачивании файлов вам предлагают ввести свой номер, или внезапно появляется блокирующее окно, которое якобы можно убрать с помощью отправки SMS.

При отправке SMS, в лучшем случае, можно лишиться 300-600 рублей на счету телефона – если нужно будет отправить сообщение на короткий номер для оплаты, в худшем – на компьютере появится ужасный вирус.

Поэтому никогда не отправляйте SMS-сообщения и не вводите свой номер телефона на сомнительных сайтах при регистрации.

6. Пользуйтесь лицензионным ПО. (Слайд 35)

Если вы скачиваете пиратские версии программ или свеженький взломщик программы, запускаете его и сознательно игнорируете предупреждение антивируса, будьте готовы к тому, что можете поселить вирус на свой компьютер. Причем, чем программа популярнее, тем выше такая вероятность.

Лицензионные программы избавят Вас от подобной угрозы!

7. Используйте брандмауэр. (Слайд 36)

Используйте брандмауэр Windows или другой брандмауэр оповещают о наличии подозрительной активности при попытке вируса или червя подключиться к компьютеру. Он также позволяет запретить вирусам, червям и хакерам загружать потенциально опасные программы на компьютер.

8. Используйте сложные пароли. (Слайд 37)

Как утверждает статистика, 80% всех паролей — это простые слова: имена, марки телефона или машины, имя кошки или собаки, а также пароли вроде 123. Такие пароли сильно облегчают работу взломщикам. В идеале пароли должны состоять минимум из семи, а лучше двенадцати символов. Время на подбор пароля из пяти символов — два-четыре часа, но, чтобы взломать семисимвольный пароль, потребуется два-четыре года.

Лучше использовать пароли, комбинирующие буквы разных регистров, цифры и разные значки.

9. Делайте резервные копии. (Слайд 38)

При малейшей угрозе ценная информация с вашего компьютера может быть удалена, а что ещё хуже – похищена. Возьмите за правило обязательное создание резервных копий важных данных на внешнем устройстве – флеш-карте, оптическом диске, переносном жестком диске.

10. Функция «Родительский контроль» обезопасит вас. (Слайд 39)

Для детской психики Интернет – это постоянная угроза получения психологической травмы и риск оказаться жертвой преступников.

Не стремитесь утаивать от родителей круг тем, которые вы обсуждает в сети, и новых Интернет-знакомых, это поможет вам реально оценивать информацию, которую вы видите в сети и не стать жертвой обмана.

Соблюдая эти не сложные правила, вы сможете избежать популярных сетевых угроз. (Слайд 40).

5. Самостоятельная работа (7-10 мин.);

Закрепление материала - компьютерное тестирование.

А теперь, давайте проверим, насколько внимательно вы сегодня слушали данный материал.

- Займите места за компьютером.
- Загрузите программу My Test Student.
- Выберите файл «Безопасность в сети Интернет»

Тест содержит 10 вопросов, в каждом вопросе есть только один правильный ответ.

По результатам теста, вы увидите окно со своим результатам. Оценка, которую поставит вам компьютер, и будет вашей оценкой за сегодняшний урок.

Тест:

1. Закончите предложение: Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно…

A. Административному кодексу
B. Трудовому кодексу
C. Уголовному кодексу
D. Гражданскому кодексу

2. Какой классификации вирусов на сегодняшний день не существует?

A. По поражаемым объектам
B. По поражаемым операционным системам и платформам
C. По количеству поражаемых файлов
D. По дополнительной вредоносной функциональности

3. Какой из приведенных паролей является более надежным

A. 123456789
H. qwerty
I. annaivanova
J. 13u91A_Ivanova

4. Для того, чтобы антивирусные программы обеспечивали наилучшую безопасность вашего ПК, необходимо:

A. Установить несколько антивирусных программ
B. Удалить все файлы, загруженные из сети Интернет
C. Своевременно обновлять антивирусные базы
D. Отключить компьютер от сети Интернет

5. Какой из браузеров считается менее безопасным, чем остальные:

A. Mozilla Firefox
B. Internet Explorer
C. Google Chrome
D. Opera

6. Какие действия не рекомендуется делать при работе с электронной почтой?

A. Отправлять электронные письма
B. Добавлять в свои электронные письма фотографии
C. Открывать вложения неизвестной электронной почты
D. Оставлять электронные письма в папке Отправленные

7. Что необходимо сделать, если на экране появилось окно с просьбой отправить SMS для дальнейшей работы?

A. Отправить SMS сообщение
B. Выполнить форматирование жесткого диска
C. Перезагрузить компьютер
D. Не отправлять SMS сообщение

8. Согласно какому документу в России проводится правой ликбез по вопросам защиты информации в ЭВМ?

A. Трудовому кодексу РФ
B. Доктрине информационной безопасности РФ
C. Стратегии развития информационного общества РФ
D. Конвенции о правах ребенка

9. Зачем необходимо делать резервные копии?

A. Чтобы информация могла быть доступна всем желающим
B. Чтобы не потерять важную информацию
C. Чтобы можно было выполнить операцию восстановления системы
D. Чтобы была возможность распечатать документы

10. Что необходимо сделать, если на сайте в Интернет, вдруг появилось сообщение о быстрой проверке ПК с просьбой перезагрузки компьютера?

A. Перезагрузить компьютер
B. Отформатировать жесткий диск
C. Закрыть сайт и выполнить проверку ПК
D. Выключить компьютер.

6. Итог урока (2-3 мин.);

Домашнее задание.

Ребята, домашнее задние у вас будет тоже связано с нашей темой. Разделимся на группы – вы сидите за компьютерами и по номеру компьютера мы и определим, какая группа будет готовить материал:

1. Учащиеся за компьютерами №1-№4 – Вам необходимо найти информацию о праздниках, связанных с информацией и сетью Интернет, которые отмечаются в нашей стране.

2. Учащиеся за компьютерами №5-№8 – Вам необходимо найти правила общения в сети, которые называются «Сетевым этикетом»

3. Учащиеся за компьютерами №9-№12 – Вам необходимо найти информацию об антивирусных программах – их виды и краткую характеристику популярных антивирусов.

## Урок № 4 «Предупреждён – значит вооружён»

Цель: способствовать формированию знаний о правилах безопасного поведения в современной информационной среде, в частности – сети Интернет.
Задачи:
- Заставить задуматься о своем месте в этом мире.
- Познакомить видами Интернет-угроз и противоправных посягательствах в сети Интернет.
- Познакомить студентов с правилами медиабезопасности, с сайтами помощи в случае Интернет-угроз.
- Сформировать чувство ответственности за свое пребывание в Интернет, за воспитание будущих поколений.
- Продемонстрировать методику проведения подобных занятий для учащихся
Оборудование: анкеты, памятки, презентация, видеофрагменты («Безопасность в Интернете», «Развлечения и безопасность в Интернете», социальный ролик «Безопасный Интернет-детям!»), проектор, ПК.
Используемые понятия:
«Интернет-угроза» - действие в сети Интернет, которое причиняет вред пользователю Интернета путем опубликования или пересылки некоей информации, а также Интернет-коммуникация, направленная на причинение вреда собеседнику в Сети.
«Секта» - религиозная организация.
«Вербовка», «Вербовать» - найти желающего на выполнение каких-либо работ.
«Киберунижение» – распространение унижающей достоинство человека информации (изображение, видео, текста) в Интернете, а также использование Интернета для оскорблений и травли.
«Экстремистские группировки» - организованные группы людей, занимающиеся преступной и опасной для людей деятельностью (например: убийство, нанесение тяжких телесных повреждений, массовые беспорядки, терроризм)
Терроризм – массовое устрашение либо уничтожение людей.
Ход киберурока.
1. Организационный момент.
Добрый день, ребята! Нашу встречу с вами я хочу начать со следующего стихотворения:
Ты есть, я есть, он есть,
А жизнь у каждого своя.
И ей цена – достоинство и честь,
Есть возраст переходных лет,
Какой бы сложной не была она.
Для многих начинается рассвет,
А кто-то погружается во тьму.
Ты есть, я есть, он есть,
Лишь вместе мы сумеем зло пресечь
И сохранить достоинство, чтоб жить.
2. Сообщение темы, цели, задач занятия.
Сегодня наш урок называется «Урок медиабезопасности». Как вы полагаете, о чем мы на этом уроке поговорим? (ответы)
А кто может сказать, что такое медиабезопасноть? (ответы)

Слово «медиабезопасность» сочетает в себе два термина – медиаграмотность и информационная безопасность.

В международном праве «Медиаграмотность - грамотное использование детьми и их преподавателями инструментов, обеспечивающих доступ к информации, развитие критического анализа содержания информации и привития коммуникативных навыков, содействие профессиональной подготовке детей и их педагогов в целях позитивного и ответственного использования ими информационных и коммуникационных технологий и услуг». В российском законодательстве «Информационная безопасность детей – это состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией, в том числе распространяемой в сети Интернет, вреда их здоровью, физическому, психическому, духовному и нравственному развитию». Такие понятия появились благодаря инициативе Уполномоченного при Президенте РФ по правам ребенка Павла Астахова, который сказал:

«Зачастую дети принимают все, что видят по телевизору и в Интернете, за чистую монету. В силу возраста, отсутствия жизненного опыта и знаний в области медиаграмотности они не всегда умеют распознать манипулятивные техники, используемые при подаче рекламной и иной информации, не анализируют степень достоверности информации и подлинность ее источников. Мы же хотим, чтобы ребята стали полноценными гражданами своей страны – теми, кто может анализировать и критически относиться к информационной продукции. Они должны знать, какие опасности подстерегают их в сети и каких избежать».

Я думаю, что каждый хочет жить в мире и безопасности, а это значит, что на душе будет радостно и спокойно. Мы не зря поднимаем сегодня этот вопрос. Как было бы здорово, если бы каждый человек соблюдал все правила приличия, был бы всегда доброжелателен. Но, к сожалению, так не бывает. И очень часто по чьей-то вине, нарушается мир другого человека. С 1 сентября 2012 г. вступил в силу закон «О защите детей от информации, причиняющий вред их здоровью и развитию». В связи с этим, каждый пользователь должен знать о правилах ответственного и безопасного поведения в современной информационной среде, способной нанести вред физическому и психическому здоровью человека.

Не многие знают, что более 80% вербовочного процесса детей, подростков и молодых людей проходит через Интернет! Сегодня мы рассмотрим наиболее распространённые виды Интернет-угроз, через которые злоумышленники воздействуют на человека, а также узнаем о способах защиты от противоправных посягательств в сети Интернет и мобильной сотовой связи. Ведь недаром поговорка гласит: «Предупреждён – значит вооружён».

3. Работа по теоретической части занятия.

Интернет – это не только пространство для поиска информации, ведения личной переписки, знакомства с новыми людьми и общения, это еще и источник опасности, которую можно предотвратить.

Для это нужно быть осведомленным о видах угроз, исходящих из Сети.

Какие угрозы встречаются наиболее часто? Прежде всего:

Угроза заражения вредоносным ПО.

Доступ к нежелательному содержимому. Это насилие, наркотики порнография, страницы, подталкивающие молодежь к самоубийствам, анорексии (отказ от приема пищи),

убийствам, страницы с националистической или откровенно фашистской идеологией и многое другое. Ведь все это доступно в Интернет без ограничений. Часто бывает так, что просмотр этих страниц даже не зависит от ребенка, ведь на многих сайтах отображаются всплывающие окна, содержащие любую информацию, чаще всего порнографического характера;

Контакты с незнакомыми людьми с помощью чатов, электронной почты или социальных сетей. Все чаще и чаще злоумышленники используют эти каналы для того, чтобы заставить молодежь выдать личную информацию.

Неконтролируемые покупки в Интернет-магазинах.

Подростки и молодые люди в возрасте 18-20 лет являются наиболее уязвимой группой и подвергаются наибольшей опасности. Они стремятся исследовать свою сексуальность, уйти из-под контроля родителей и завязать новые отношения вне семьи. Несмотря на то, что общение в Интернете может быть полностью анонимным, они больше подвержены опасности, даже если до конца не осознают возможные последствия.

Наиболее уязвимыми для злоумышленников являются следующие категории молодых людей:

- новички в Интернете, не знакомые с сетевым этикетом;
- недружелюбные пользователи;
- те, кто стремится попробовать все новое, связанное с острыми ощущениями;
- активно ищущие внимания и привязанности;
- бунтари;
- одинокие или брошенные;
- любопытные;
- испытывающие проблемы с сексуальной ориентацией;
- те, кого взрослые могут легко обмануть;
- те, кого привлекает субкультура, выходящая за рамки понимания их родителей.

Современный Интернет называют большой душеловкой? Как она работает? Мошенничество в Интернете существует столько же, сколько и сама Всемирная Сеть. На просторах Интернета оно подстерегает нас везде: в электронной почте, социальных сетях, на различных сайтах. Из года в год злоумышленники придумывают всё новые и новые уловки, направленные на то, чтобы обмануть своих потенциальных жертв. В отличие от таких интернет- угроз, как вирусы, троянские программы, программы-шпионы, СМС-блокеры, спам и др…, мошенничество примечательно тем, что мишень злоумышленника – не компьютер, а человек у которого, как известно, свои слабости (н-р, страх, любопытство, легковерность…). Человек в наше время стал товаром. Рынок живого товара сейчас догоняет обороты наркотиков. Поэтому, только сам пользователь может сделать свою жизнь в виртуальном пространстве безопасной.

По статистике, число детей и подростков – пользователей Интернета в России составляет около 14 млн. человек, из которых две трети выходят в Интернет ежедневно. Возраст начала самостоятельной работы в Сети для российских детей сейчас составляет 10 лет. Примерно 30% детей, пользующихся Интернетом, проводят в Сети ежедневно более трех часов в день. Чтобы узнать, какова картина наших пользователей Интернета, проведем анонимное анкетирование. У каждого из вас есть анкета. Заполните ее. (заполняют и сдают). А теперь проанализируйте свои ответы: если вы получили больше ответов «ДА»,

то вам следует задуматься над тем, что вы подвергаетесь серьезной опасности не только стать жертвой угроз Интернета, но и иметь серьезную степень Интернет-зависимости.
Как Вы думаете, какие угрозы в сети Интернет существуют для Вас? (ответы). Верно. Рассмотрим некоторые из них.
При общении в Сети у каждого обязательно появляются виртуальные знакомые и друзья. Такая форма общения очень часто привлекает преступников, т.к. различия киберпреступлений от традиционных реальных преступных посягательств обусловлены особенностями интернет-среды: анонимностью, возможностью фальсификации, наличием огромной аудитории, возможностью достать жертву в любом месте и в любое время. Так очень легко завладеть вниманием собеседника, применяя приемы психологического воздействия, так называемый кибербуллинг — это нападения с целью нанесения психологического вреда, которые осуществляются через электронную почту, сервисы мгновенных сообщений, в чатах, социальных сетях, на web-сайтах, а также посредством мобильной связи. Такое многократно повторяемое агрессивное поведение имеет целью навредить человеку и базируется на дисбалансе власти (физической силы, социального статуса в группе). (видеофрагмент «Безопасность в Интернете»).
Наиболее опасными видами кибербуллинга являются киберпреследование - скрытое выслеживание жертвы с целью организации нападения, избиения, изнасилования и т.д., а также хеппислепинг — видеоролики с записями реальных сцен насилия.
Встречается в виртуальной среде и так называемый буллицид – доведение человека до самоубийства путем психологического насилия.
Для безопасности несовершеннолетнего особую угрозу представляют личные встречи с виртуальными знакомыми в реальной жизни, о которых никто может ничего не знать.
Опасная для молодежи информация, способная причинить серьезный вред их здоровью, развитию и безопасности может содержаться на электронных ресурсах, содержащих материалы экстремистского и террористического характера. Не случайно сегодня оченьчасто возникает вопрос об участии молодых людей славянской, национальности никогда не бывавших в восточных странах, в незаконных террористических организациях и готовящих террористические акции на территории России. Одной из причин такой ситуации – это вовлечение этой части молодежи в незаконные действия путем Интернет-вербовки.
Особую опасность представляют для незрелой психики несовершеннолетних электронные ресурсы, созданные и поддерживаемые деструктивными религиозными сектами.
Вот один из примеров: Оксана познакомилась в соц сетях с обаятельной девушкой. Разговорились, девушка пригласила Оксану прийти на вечеринку «Истинных сестер»: «У нас так здорово, мы так дружны и очень интересно проводим время». Оксана согласилась и через несколько дней попала в сомнительную компанию, где надо было в обнаженном виде совершать странные обряды. Но члены секты под угрозой смерти запретили Оксане об этом кому-нибудь рассказывать. Оксана стала замкнутой и задумчивой, перестала хорошо учиться, с родителями почти не разговаривала. Ее постоянно мучил вопрос: как покинуть секту?
Доверчивость и наивность детей нередко используют в своих целях компьютерные мошенники, спамеры, фишеры. Несовершеннолетнего пользователя взрослые преступники могут с использованием электронных ресурсов втянуть в совершение

антиобщественных, противоправных, в том числе уголовно-наказуемых деяний. Известны случаи вовлечения подростков через Интернет:

- в действия, носящие оскорбительный и клеветнический характер;
- в экстремистскую деятельность;
- в преступную деятельность по изготовлению и сбыту наркотических средств и психотропных веществ и склонению к их потреблению несовершеннолетних, незаконному обороту оружия, взрывных устройств и взрывчатых веществ, сильнодействующих или ядовитых веществ в целях сбыта.

Вам следует знать, что указанные общественно опасные деяния, независимо от того, совершаются ли они с применением традиционных способов и средств или с использованием информационно- телекоммуникационных сетей, уголовно наказуемы, в том числе для под- ростков, достигших установленного законом возраста уголовной ответственности (16 лет, аза отдельные виды преступлений – с 14 лет).

1. Пропаганда наркотиков, насилия и жестокости, суицидального поведения, самоповреждений может быть весьма опасной для неокрепшей подростковой психики. Согласно Конвенции ООН о правах ребенка такие действия есть не что иное, как криминальная, в том числе коммерческая эксплуатация ребенка.

2. Киберунижение и кибертравля. Они чаще встречаются в социальных сетях, на форумах и в чатах; для кибертравли используются также электронная почта и онлайн-мессенджеры (например, Аська, СМСки). Опасность распространения унижающей человека информации заключается в том, что в отличие от «обычного» унижения, сцены, изображающие сам процесс унижения, распространяются на неограниченный круг лиц. Таким образом, такие видео или фото могут быть доступны будущим друзьям и знакомым даже в случае переезда в другой город. Еще одна опасность заключается в том, что на данный момент удалить все экземпляры унижающих текстов или изображений из Интернета почти невозможно – ничто не мешает кому-то сохранить их на своем компьютере и опубликовать в Сети повторно даже через несколько лет.

Это не полный перечень тех опасностей, которые могут подстерегать вас в Интернете. Самое главное уметь применять элементарные правила безопасности в Интернете. (видеофрагмент «Развлечения и безопасность в Интернете»). Чтобы знать, как поступить, предлагаем вам свод правил поведения в Интернете (памятки для студентов).

А что делать, если вы уже подверглись угрозе со стороны Интернет- мошенников или стали членом Интернет-клубов сомнительного характера, или у вас проявляются признаки Интернет-зависимости? В этом случае есть возможность обратиться в службу «Горячей линии» Центра безопасного Интернета в России. На «Горячую линию» можно попасть круглосуточно, набрав адрес www.saferunet.ru и нажав на красную кнопку «Горячая линия». Горячая линия принимает сообщения по следующим категориям противоправного контента:

- сексуальная эксплуатация несовершеннолетних;
- вовлечение детей в сексуальную деятельность (grooming);
- расизм, национализм, иные формы ксенофобии;
- киберунижение и кибертравля;
- сцены насилия над детьми;
- пропаганда и распространение наркотиков;
- пропаганда и публичное оправдание терроризма.

Отправка сообщения на «Горячую линию» производится анонимно и бесплатно. При этом могут быть не только текстовые формы обращения, но и пересылка ссылок на нежелательные ресурсы, которые могут быть оценены специалистами и закрыты.

Еще одним средством помощи детям и их родителям в области Интернет-угроз является линия помощи «Дети онлайн» – служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования детьми и подростками Интернета и мобильной связи.

Обратиться на «Линию помощи» можно по телефону или через Интернет (все сведения у вас есть в правилах). На «Линии помощи» психологическую и информационную поддержку оказывают психологи факультета психологии МГУ имени М. В. Ломоносова и Фонда развития Интернет, прошедшие специальную подготовку по психологическому и информационному консультированию по проблемам безопасного использования детьми и подростками Интернета и мобильной связи.

В ряде случаев сотрудники «Линии помощи» перенаправляют поступивший запрос или рекомендует позвонившим самим обратиться в другие организации, с которыми сотрудничает служба «Дети онлайн». К ним относятся: специализированные телефоны доверия, горячие Линии (в частности, Горячая Линия по приему сообщений о детской порнографии Фонда «Дружественный Рунет»), службы психологической и социальной помощи, органы МВД (в частности, управление «К», которое занимается расследованиями в области кибер-преступности).

В Оренбургской области работают также региональные службы помощи и детские телефоны доверия.

Владение правилами медиабезопасности являются важной составляющей каждого человека, так как вы все в будущем кто-то учитель, а кто-то родитель. На вас будет лежать ответственность за воспитание будущих поколений. Чтобы ваши дети росли в безопасности, научите их самым элементарным правилам пользования сетью, расскажите о возможных угрозах и будьте всегда рядом, если у него возникают какие-то проблемы. (видеофрагмент «Социальный ролик «Безопасный Интернет – детям!»).

В этом могут помочь специальные программы контентной фильтрации, т.е. программы, фильтрующие сайты и ресурсы Интернета на наличие нежелательной информации и ограничивающие возможность их просмотра. На рынке программных ресурсов на сегодняшний день существует множество программ выполняющих, так называемую функцию Родительского контроля. Наибольшей популярностью пользуются антивирусные программы, содержащие такую функцию. Они удобны тем, что позволяют защитить компьютер не только от вредоносных программ, но и ограничить время пребывания в сети и доступ ребенка к нежелательным сайтам. Это такие продукты как Антивирус Касперского Security или Crystal, DrWeb Security и другие. Есть и программы, созданные специально для ограничения контента.

4. Итог

Современный мир, который вас окружает, сложен и труден. Нужно быть очень умным, осторожным, сообразительным, чтобы жить в нем. Безопасность в этом мире зависит от каждого из нас, прежде всего, от отношения к самому себе.

Природа создала всё для того, чтобы человек был счастлив. Деревья, яркое солнце, чистую воду, плодородную почву. И нас людей – сильных, красивых, здоровых, разумных. Человек рождается для счастья.

5. Рефлексия.

И в заключении я попрошу тех, кому этот урок стал интересным, полезным и кто считает, что Интернет должен стать для нас другом, хором сказать «Я за безопасный Интернет!». Всем спасибо.

Приложение 1.

Анкета для учащихся:

| № п/п | Вопрос | Да | Нет |
|---|---|---|---|
| 1. | Часто ли вы замечаете, что находитесь в Интернете дольше запланированного времени? | | |
| 2. | Часто ли вы откладываете свои домашние дела из-за необходимости находиться в Интернете? | | |
| 3. | Используете ли вы смайлики в обычной, не электронной переписке? | | |
| 4. | Думаете ли вы, что без Интернета ваша жизнь стала бы скучна и неинтересна? | | |
| 5. | Находите ли вы себя усиленно думающим: «Чего бы еще поискать в Сети?» | | |
| 6. | Читая книгу, ищите ли вы полосу прокрутки с правой стороны, чтобы прокрутить текст? | | |
| 7. | Вы быстрее вспоминаете адрес своей странички в Интернете, чем номер мобильного телефона? | | |
| 8. | Часто ли вы говорите себе: «Еще несколько минут и выхожу», находясь в Интернете? | | |

Приложение 2.

Памятка для Учащихся:

Основные правила безопасности в Интернете

Вы должны это знать:

* При регистрации на сайтах, старайтесь не указывать личную информацию, т.к. она может быть доступна незнакомым людям. Так же, не рекомендуется размещать свою фотографию, давая, тем самым, представление о том, как вы выглядите, посторонним людям.
* Используйте веб-камеру только при общении с друзьями. Проследите, чтобы посторонние люди не имели возможности видеть ваш разговор, т.к. он может быть записан.
* Если вы получили нежелательное письмо от незнакомых людей, не отвечайте на него. В случае, если Вы ответите на подобное письмо, отправитель будет знать, что вы пользуетесь своим электронным почтовым ящиком и будет продолжать посылать вам спам.
* Если вам пришло сообщение с незнакомого адреса, его лучше не открывать. Подобные письма могут содержать вирусы.
* Если вам приходят письма с неприятным и оскорбляющим вас содержанием, если кто-то ведет себя по отношению к вам неподобающим образом, сообщите об этом.
* Если вас кто-то расстроил или обидел, расскажите родителям. Родители самые близкие люди, они вас выслушают, помогут и защитят.

* Не желательно размещать персональную информацию в Интернете. Персональная информация — это номер вашего мобильного телефона, адрес электронной почты, домашний адрес и фотографии вас, вашей семьи или друзей.
* Не размещайте фото или видеоматериалы, содержащую изображение других лиц, без их согласия. Помните, если вы публикуете фото или видео в Интернете — каждый может посмотреть их.
* Не открывайте файлы, которые прислали неизвестные Вам людей. Вы не можете знать, что на самом деле содержат эти файлы – в них могут быть вирусы или фото/видео с «агрессивным» содержанием.
* Не добавляйте незнакомых людей в свой контакт лист в IM (ICQ, MSN messenger и т.д.)
* Помните, что виртуальные знакомые могут быть не теми, за кого себя выдают.
* Если рядом с вами нет родственников, не встречайтесь в реальной жизни с людьми, с которыми вы познакомились в Интернете. Если ваш виртуальный друг действительно тот, за кого он себя выдает, он нормально отнесется к вашей заботе о собственной безопасности!
* Никогда не поздно рассказать взрослым, если вас кто-то обидел.

Памятка по безопасному поведению в Интернете

* Для того, чтобы обезопасить себя, свою семью, своих родителей от опасностей Интернета и причинения возможного ущерба, вы должен предпринимать следующие меры предосторожности при работе в Интернете:
* По возможности не сообщайте свои личные данные: имя, номер телефона, адрес проживания или учебы, любимые места отдыха или проведения досуга. Помните, что всё, что вы о себе сообщите в социальных сетях, чатах или форумах, может быть доступно, прочтено и использовано любым человеком в мире: Интернет прозрачен и глобален.
* Никогда не сообщайте в открытых источниках конфиденциальные данные: пароли или номера кредитных карт, пин-коды и другую финансовую информацию.
* При регистрации на интернет страницах используйте нейтральное имя, а если потребуется выбрать пароль, используйте комбинацию из строчных и заглавных букв и цифр, по возможности сложную.
* Всегда сообщайте взрослым обо всех случаях в Интернете, которые вызвали у вас смущение или тревогу. И советуйтесь по сложным ситуациям, когда вы сталкиваетесь с чем-то необычным.
* Используйте защитные программы, антивирусы, фильтры электронной почты, программы для блокирования спама и нежелательных сообщений.
* Будьте сдержаны и, по возможности, вежливы в интернет-общении. Прекращайте любые контакты с теми, кто начинает задавать вам вопросы раздражающие, личного характера или содержащие сексуальные намеки. Обязательно расскажите об этом родителям

## Урок № 5 «Информационная безопасность»

Цель: формирование представления об информационной безопасности.
Задачи:
обучающие:

- познакомить с понятием информационной безопасности
- рассмотреть различные угрозы информационной безопасности развивающие:
- совершенствовать коммуникативные навыки через умение излагать мысли, умение вести диалог
- определить план действий для предотвращения угрозы информационной безопасности воспитывающие:
- воспитывать ответственность за свои действия

План урока:

1. Организационный момент
2. Подготовка учащихся к усвоению нового материала
3. Теоретическая часть. Изучение нового материала
4. Практическая часть. Первичное закрепление знаний
5. Домашнее задание
6. Итог урока.

Оборудование и методические материалы: Мультимедийный проектор, ПК на РМУ, презентация, набор карточек, памятка для обучающихся.

Ход урока

Организационный момент

Подготовка к усвоению нового материала

Тема урока «Информационная безопасность».

Цель урока: Формирование представления об информационной безопасности.

Теоретическая часть. Изучение нового материала

- Что такое «информационная безопасность»?

Дети высказывают свое мнение, как они понимают этот термин. Обобщая, учитель сообщает определение, которое записывается в тетрадь

Информационная безопасность — это защищенность информации от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации или ее владельцам.

- Какие воздействия могут нанести ущерб информации или владельцу, то есть что представляет угрозу информационной безопасности?

Дети делают свои предположения и определяются 7 направлений:

1. Кража личных данных, утечка информации
2. Вирусы, черви, трояны
3. Спам
4. Хакеры
5. Авторское право, нелицензионное ПО
6. Мошенничество
7. Дезинформация

Задачи информационной безопасности сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий.

Давайте разделимся на группы и установим, какие действия нужно предпринять, чтобы обезопасить себя от таких воздействий. Работа группами по карточкам, обсуждение - 10 минут, затем представители от каждой группы сообщают всем свои методы защиты (принимая или оспаривая), учитель принимает участие в обсуждении - разрабатывается памятка

Кража личных данных, утечка информации
- старайтесь не «светить» номер кредитки в Сети;
- совершая онлайновую покупку, обращайте внимание на защищенность канала передачи данных;
- отслеживайте файлы cookies на жестком диске, регулярно проверяйте их принадлежность и удаляйте подозрительные.
Итог урока
Учитель подводит итог урока, выставляет оценки.

Набор карточек
1 группа Утечка или кража личных данных.
Суть: Ваша персональная информация может оказаться в чужих руках, что грозит печальными последствиями, вплоть до серьезного последствия.
Факты: если у вас есть кредитная карта и банковский счет, то весьма соблазнительно выглядит перспектива оплаты услуг Internet-магазинов в режиме on-line. Действительно, это ведь так удобно! Таким образом, в Европе за прошлый год счета «облегчились» на 533 млн $.
Защита:
2 группа Вирусы.
Суть: на ваш компьютер могут напасть вредоносные программы, уничтожающие данные или приводящие к неработоспособности всего компьютера.
Факты: Вирусов стоит бояться и в оффлайновой жизни, но на просторах Internet распространение вирусов может выливаться в настоящие эпидемии. Коварные создатели вредоносных программ используют почтовые сообщения. Приходится быть осторожными с программами, которые вы скачиваете из Internet.
Защита:
3 группа Спам.
Суть: Ваш почтовый ящик начинает переполняться несанкционированными рекламными сообщениями, делая практически невозможной нормальную обработку электронной почты. Факты: Ленивые и неудачные торговцы, вместо того, чтобы заняться повышением уровня своих товаров и услуг, стремятся делать бизнес на некачественной рекламе.
Защита:
4 группа Хакеры.
Суть: В ваш компьютер могут проникнуть из Internet с целью кражи личной информации либо для использования вашего компьютера в качестве плацдарма для дальнейших атак.
Факты: Всего лишь пару лет можно было успокоить домашних пользователей, что хакерам нужен доступ только на крупные, мощные машины – теперь времена изменились. Даже информация о подключении к Internet-провайдеру (телефон+логин+пароль) – лакомая добыча для хакера.
Защита:

Приложение 1.

Вирусы, черви, трояны
Приобретите хороший антивирусный пакет, установите его в режиме максимальной безопасности, и своевременно обновляйте;
Спам

Не сообщайте посторонним ваш адрес электронной почты, особенно тот, который предоставлен провайдером или особенно важен для вас;
Пользуйтесь почтовыми серверами с установленными фильтрами.
Хакеры
Никогда не храните пароли на винчестере (даже в зашифрованном виде), не ленитесь каждый раз набирать их вручную;
От соединяйтесь от Internet при подозрении на хакерскую атаку, запускайте антивирусную программу, изменяйте пароли;
Старайтесь меньше пользоваться общедоступными программами сомнительного происхождения;
Просматривайте чаще системный реестр на предмет подозрительных записей;
Обязательно делайте резервные копии данных на дискеты или CD R/RW;
Авторское право, нелицензионное ПО
Укрепление законодательной базы;
Пресекайте попытки воровства вашего творчества;
Используйте только лицензионное ПО. Мошенничество (денежное надувательство).
Просто будьте более скептичными и менее доверчивыми. Дезинформация.
Разумный скептицизм плюс ее проверка в других средствах массовой информации.
- Рассмотрим, как можно защитить информацию из своего файла от посторонних глаз, защитить файл от изменений.
Демонстрируется презентация.
Создание текстового файла, который требует пароль при открытии
1. Необходимо нажать в строке меню Сервис / Параметры
2. Появится окно Параметры, выбрать вкладку Безопасность
3. В поле Пароль для открытия файла ввести пароль, нажать Ок
4. Появится окно о подтверждении
5. Внимание!!! Не забудьте свой пароль!

Создание текстового файла, который не позволяет вносить изменения
1. Необходимо нажать в строке меню Сервис / Защитить документ
2. Появится справой стороны панель Защита документа
3. В поле Ограничение на редактирование поставить галочку и указать вариант только чтение
4. Нажать кнопку да, включить защиту.

Практическая часть. Первичное закрепление знаний
Создайте файлы:
Работа 1, который требует пароль для открытия
Работа 2, который не позволяет вносить изменения в файл Обучающиеся создают и сохраняют файлы с необходимым условием
Домашнее задание
- Выучить записи в тетради. Ознакомить друзей с памяткой.

Приложение 2

Памятка для обучающихся

БУДЬ БДИТЕЛЕН!
Утечка или кража личных данных
– старайтесь не «светить» номер кредитки в Сети;

– совершая онлайновую покупку, обращайте внимание на защищенность канала передачи данных;
– отслеживайте файлы cookies на жестком диске, регулярно проверяйте их принадлежность и удаляйте подозрительные
Вирусы.
– приобретите хороший антивирусный пакет, установите его в режиме максимальной безопасности, и своевременно обновляйте;
Спам.
– не сообщайте посторонним ваш адрес электронной почты, особенно тот, который предоставлен провайдером или особенно важен для вас;
– пользуйтесь почтовыми серверами с установленными фильтрами.
Хакеры.
– никогда не храните пароли на винчестере (даже в зашифрованном виде), не ленитесь каждый раз набирать их вручную;
– отсоединяйтесь от Internet при подозрении на хакерскую атаку, запускайте антивирусную программу, изменяйте пароли;
– старайтесь меньше пользоваться общедоступными программами сомнительного происхождения;
– просматривайте чаще системный реестр на предмет подозрительных записей;
– обязательно делайте резервные копии данных на дискеты или CD R/RW.
Нарушение авторского права.
– укрепление законодательной базы;
– пресекайте попытки воровства вашего творчества.
Вероятность дезинформации.
– разумный скептицизм плюс ее проверка в других средствах массовой информации.
Денежное надувательство.
– просто будьте более скептичными и менее доверчивыми.

## Урок № 6 «Безопасность в сети Интернет»

Цель урока: познакомить с приемами безопасной работы в сети Интернет.
Задачи:
Образовательные: находить нужную информацию в сети Интернет, научить применять полученные знания в проектной деятельности.
Развивающие: развивать умение анализировать и систематизировать имеющуюся информацию.
Воспитательные: развивать навыки работы в группе, формировать сознательность и внимание к информационно безопасности, прививать навыки безопасного использования сети Интернет.
Оборудование: компьютер с доступом в Интернет, видеопроектор, экран
План урока:
1. Организационный момент
2. Вступление в тему
3. Плюсы и минусы Интернета

4. Советы безопасности
5. Работа в группах
6. Подведение итогов

Ход урока:

1) Организационный момент.

2) Вступление в тему

Слово учителя: Развитие глобальной сети изменило наш привычный образ жизни, расширило границы наших знаний и опыта. Теперь появилась возможность доступа практически к любой информации, хранящейся на миллионах компьютерах во всём мире. Но, с другой стороны, миллионы компьютеров получи доступ к вашему компьютеру. И не сомневайтесь, они воспользуются этой возможностью. И не когда-то, а прямо сейчас.

В повседневной жизни каждый из вас сталкивался с Интернетом. А давайте попробуем выяснить, что же такое Интернет? (ученики дают определение).

Интернет – всемирная глобальная компьютерная сеть для хранения и передачи информации. Просмотр видеоролика: «Знакомство с Интернетом»: http://www.youtube.com/ watch?v=DOaxn1JB7vE

Что из этого вы уже знали? Что было новым для вас? (ответы учащихся) Для чего вы используете Интернет? (ответы учащихся)

Всегда ли безопасно использовать всемирную сеть?

3) Плюсы и минусы Интернета

Давайте немного подумаем, сейчас на доске у нас появятся высказывания, вы должны привести аргументы за или против.

Попробуйте привести аргументы, отражающие противоположную точку зрения.

1. Интернет имеет неограниченные возможности дистанционного образования.
2. Интернет — это глобальный рекламный ресурс. И это хорошо!
3. Общение в Интернете — это плохо, потому что очень часто подменяет реальное общение виртуальному.
4. Интернет является мощным антидепрессантом.
5. В Интернете можно узнать сведения о человеке (место проживания и адрес электронной почты, номер мобильного телефона). И это хорошо!

Какие опасности подстерегают нас в сети?

(Интернет-зависимость, вредоносные и нежелательные программы, психологическое воздействие на человека, материалы нежелательного содержания, Интернет-мошенники и др.) Давайте посмотрим, как нам уберечься от этих угроз.

4) Советы безопасности

Перед тем как приступить к групповой работе (по 2 человека) давайте посмотрим с вами несколько видеороликов про безопасность в сети интернет, они вам помогут в дальнейшем в составлении памятки.

Учащимся предлагается к просмотру 3 видеоролика (по 2 мин.). Во время просмотра ребята должны подумать, какие советы они включили бы в свою памятку по безопасности в Интернете.

Просмотр видеоролика «Развлечения и безопасность в Интернете»: http://www.youtube.com/watch?v=3Ap1rKr0RCE

Просмотр видеоролика: «Остерегайся мошенничества в Интернете»: http://www.youtube.com/watch?v=AMCsvZXCd9w

Просмотр видеоролика «Как обнаружить ложь и остаться правдивым в Интернете»:http://www.youtube.com/watch?v=5YhdS7rrxt8

Какие советы кажутся вам наиболее актуальными? Давайте составим вашу собственную памятку по безопасному общению в Интернете.

Работа в группе. Составление слайда «ПАМЯТКА БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ ИНТЕРНЕТОМ».

5) Подведение итогов

Итогом урока станет памятка по безопасному поведению в сети интернет. В конце урока учащиеся высказывают свои мнения о значении Интернета и вопросов информационной безопасности.

Приложение 1.

ПАМЯТКА БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ ИНТЕРНЕТОМ

1. Преступление против собственности

- Обращайте внимание на стоимость предлагаемой Вам услуги в интернете.
- Не отправляйте смс сервисам, которые вызывают у вас подозрение.
- Помните, бесплатный сыр - только в мышеловке.

2. Угрозы, направленные на наше эмоциональное и психическое состояние

- Ни под каким предлогом не соглашайтесь на разглашение личных данных: фамилий и имен, возраста, адресов электронной почты, номеров мобильных телефонов.
- Настороженно относитесь к сообщениям, содержащим призыв о помощи или предложения встречи.

3. Угрозы, направленные на наше эмоциональное и психическое состояние

- При работе с файлами будьте осторожны, убедитесь, что документ предназначался именно для Вас, проверьте, не является ли данный файл вирусом.
- Пользуйтесь антивирусным программным обеспечением, список рекомендованных про грамм можно найти на сайте «Управление К» и «Лиги безопасного интернета».

## Урок № 7 «Безопасность в сети Интернет. Нормы поведения в сети»

Цель: обратить внимание учащихся на возможные угрозы в сети Интернет, повысить грамотность учащихся в вопросах безопасности в сети, формировать общепринятые нормы поведения в сети.

Задачи:

1. Знакомство учащихся с потенциальными угрозами, которые могут встретиться при работе в сети Интернет.
2. Выработка правила безопасного поведения в сети.
3. Выработка необходимости использования в сети общепринятых нравственных норм поведения.

Оборудование: компьютер, проектор, интерактивная доска, памятка учащимся;

Ожидаемые результаты:

- повышение уровня осведомленности учащихся о проблемах безопасности при использовании сети Интернет, потенциальных рисках при использовании Интернета, путях защиты от сетевых угроз.

- формирование культуры ответственного, этичного и безопасного использования Интернета.

План и этапы урока:

1. Введение
2. Объявление темы. Постановка задач
3. Просмотр социального ролика «Безопасный интернет – детям»
4. Сказка о золотых правилах безопасного поведения в Интернет
5. Физкультминутка
6. Рефлексия

Ход урока

1. Введение.

Создание проблемной ситуации

А сейчас я предлагаю вам отгадать загадки, чтобы понять, о чем пойдет речь на уроке.

Игра «Угадай-ка».

Что за чудо-агрегат
Может делать все подряд –
Петь, играть, читать, считать,
Самым лучшим другом стать? (компьютер.)

На столе он перед нами, на него направлен взор, подчиняется программе, носит имя... (монитор).

Не зверушка, не летаешь, а по коврику скользишь
и курсором управляешь. Ты – компьютерная... (мышь).

Нет, она – не пианино, только клавиш в ней – не счесть! Алфавита там картина, знаки, цифры тоже есть.
Очень тонкая натура. Имя ей ... (клавиатура).

Сохраняет все секреты «ящик» справа, возле ног,
и слегка шумит при этом. Что за «зверь?». (системный блок).

Есть такая сеть на свете
Ею рыбу не поймать.
В неё входят даже дети, чтоб общаться, иль играть.
Информацию черпают,
И чего здесь только нет!
Как же сеть ту называют?
Ну, конечно ж... (Интернет)

2. Объявление темы. Постановка задач.

Как вы думаете, о чём мы сегодня будем говорить?

Правильно, мы с вами поговорим об интернете, точнее о безопасности в интернете. Мы живём в эпоху Интернета, без которого, увы, сейчас трудно справиться. Интернет заменил у нас многое. Это нам облегчило жизнь. Сейчас всего лишь при помощи одного небольшого устройства мы можем обмениваться мгновенными сообщениями, покупать книги или музыку, получать любую необходимую информацию и многое другое. Интернет ворвался в нашу жизнь.

У кого дома есть компьютер? Как вы им пользуетесь? А у кого дома есть Интернет?

А как вы думаете, какая опасность может подстерегать пользователей интернета? (ответы детей).

Мы можем найти в интернете любую информацию, но некоторые сайты могут быть заражены, и наш компьютер может «заболеть».

Поэтому постарайтесь запомнить основные правила безопасного интернета.

3. Просмотр социального ролика «Безопасный интернет – детям»

(Этот ролик создала Студия Mozga.ru, приняла участие в конкурсе «Безопасный интернет -детям!», проведённом Mail.ru.)

https://www.youtube.com/watch?v=789j0eDglZQ&feature=youtu.be

4. А сейчас послушайте сказку о золотых правилах безопасного поведения в Интернет

СКАЗКА

В некотором царстве, Интернет - государстве жил-был Смайл-царевич- королевич, который правил славным городом.

И была у него невеста – прекрасная Смайл-царевна-Королевна, день и ночь, проводившая в виртуальных забавах.

Сколько раз предупреждал её царевич об опасностях, подстерегающих в сети, но не слушалась его невеста. Не покладая рук трудился Смайл-царевич, возводя город, заботился об охране своих границ и обучая жителей города основам безопасности жизнедеятельности в Интернет-государстве. И не заметил он, как Интернет-паутина всё-таки затянула Смайл-царевну в свои коварные сети. Погоревал – да делать нечего: надо спасать невесту. Собрал он королевскую – дружину. Стали думать головы мудрые, как вызволить царевну из плена виртуального. И придумали они «Семь золотых правил безопасного поведения в Интернет», сложили их в котомку Смайл- царевичу, и отправился он невесту искать. Вышел на поисковую строку, кликнул по ссылкам поганым, а они тут как тут: сообщества Змея-искусителя-Горыныча, стрелялки-убивалки Соловья- разбойника, товары заморские купцов шаповских, сети знакомств - зазывалок русалочьи… Как же найти-отыскать Смайл-царевну? Крепко задумался Смайл-королевич, надел щит антивирусный, взял в руки меч-кладенец кодовый, сел на коня богатырского и ступил в трясину непролазную. Долго бродил он, и остановился на распутье игрища молодецкого трёхуровневого, стал читать надпись на камне: на первый уровень попадёшь – времени счёт потеряешь, до второго уровня доберёшься – от родных-близких отвернёшься, а на третий пойдёшь - имя своё забудешь. И понял Смайл-царевич, что здесь надо искать невесту. Взмахнул он своим мечом праведным и взломал код игрища страшного! Выскользнула из сетей, разомкнувшихся Смайл-царевна, осенила себя паролем честным и бросилась в объятия своего суженого. Обнял он свою невесту горемычную и протянул котомочку волшебную со словами поучительными:«Вот тебе оберег от козней виртуальных, свято соблюдай наказы безопасные!»

1. Спрашивай взрослых

Если что-то непонятно, страшно или неприятно,
быстро к взрослым поспеши,
Расскажи и покажи.

Всегда спрашивай родителей о незнакомых вещах в Интернете. Они расскажут, что безопасно делать, а что нет.

2. Установи фильтр

Как и всюду на планете,
Есть опасность в интернете.
Мы опасность исключаем,

Если фильтры подключаем.
Чтобы не сталкиваться с неприятной и огорчительной информацией в интернете, установи на свой браузер фильтр, или попроси сделать это взрослых — тогда можешь смело пользоваться интересными тебе страничками в интернете.

3. Не открывай файлы

Не хочу попасть в беду —
Антивирус заведу!
Всем, кто ходит в интернет, пригодится наш совет.
Не скачивай и не открывай неизвестные тебе или присланные незнакомцами файлы из Интернета. Чтобы избежать заражения компьютера вирусом, установи на него специальную программу — антивирус!

4. Не спеши отправлять SMS

Иногда тебе в сети,
Вдруг встречаются вруны.
Ты мошенникам не верь,
Информацию проверь!
Если хочешь скачать картинку или мелодию, но тебя просят отправить смс - не спеши! Сначала проверь этот номер в интернете – безопасно ли отправлять на него смс и не обманут ли тебя. Сделать это можно на специальном сайте.

5. Осторожно с незнакомцами

Злые люди в Интернете,
Расставляют свои сети.
С незнакомыми людьми
Ты на встречу не иди!
Не встречайся без родителей с людьми из Интернета вживую. В Интернете многие люди рассказывают о себе неправду.

7. Будь дружелюбен

Сгрубиянами в сети,
Разговор не заводи.
Ну и сам не оплошай –
Никого не обижай.
Общаясь в Интернете, будь дружелюбен с другими. Не пиши грубых слов! Ты можешь нечаянно обидеть человека, читать грубости так же неприятно, как и слышать.

8. Не рассказывай о себе

Чтобы вор к нам не пришёл,
И чужой нас не нашёл,
Телефон свой, адрес, фото,
В интернет не помещай.
И другим не сообщай.
Никогда не рассказывай о себе незнакомым людям: где ты живешь, учишься, свой номер телефона. Это должны знать только твои друзья и семья!
Залилась совестливыми слезами дева красная, дала своему наречённому слово честное, что не будет пропадать в забавах виртуальных, а станет трудиться на благо народа города своего, сама начнёт обучаться и помогать будет люду заблудшему и погрязшему в трясине сетевой. И зажили они дружно и счастливо с мечтою расширить границы образования.

Тут и сказочке конец, а кто слушал - МОЛОДЕЦ!

Учитель: Какова мораль этой сказки? А сейчас немного отдохнём и поиграем.

5. Физкультминутка Игра «Вирусы»

Цель игры: Эмоциональная разрядка, снятие напряжения.

Вспомогательные материалы: Листы А4 двух цветов и лента, которой можно будет обозначить линию, разделяющую две команды.

Процедура проведения: Листы А4 нужно скомкать и сделать из них снежки двух разных цветов. Снежки одного цвета обозначают, например, вирусы, спам, зараженные файлы, снежки другого цвета – безопасная информация, безопасные файлы. Участники делятся на две команды так, чтобы расстояние между командами составляло примерно 3 м. В руках каждой команды снежки двух цветов, которые они, по команде ведущего, бросают другой команде. Задача: как можно быстрее закидать противоположную команду снежками, при этом успевая откидывать все «опасные» снежки и сохранять у себя все «безопасные». Ведущий засекает 10 секунд и, услышав команду «Стоп!», участники должны прекратить игру. Выигрывает та команда, на чьей стороне оказалось меньше «опасных» и больше «безопасных» снежков. Перебегать разделительную линию запрещено.

Учитель: Ребята, давайте попробуем почувствовать на себе вирусную атаку и постараться защититься от нее! Правила будут такие. Вам нужно разбиться на 2 команды. Но сначала из листочков бумаги черного и белого цвета сделаем снежки! Каждый должен сделать по 2снежка белого и черного цвета. Черные снежки – «опасные», а белые – «безопасные». По моей команде начинаем бросать друг в друга снежки! Задача одной команды – как можно быстрее закидать противоположную команду снежками.

Также задача каждой команды – успеть откидывать все черные снежки и сохранять у себя белые.

Сейчас я вручу каждому памятку с правилами. Прочитайте правила и постарайтесь их выполнять (вручение памяток).

6. Рефлексия

Подведём итог нашего урока. Прочитайте предложение и продолжите. Мне было интересно узнать…

Мне понравилось…Меня удивило… Мне захотелось…

Интернет может быть прекрасным и полезным средством для обучения, отдыха или общения с друзьями. Но – как и реальный мир – Сеть тоже может быть опасна!

Желаю, чтобы и в жизни, и на просторах Интернета у вас было всё просто отлично!

Памятки о правилах безопасного пользования интернетом остаются вам.

Приложение 1.

Памятка по безопасному поведению в Интернете

Это важно знать!

- Я не скажу о себе ничего (ни адреса, ни телефона, ни других сведений) без разрешения родителей.
- Я никогда не передам по Интернет своей фотографии.
- Я никогда не встречусь ни с кем, кого знаю только по Интернет, без разрешения родителей. На встречу я пойду с отцом или с матерью.
- Я никогда не отвечу на сообщение, которое заставляет меня краснеть, будь то электронное письмо или общение в чате.
- Я буду разговаривать об Интернет с родителями.

- Я буду работать только тогда, когда они разрешат мне, и расскажу им обо всем, что я делал в Интернет.

8 урок «Моя безопасность в сети»

Цель занятия: формирование культуры безопасного и эффективного использования цифровых ресурсов и устройств, знакомство с основами безопасности в сети и повышение уровня цифровой грамотности.

Структура занятия

Часть 1. Мотивационная (до 5 минут).

Педагог.

Ребята, сегодня наше занятие посвящено кибербезопасности. Жизнь современного человека трудно представить без цифровых сервисов и приложений. Мы используем их для решения самых разных повседневных задач. При этом онлайн-среда связана не только с массой полезных возможностей, но и с рисками для безопасности пользователя. Именно поэтому так важно развивать собственную цифровую грамотность, знать о возможных рисках и владеть разными методами защиты, в том числе и технологическими. Также сфера кибербезопасности активно развивается, поэтому это ещё и перспективное направление для профессионального развития.

Педагог.

В продолжение занятия предлагаю вам погрузиться в настоящее состязание кибермошенников и специалистов по информационной безопасности. Мы проведем командную игру и научимся противостоять киберугрозам, разберём типичные сценарии атак и узнаем, как пользователи могут себя защищать.

Часть 2. Основная (до 20 минут).

Описание игры «Кибербезопасность».

Класс делится на две команды – «Кибермошенники» и «Специалисты по информационной безопасности» (как вариант, можно предложить разделить класс на несколько команд - специалистов по информационной безопасности; в этом варианте педагог сам озвучивает все карточки с киберугрозами).

Каждая команда получает набор карточек с возможными действиями (см. дополнительные материалы).

Механика игры:

1. Педагог выбирает одну из карточек угроз (в любой последовательности) и озвучивает её.
2. Задача команды «Кибермошенники» — подобрать из набора карточек с действиями те, что злоумышленники типично используют в такой ситуации.
3. Задача команды «Специалисты по информационной безопасности» – оставить план защиты из своего набора карточек-действий и описать модель поведения пользователя.

На обсуждение отводится 3–5 минут.

4. «Кибермошенники» презентуют свой вариант плана «нападения», а «специалисты по информационной безопасности» – план защиты.
5. Педагог оценивает, отражена ли атака (при необходимости используя ключи к ситуациям, в которых представлены примерные планы атаки и защиты), если да, то присваивает балл команде «специалистов по ИБ».

Возможен вариант выбора команды экспертов из числа детей, которые будут качественно оценивать планы действий команд и при необходимости дополнять их.

Тематики заданий из сферы кибербезопасности, которые встречаются в игре:

- фишинговые ссылки;
- социальная инженерия;
- защита личной информации;
- защита профиля.

Карточки-угрозы, карточки-действия для команды «Кибермошенники» и «Специалисты по информационной безопасности», ключи к ситуациям представлены в Приложении к сценарию и дополнительных материалах.

Пример проведения одного тура игры «Кибербезопасность».

Педагог.

Итак, герой нашей истории молодой ученый Алексей, который давно ведёт свой профиль, у него много подписчиков, интересные и полезные научно-популярные публикации — потерять аккаунт для него будет обидно.

Первая угроза: кибермошенники пытаются совершить кражу профиля Алексея через взлом логина/пароля.

Педагог.

Команда «Кибермошенников» из своих карточек–действий составляет план атаки. Вам нужно отобрать те действия, которые злоумышленники типично используют в такой ситуации (можете добавить свои варианты действий).

Команда «Специалистов по информационной безопасности» составляет из своих карточек план защиты. Ваша задача – собрать эффективную при такой угрозе модель поведения для пользователя (можете добавить свои варианты действий).

Работа в группе 3–5 минут.

Педагог.

Время для обсуждения закончилось, давайте дадим слово каждой группе и узнаем, какие планы получились у команд. Слово команде «кибермошенников».

(Ответ представителей команды «кибермошенников».)

Педагог.

Теперь время ответить на атаку, вторая команда, вам слово.

(Ответ представителей команды «специалистов по информационной безопасности».)

Педагог.

С учетом планов команд я могу объявить победителей этого тура (Педагог комментирует ответы команд, при необходимости используя ключ с примерными планами атак и защиты, и называет команду-победителя первого тура.).

Следующие туры проходят по такой же схеме. Количество туров педагог определяет самостоятельно.

Методический комментарий.

Игра может проходить и в формате, когда все обучающиеся играют роль специалистов по информационной безопасности.

В таком варианте педагог озвучивает угрозу и выводит на экран примерный план атаки кибермошенников (из ключа к ситуациям, представленным в приложении).

Задача – всем вместе найти вариант отражения атаки и обезопасить профиль молодого ученого Алексея.

Педагог.
Теперь вы знаете чуть больше о том, как действуют мошенники онлайн и как можно предусмотреть риски. Это была отличная тренировка для вас.
Предлагаю вам из тех полезных правил для пользователя, что мы сегодня услышали и из тех, что вы можете назвать самостоятельно, составить список – топ-5 полезных привычек кибербезопасности, которые каждый из нас может начать придерживаться с сегодняшнего дня.
Обучающиеся предлагают полезные привычки кибербезопасности, педагог модерирует составление списка.
Педагог.
Спасибо вам за ваши идеи и комментарии, предлагаю подвести итоги занятия.
Часть 3. Заключение (до 5 минут).
Педагог.
Сегодня мы рассмотрели ситуации, когда пользователи не задумываются о последствиях своих действий и сами ставят себя под угрозу. Наша ответственность как пользователей цифровых сервисов — быть внимательными и стремиться повышать уровень своей цифровой грамотности. Теперь мы можем соблюдать простые правила и внедрять в свою жизнь полезные привычки кибербезопасности. Чтобы узнать больше о том, как с технической стороны обеспечивается наша с вами информационная безопасность, послушаем рекомендации от эксперта компании VK и популярного российского певца Егора Крида.
Демонстрация видео с Е. Кридом.
Приложение

| **Карточки-угрозы** |
|---|
| кража профиля пользователя через взлом логина/пароля |
| манипуляция, чтобы пользователь самостоятельно передал своиданные |
| получение доступа к сохраненным личным данным/данным банковской карты |
| продуманное мошенничество на основе доступной информации о человеке |
| мошенничество через подменные/анонимные профили |
| мошенничество на основе утечки данных пользователя на сторонних ресурсах |

Набор карточек для группы «Специалисты по информационной безопасности»

- Проверьте профиль, человека, действительно ли такой человек существует? Попросите незнакомца поподробнее рассказать о себе.

- Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.
- Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.
- Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.
- Прежде чем знакомиться в социальных сетях, внимательно изучите страницу пользователя. Есть ли у него друзья, посты, отметки на странице? Или аккаунт выглядит подозрительно?
- Не переходите по ссылкам от малознакомых людей.
- Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.
- Сравните предлагаемую цену с другими сайтами: обычно цены на поддельных сайтах подозрительно низкие.
- Не публикуйте персональные данные — например, домашний адрес, телефон, геолокации.
- Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.
- Не поддавайтесь агрессии и не введитесь на провокации.
- Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.
- Выделите время и разберитесь в настройках приватности своего профиля во всех соцсетях.
- Защищайте всю информацию, даже если думаете, что она не важна. Делясь важной или личной информацией, используйте фильтр
- «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.

Набор карточек для группы «Кибермошенники»

- Проследить за открытой информацией в профиле, изучить подробности жизни человека.
- Спровоцировать на эмоции, вызвать интерес у пользователя, использовать приём ограниченного времени.
- Начать торопить пользователя, чтобы не дать разобраться в происходящем. Разослать спам-сообщение друзьям пользователя.
- Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.
- Создать копию хорошо известного официального сайта, но в адресной строке использовать буквы, схожие по написанию с настоящим адресом.
- Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя. Отправить человеку сообщение якобы от лица организации (создать

копию профиля этой организации) о серьезной проблеме: например, сообщить о штрафе или о том, что родственник попал в беду.

- Представиться сотрудником технической поддержки и выманить конфиденциальные данные или склонить к выполнению сомнительных действий.
- Предложить продолжить знакомство офлайн и отправить ссылку для покупки билетов на мероприятие — например, в кино.
- Поставить на поддельном сайте низкую заманчивую цену на популярный товар, чтобы побудить ввести данные банковской карты.
- Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Ключи к ситуациям угрозы (примерные планы атаки и защиты)

Угроза: кража профиля пользователя через взлом логина/пароля.

Пример атаки:

1. Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.
2. Начать торопить пользователя, чтобы не дать разобраться в происходящем.
3. Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.
4. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Пример защиты:

1. Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.
2. Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.
3. Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.
4. Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.

Угроза: манипуляция, чтобы пользователь самостоятельно передал свои данные.

Пример атаки:

1. Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.
2. Поставить на поддельном сайте низкую заманчивую цену на популярный товар, чтобы побудить ввести данные банковской карты.
3. Спровоцировать на эмоции, вызвать интерес у пользователя, использовать прием ограниченного времени.

Пример защиты:

1. Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.
2. Сравните предлагаемую цену с другими сайтами: обычно цены на поддельных сайтах подозрительно низкие.
3. Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.

Угроза: получение доступа к сохраненным личным данным/данным банковской карты.

Пример атаки:

1. Предложить продолжить знакомство офлайн и отправить ссылку для покупки билетов на мероприятие — например, в кино.
2. Создать копию хорошо известного официального сайта, но в адресной строке использовать буквы, схожие по написанию с настоящим адресом.
3. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).

Пример защиты:

1. Прежде чем знакомиться в социальных сетях, внимательно изучите страницу пользователя. Есть ли у него друзья, посты, отметки на странице? Или аккаунт выглядит подозрительно?
2. Проверьте профиль, человека, действительно ли такой человек существует? Попросите незнакомца поподробнее рассказать о себе.
3. Не переходите по ссылкам от малознакомых людей.
4. Защищайте всю информацию, даже если думаете, что она не важна. Угроза: продуманное мошенничество на основе доступной информации о человеке.

Пример атаки:

1. Создать профиль, похожий на официальный профиль администрации сайта. Выдать себя за администраторов и модераторов сайта, чтобы получить данные или пароль пользователя.
2. Проследить за открытой информацией в профиле, изучить подробности жизни человека.
3. Разослать спам-сообщение друзьям пользователя.

Пример защиты:

1. Не публикуйте персональные данные — например, домашний адрес, телефон, геолокации.
2. Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.
3. Настройте двухфакторную аутентификацию в соцсетях, чтобы аккаунт не перешел в руки недоброжелателей. Привяжите актуальный номер вашего телефона к профилю, а

также укажите ваши настоящие имя, фамилию, установите реальное фото: так восстановить профиль в случае взлома будет проще.

4. Не поддавайтесь агрессии и не введитесь на провокации. Угроза: мошенничество через подменные/анонимные профили. Пример атаки:

1. Проследить за открытой информацией в профиле, изучить подробности жизни человека.
2. Отправить человеку сообщение якобы от лица организации (создать копию профиля этой организации) о серьезной проблеме: например, сообщить о штрафе или о том, что родственник попал в беду.
3. Создать и оформить сайт так, чтобы он был очень похож на официальный, где пользователю предлагается оплатить штраф или просто купить какой-то товар или услугу.
4. Начать торопить пользователя, чтобы не дать разобраться в происходящем.

Пример защиты:

1. Запросите больше информации о том, что вам предлагают. Проверьте официальный сайт компании, от лица которой вам пишут и уточните информацию о контактах службы поддержки.
2. Не поддавайтесь агрессии и не введитесь на провокации.
3. Делясь важной или личной информацией, используйте фильтр «Только для друзей». Не делитесь в интернете важной информацией: фото паспорта и других документов, билетов, посадочных талонов и др.
4. Выделите время и разберитесь в настройках приватности своего профиля во всех соцсетях.
5. Воспользуйтесь функцией «Пожаловаться» на комментарий, человека, пост в службу модерации в социальной сети или «Добавить в спам» в своем почтовом ящике.

Угроза: мошенничество на основе утечки данных пользователя на сторонних ресурсах.

Пример атаки:

1. Совершить покупки с аккаунта пользователя, если данные банковской карты сохранены в профиле и не требуют дополнительного подтверждения (двухфакторной аутентификации).
2. Разослать спам-сообщение по друзьям пользователя.

Пример защиты:

1. Авторизуйтесь через свои аккаунты и вводите данные только на официальных сайтах.
2. Не переходите по ссылкам от малознакомых людей.
3. Проверьте адресную строку сайта. Внимательно изучайте любой сайт, на котором вам предлагается ввести какие-либо конфиденциальные данные.
4. Используйте разные пароли на различных сервисах. Выбирайте сложные пароли, не используйте ваши имя и дату рождения при создании пароля.
5. Защищайте всю информацию, даже если думаете, что она не важна.

## МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ДЛЯ КЛАССНОГО ЧАСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Старшая школа (10 - 11 классы)

Цель: создание условий для повышения уровня грамотности учащихся в вопросах информационной безопасности, расширение знаний учащихся о кибербезопасности и киберугрозах, формирование навыков их распознавания и оценки рисков, их минимизация

Задачи:

- ознакомить учащихся с нормативно-правовой базой;
- ознакомить обучающихся с адресами помощи в случае интернет- угрозы и интернет-насилия, номером всероссийского детского телефона доверия;
- выявить и обсудить основные правила обеспечения информационной безопасности в сети Интернет, научиться выявлять риски и минимизировать их;
- закрепить полученные знания путем выполнения творческого задания. Ожидаемые результаты: повышение уровня осведомленности учащихся о проблемах информационной безопасности при использовании сети Интернет, умение оценивать потенциальные риски и минимизировать их.

В рамках урока «Информационная безопасность» в старших классах целесообразно познакомить обучающихся с международными стандартами в области информационной безопасности детей, которые отражены в российском законодательстве:

- Федеральный закон Российской Федерации № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» (Закон определяет информационную безопасность детей как состояние защищѐнности, при котором отсутствует риск, связанный с причинением информацией (в том числе распространяемой в сети Интернет) вреда их здоровью, физическому, психическому, духовному и нравственному развитию.);
- № 252-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию», (направленный на защиту детей от разрушительного, травмирующего их психику информационного воздействия, переизбытка жестокости и насилия в общедоступных источниках массовой информации, от информации, способной развить в ребѐнке порочные наклонности, сформировать у ребѐнка искаженную картину мира и неправильные жизненные установки.)

Необходимо обратить внимание обучающихся на классификацию вредоносных информационных ресурсов:

- информация, причиняющая вред здоровью и (или) развитию детей;
- информация, запрещенная для распространения среди детей;
- информация, ограниченнаядля распространения среди детей определенных возрастных категорий.

На уроке необходимо затронуть следующие аспекты:
- перечень рисков, подстерегающих ребенка в сети Интернет;
- рекомендации по грамотному использованию электронной почты;
- технологии безопасного общения в средах мгновенного обмена сообщениями.

Необходимо обеспечить обучающихся:
- инструкциями по безопасному общению в чатах;
- советами по профилактике и преодолению Интернет-зависимости;
- общими правилами по безопасности детей в сети Интернет.

Также рекомендуется рассмотреть следующие объекты, являющиеся опасными в Интернете:
- нежелательные программы;
- защита личных данных;
- мошенничество;
- виртуальные «друзья»;
- пиратство;
- on-line-игры;
- этика;
- критический подход к информации.

Важно обеспечить обучающихся информацией о программном обеспечении, позволяющим осуществлять безопасную работу в сети Интернет, контентной фильтрации.

Важно ознакомить обучающихся с адресами помощи в случае интернет-угрозы и интернет-насилия, номером всероссийского детского телефона доверия (https://politech47.mskobr.ru/files/informaciya_o_liniyah_pomowi_v_slu chae_internet-ugroz.pdf).

Линия помощи в случаях Интернет-угроз «Горячая линия». На «Горячую линию» можно попасть круглосуточно, набрав адрес www.saferunet.ru и нажав на красную кнопку «Горячая линия».

Линия помощи «Дети онлайн». Линия помощи «Дети онлайн» – служба телефонного и онлайн консультирования для детей и взрослых по проблемам безопасного использования детьми и подростками Интернета и мобильной связи. Обратиться на «Линию помощи» можно:
- по телефону 8 800 250 00 15 (с 9 до 18 по рабочим дням, время московское)
- по электронной почте helpline@detionline.com •
- на сайте www.detionline.com

Возможные формы проведения урока в 9-11 классах – лекция, деловая игра, урок-презентация проектов, мозговой штурм «Интернет- безопасность», дискуссия, дебаты, встреча со специалистами медиа-сферы, системными администраторами и т.д.

Для учащихся старших классов средней школы будет актуальным урок с использованием кейс-технологии.

Кейс «Новый смартфон для отца»

Илья Комаров, студент 4-го курса экономического факультета, вернулся домой после сдачи последнего экзамена зимней сессии. Экзамен был сдан на «отлично», и настроение у Ильи было соответствующим. Тем более что на телефон пришло сообщение от банка о начисление первой заработной платы от крупной энергетической компании, где он проходил стажировку.

Особенно его обрадовало начисление обещанной премии в размере 15000 рублей. Теперь у Ильи наконец-то появились деньги для покупки подарка ко дню рождения отца.

Выбирать подарок Илье не пришлось, недавно у его отца, Петра Петровича Комарова, сломался телефон. Вирусное приложение не только

«съело» все деньги со счета отца, но и безвозвратно повредило операционную систему старенького смартфона. Илья однозначно решил подарить отцу новый смартфон.

Он привычным движением открыл ноутбук и начал изучать предложения различных магазинов, сравнивая цены и параметры предлагаемых моделей.

Полчаса поисков в интернете привели Илью на сайт интернет- магазина, предлагающего современные устройства по низкой цене.

Информация с сайта интернет-магазина:

1. Интернет адрес: http://i-crop.ru/
2. Указанный адрес: г. Калининград.
3. Происхождение товара: таможенный конфискат.
4. Цены на товары: на 50% меньше рыночных.
5. Способ оплаты: кошелек QIWI.
6. Сроки доставки: от 1 -го до 20-ти дней.
7. Гарантии: Опись вложения содержимого бандероли.

Характеристика роли в ситуации. Представьте себя на месте советника по личной информационной безопасности, к которому обратился Илья Комаров.

Постановка задачи. Помогите Илье оценить безопасность покупки в данном интернет-магазине. Ответьте на поставленные вопросы:

1. Какая представленная информация вызывает доверие у потенциального клиента?
2. Выделите незнакомые понятия, которые присутствуют в тексте, и дайте им определение.
3. Какая информация на сайте не вызывает вашего доверия?
4. Каким образом можно проверить добросовестность интернет-магазина? Перечислите как можно больше способов.
5. Какой совет вы бы дали Илье Комарову?

За дополнительной информацией вы можете обратиться на сайт или в приложение к кейсу (см. ниже).

Приложение

О магазине. Мы находимся в г. Калининград и успешно работаем с 2005 года! Аппараты были изъяты у различных фирм и предпринимателей при попытке контрабандного ввоза в Россию, без уплаты таможенной пошлины и соответствующих налогов. Как правило, предприниматели, желающие сэкономить на уплате налогов, пытаются провезти контейнеры со смартфонами и планшетами под видом радиодеталей или радиоэлектронного лома, на которые таможенная пошлина на ввоз существенно ниже, чем

на мобильные телефоны и планшетные компьютеры. Наша цель - максимально быстро реализовать товар, поэтому мы устанавливаем столь доступные цены.
Вся продукция - оригинальная, от официальных производителей. Техника поставляется из США и Европы. Мы не продаем китайские подделки. На весь товар предоставляется гарантия 1 год. Гарантийное обслуживание обеспечивают официальные сервисные центры на территории РФ. Все телефоны русифицированы. Комплектация полная (заводская).
Мы всегда отправляем заказы своим клиентам посылкой с описью вложения содержимого. В этом случае сотрудники почты обязаны в Вашем присутствии вскрыть посылку до оплаты наложенного платежа, чтобы сверить содержимое посылки с описью. Таким образом, Вы сможете убедиться, что в посылке действительно находится мобильный телефон или планшетный компьютер надлежащего качества. Перед отправкой посылки заказчику, товар проверяется на отсутствие дефектов или брака. Данные условия гарантируют отсутствие в изделии дефектов и удовлетворяют законным требованиям Потребителя в течении гарантийного срока с момента передачи товара потребителю».
Доставка и оплата. Доставка осуществляется Почтой России или курьером службы экспресс-доставки DHL по всей территории РФ и СНГ. Самовывоза нет. Оплата только через QIWI кошелек (VISA QIWI Wallet).
СПОСОБЫ ДОСТАВКИ:
1. Доставка курьером экспресс-почты DHL: 1-3 дня (только при условии полной предоплаты заказа).
2. Доставка бандеролью наложенным платежом: 7-20 дней (требуется оплата гарантийного взноса 500 рублей*).
*Гарантийный взнос — это обязательное и неоспоримое условие, которое гарантирует серьезность Вашего намерения приобрести товар. Сумма гарантийного взноса не зависит от модели телефона или планшетного компьютера и составляет 500 рублей за каждую единицу
товара. Доставка по России и СНГ - бесплатно. Экспресс-доставка курьером DHL также осуществляется бесплатно, но только после полной предоплаты заказа.
ОПЛАТА ЧЕРЕЗ QIWI КОШЕЛЕК:
1. Зарегистрируйтесь на сайте QIWI кошелька "VISA QIWI Wallet" (используйте тот же номер телефона, который укажете в заказе).
2. Пополните счет QIWI кошелька на сумму равную стоимости заказа или гарантийный взнос 500 рублей (см. способы пополнения).
3. На сайте WWW.QIWI.COM войдите в свой кошелек и выберите ПЕРЕВЕСТИ -> ПО E-MAIL.
4. В форме перевода укажите сумму, равную стоимости заказа или гарантийный взнос 500 рублей и e-mail platezh@i-crop.ru. Оплатите.
5. Сообщите на наш e-mail (info@i-crop.ru) номер заказа, номер Вашего телефона, сумму платежа, дату и время перевода.
6. Заказ будет отправлен на следующий день. Мы сообщим Вам трек-номер для отслеживания посылки.
Пополнить QIWI кошелек можно через QIWI терминалы, банковской картой, со счета мобильного телефона и многими другими способами.
Если Вы выбрали способ "доставка наложенным платежом", то при получении посылки Вас попросят оплатить наложенный платеж в кассе почтового отделения.

Для чего требуется гарантийный взнос: это вынужденная мера с нашей стороны, поскольку у нас часто бывают случаи, когда заказчик, по независящим от нас причинам, не является на почту и не выкупает посылку с заказом, в результате чего нам приходится платить за пересылку посылки в оба конца + почтовый сбор за хранение посылки на почте сверх установленного срока. В связи с этим, чтобы избежать лишних финансовых потерь, мы просим Вас оплатить гарантийный взнос. Схема здесь действует следующая: если Вы не являетесь на почту и не выкупаете посылку, то сумма гарантийного взноса покрывает наши расходы, затраченные на пересылку товара в оба конца. Никакого перерасхода с Вашей стороны не будет, так как при отправке заказа сумма гарантийного взноса вычитается из его стоимости. Просим Вас с пониманием отнестись к данным условиям.

Материалы для педагога по обсуждению кейса Какая информация призвана вызвать доверие у клиента: Срок существования магазина

Указанная информация призвана вызывать доверие к магазину у покупателей. Однако написать на сайте все что угодно. Поэтому подобной информации не следует доверять.

Что такое Русификация?

Русификация в информатике - приспособление аппаратного и программного обеспечения к работе с русским языком; переход на использование русского языка в интерфейсе компьютеров и компьютеризованной бытовой техники.

Самое интересное что одним из признаков контрабандного товара (которым якобы торгуют владельцы магазина) является отсутствие русификации. А если заводская(лицензионная) русификация на оборудовании все-таки произведена значит оборудование уже на заводе планировалось поставлять в Россию. Тогда как он мог стать контрабандным?

Не знакомые понятия:

Что такое QIWI КОШЕЛЕК?

Электронная платежная система QIWI кошелек создана в 2006 году. С помощью QIWI кошелька можно не только оплачивать услуги связи, но и покупки в интернет магазинах. Сам по себе QIWI кошелек безопасен. Вызывает подозрение то, что интернет магазин работает ТОЛЬКО С QIWI КОШЕЛЬКОМ!!!

Что такое ТАМОЖЕННЫЙ КОНФИСКАТ?

Понятно, что это импортный товар, который прошел через таможню. Но вот словом "конфискат" обычно в русском языке означают что-то конфискованное. По закону, всё конфискованное на таможне храниться до решения суда. А после вынесения решения суда конфискованный (без слова таможенный) товар либо продают (безопасный товар) либо сжигают (небезопасный товар).

Что такое Наложеный платеж?

Наложенный платёж — денежная сумма, которую почта взыскивает по поручению отправителя с адресата при вручении последнему почтового отправления, и которая пересылается отправителю (или указанному им лицу) почтовым или телеграфным переводом.

Т.е. вы оплачиваете свою покупку на почте, когда забираете товар. А почтовые работники отправляют полученные средства продавцу. Наложный платеж является одним из самых безопасных способов оплаты интернет- покупки. Особенно если производится Опись содержимого посылки.

Трек-номер (Почтовый идентификатор)

При помощи почтового идентификатора, возможно, узнать о местонахождении и состоянии почтового отправления. Добросовестные продавцы действительно отправляют своим клиентам Трек-номера, которые позволяют следить за доставкой. Мошенники всегда стараются вызвать доверие мнимой прозрачностью своей деятельности.

Что такое ОПИСЬ ВЛОЖЕНИЯ БАНДЕРОЛИ?

Опись вложения – это бланк утвержденной формы, который заполняет отправитель. В бланке перечисляются все вложения, каждому вложению присваивается оценочная стоимость. Опись вложения защищает от воровства на ПОЧТЕ. А значит гарантией честности магазина быть не может.

Информация, не вызывающая доверия:

Отсутствие полного юридического адреса

Мошенники всегда стараются скрыть свою личность. Если на сайте нет указания юридического адреса продавца. То скорее всего владельцы сайта мошенники. И в том случае если ваша покупка не будет вам доставлена вы даже не сможете написать заявление в правоохранительные органы.

Гарантийный платеж

Тревожный признак. Согласитесь, странно получается, с одной стороны продавец уверяет что товар вам понравиться, и он надлежащего качества, с другой он боится, что вы откажетесь от доставленного товара. Эти 500 рублей мошенники оставят себе, и конечно же никакого товара вы не получите.

Полная предоплата как обязательное условие

Тревожный признак. Полная предоплата, тем более проведенная переводом с QIWI кошелька, фактически означает что вы просто подарили мошенникам деньги. Достойные доверия интернет-магазины не работают по такой схеме.

Отсутствие самовывоза

Тревожный признак. Скорее всего, у мошенников нет даже офиса. Работают и отвечают клиентам из интернет-кафе или с домашнего компьютера.

Перевод через QIWI кошелек по электронному адресу

Тревожный признак. E-mail нельзя отследить, и соответственно очень сложно установить личность продавца.

Для проверки добросовестности магазина можно предпринять следующие действия:

1. Проверить отзывы о магазине на форумах. Если отзывы отрицательные воздержитесь от покупки.
2. Проверить входит ли магазин в черный список, воспользовавшись соответствующим сайтом. Если магазин входит в черный список -воздержитесь от покупки.
3. Проверить срок регистрации сайта. Если срок регистрации домена очень мал и не соответствует заявленному сроку существования
интернет-магазина. Воздержитесь от покупки.
4. Проанализируйте всю открытую информацию.Найдите все незнакомые понятия и узнайте, что они значат.

Совет Илье Комарову:

Воздержаться от покупки. Приобрести телефон в надежном интернет-магазине.

**ПРИЛОЖЕНИЕ 1**

**НАГЛЯДНЫЙ МАТЕРИАЛ «БЕЗОПАСНЫЙ ИНТЕРНЕТ»**

Реальная жизнь или жизнь в сети: что выбираешь ты? https://ligainternet.ru/wp-content/uploads/2022/09/vremya-v-seti-web.pdf

## СКОЛЬКО ВРЕМЕНИ СТОИТ ПРОВОДИТЬ В ИНТЕРНЕТЕ?

Знаешь ли ты, кто такой Билл Гейтс? Это один из создателей операционной сети Windows, которая, скорее всего, стоит и на твоем компьютере. Можно сказать, что именно этот человек создал для нас те компьютеры, которыми мы пользуемся. Как ты думаешь, сколько времени в день он разрешал своим детям проводить за компьютером?

**Ответ тебя удивит: 45 минут в будни и 1 час 45 минут в выходные. При этом он не разрешал детям пользоваться компьютером вечером перед сном, а до 14 лет и вовсе не давал им в руки гаджетов.**

Другой известный человек, исполнительный директор 3D Robotics Крис Андерсон ввёл родительский контроль и лимитировал время на все электронные устройства в доме. Он на своем примере убедился, к чему приводит слишком тесное взаимодействие с электронными гаджетами. По мнению Андерсона, опасность новых технологий заключается во вредном контенте и появляющейся зависимости от электронных новинок.

**Почему так? Да потому что эти люди больше других знают об опасности, которую несет Интернет-зависимость для здоровья и психики пользователей.**

**Такие развлечения легко вызывают самую настоящую зависимость. Будь внимателен и сам старайся следить за собой. Бей тревогу, если заметил у себя следующие признаки:**

1. Не ложишься спать, предварительно не посидев в смартфоне.
2. Каждый день ешь за компьютером или со смартфоном в руке.
3. Почти все выходные проводишь в Интернете, никуда не выходя.
4. Злишься или раздражаешься, когда приходится отложить смартфон или оторваться от Интернета.
5. Играешь в компьютерные игры два и более раз в неделю.
6. Сидишь в социальных сетях или «болталках» в ночное время.
7. Не высыпаешься, часто испытываешь головные боли или неприятные ощущения в глазах.

**Если ты хочешь избежать Интернет-зависимости, то старайся придерживаться следующих правил:**

1. **Сократи время использования гаджетов и компьютера.**
2. **Не бери в руки телефон хотя бы за час до того, как планируешь лечь спать.** Интернет, соцсети или игры могут вызвать яркие эмоции, которые помешают уснуть.
3. **Не ешь за компьютером и не используй телефон во время еды.** Отвлекись от них ненадолго, лучше вместо этого пообщайся с родственниками или друзьями.
4. **Старайся на выходных использовать компьютер и гаджеты как можно меньше.** В Интернете или в играх очень легко «зависнуть» и весь день пролетит незамеченным, а ты потом будешь сожалеть о потерянном свободном времени.


**ПРИЛОЖЕНИЕ 2**

**ИНТЕРНЕТ-ЗАВИСИМОСТЬ: ШКАЛА ОЦЕНКИ ЗАВИСИМОСТЬ ОТ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА, ИНТЕРНЕТА**[2]

Шкала оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему

Вопросы предъявляются в случайном порядке. Оценка производится в баллах в соответствии с выбранным респондентом вариантом ответа. Набранные баллы группируются в 4 субшкалы, в зависимости от набранных по ним баллов выводится итоговая оценка.

| № | Вопросы | Варианты ответов и баллы | | | |
|---|---|---|---|---|---|
| | | нико- гда | редко | часто | все- гда |
| | Субшкала 1 – Влечение | | | | |
| 1 | Ваш ребенок в свободное от других занятий время мечтает только о том, чтобы побыстрее сесть за компьютер или взять в руки мобильное устройство | 0 | 1 | 2 | 3 |
| 2 | Ваш ребенок при возможности выбирать между разными вариантами проведения досуга останавливает свой выбор на взаимодействии с компьютером или мобильным устройством | 0 | 1 | 2 | 3 |
| 3 | Как только появляется малейшая возможность сесть за компьютер или взять в руки мобильное устройство, ваш ребенок немедленно делает это | 0 | 1 | 2 | 3 |

| | | | | | |
|---|---|---|---|---|---|
| 4 | Ваш ребенок готов без разбора посещать любые сайты, играть в любые игры, пользоваться любыми программами, лишь бы только пользоваться компьютером или мобильным устройством | 0 | 1 | 2 | 3 |
| 5 | Вы замечали, что приступив к работе с компьютером или с мобильным устройством, ваш ребенок становится подвижным, возбужденным, у него дрожат руки, он пишет друзьям много сообщений, не обращая особого внимания на их смысл | 0 | 1 | 2 | 3 |
| 6 | Вы замечали, что если ребенок некоторое время (несколько дней, месяц) не мог воспользоваться компьютером или мобильным устройством, то снова получив его в свое распоряжение, он стал проводить за ним намного больше времени, чем прежде | 0 | 1 | 2 | 3 |
| | Минимальное число баллов – 0, максимальное – 18, группа риска – 9 и более, достоверно присутствует патологическое влечение – 12 и более | | | | |
| | Субшкала 2 – Утрата контроля | | | | |
| 7 | Если ваш ребенок сел за компьютер или взял в руки мобильное устройство, чтобы поработать пять минут, он неизбежно просидит за ним час или два | 0 | 1 | 2 | 3 |
| 8 | Ваш ребенок ведет себя так, словно играет на компьютере или работает с мобильным устройством, хотя ни компьютера, ни планшета у него в настоящее время нет | 0 | 1 | 2 | 3 |
| 9 | Ваш ребенок использует для работы с Интернет одновременно два или более устройств, хотя в этом нет тех нической необходимости* | 0 | 1 | 2 | 3 |
| 10 | Ваш ребенок использует для работы с Интернет одновременно две или более программ, хотя в этом нет технической необходимости** | 0 | 1 | 2 | 3 |
| 11 | Ваш ребенок пользуется малейшей возможностью, чтобы продлить время взаимодействия с компьютером или мобильным устройством | 0 | 1 | 2 | 3 |
| 12 | Ваш ребенок всегда мечтает о приобретении нового компьютера или мобильного устройства, даже если его собственное – новое и ультрасовременное | 0 | 1 | 2 | 3 |
| | * – исключаются случаи, когда использование второго устройства является технически необходимым или оправданным, например, при получении на смартфон пароля для доступа к сетевым сервисам<br>** – исключаются случаи, когда использование второй программы является технически необходимым или оправданным, например, | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | использование программ-переводчиков или при импорте/экспорте содержимого из одного программного продукта в другой, при конвертации файлов | | | | |
| | Минимальное число баллов – 0, максимальное – 18, группа риска – 9 и более, достоверно присутствует утрата контроля – 12 и более | | | | |
| | Субшкала 3 – Абстинентный синдром | | | | |
| 13 | Вы замечали, что у вашего ребенка, лишенного возможности взаимодействовать с компьютером или мобильным устройством***, меняется настроение, появляются головные боли, боли в мышцах, раздражительность, тревога**** | 0 | 2 | 4 | 6 |
| 14 | Вы замечали, что ваш ребенок, лишенный возможности взаимодействовать с компьютером или мобильным устройством***, становится возбужденным, суетливым, он потеет, у него дрожат руки, он ищет компьютер (телефон) или замену им вплоть до пульта от телевизора или детской игрушки**** | 0 | 2 | 4 | 6 |
| 15 | Вы замечали, что ваш ребенок, лишенный возможности взаимодействовать с компьютером или мобильным устройством***, совершает акты вандализма, рвет книги, ломает мебель, отказывается от еды, угрожает самоубийством**** | 0 | 2 | 4 | 6 |
| 16 | Вы замечали, что ваш ребенок, лишенный возможности взаимодействовать с компьютером или мобильным устройством***, становится угнетенным, грустным, малоподвижным, монотонным, говорит тихим голосом, заявляет о бессмысленности своего существования**** | 0 | 2 | 4 | 6 |
| 17 | Вы замечали, что ваш ребенок, лишенный возможности взаимодействовать с компьютером или мобильным устройством***, становится гневливым и агрессивным, сердитым и злым, лезет в драку и/или сам причиняет себе боль или повреждения, в том числе – опасные**** | 0 | 2 | 4 | 6 |
| 18 | Вы замечали, что ваш ребенок, лишенный возможности взаимодействовать с компьютером или мобильным устройством***, становится демонстративным и капризным, жалуется на боли в разных частях тела, на удушье, головокружения, падает в обмороки, испытывает приступы страха, паники**** | 0 | 2 | 4 | 6 |

*** - подразумевается, что лишение контакта с компьютером или мобильным устройством носит продолжительный характер

**** - чтобы ваш ответ был утвердительным, достаточно наличия одного из перечисленных в вопросе симптомов

Минимальное число баллов – 0, максимальное – 36, группа риска – 12 и более, достоверно присутствует абстиненция – 18 и более

| | Субшкала 4 – Рост толерантности и | поглощенность активностью | |
|---|---|---|---|
| № | Вопросы | Варианты ответов и баллы | |
| | | Нет | Да |
| 19 | Ваш ребенок тратит на взаимодействие с компьютером и/или мобильным устройством в среднем более2 часов в день и это время день за днем увеличивается***** | 0 | 6 |
| 20 | Ваш ребенок, если его не ограничивать, проводит за компьютером или с мобильным устройством все свое время, в ущерб посещению школы, питанию, ночному сну | 0 | 6 |
| 21 | Создаваемые вашим ребенком в Сети виртуальные образы (в социальных сетях, на форумах, в чатах, в сетевых играх) значительно отличаются от реального (в том числе – по возрасту, полу) | 0 | 6 |
| 22 | У вашего ребенка отмечается резкое сужение круга интересов, фиксация на игре или сетевой активности, сопровождавшиеся эмоциональной вовлеченностью, поглощенностью своими игровыми успехами или накоплением виртуальных друзей на своей странице в социальной сети | 0 | 6 |
| 23 | У вашего ребенка отмечается перенос в сферу сетевой активности большинства социальных контактов и многих социальных и даже биологических по своей природе действий, в частности – творческой активности, просмотра кинофильмов и прослушивания музыки, установления дружеских и партнерских отношений, вплоть до виртуальных сексуальных контактов | 0 | 6 |
| 24 | У вашего ребенка в связи с много-часовой ежедневной сетевой активностью, требующей значительных психических и физических усилий, отмечались выраженное переутомление, формирование астеноневротических реакций (заикания, тиков, обморочных состояний, энуреза, хронической головной боли и других) | 0 | 6 |

***** - исключаются случаи, когда работа за компьютером или с мобильным устройством объективно является необходимой (например, для получения высоких результатов в

учебе, спорте или хобби); включаются игры, посещение сайтов развлекательной тематики, социальных сетей и т.д.

---

Минимальное число баллов – 0, максимальное – 36, группа риска – 12 и более, достоверно присутствует рост толерантности и поглощенность активностью – 18 и более

---

Варианты ответов респонденту после завершения тестирования

Вариант 1. Шкала “влечение” – меньше 9 баллов, шкала “утрата контроля” – меньше 9 баллов, шкала “абстинентный синдром” – меньше 12 баллов, шкала “рост толерантности и поглощенность” – меньше 12 баллов.

Ответ 1. В результате тестирования по шкале оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему, у вашего ребенка не выявлено признаков интернет–аддикции. Если продолжаете сомневаться, обратитесь с ребенком к врачу для очной консультации.

Вариант 2. Шкала “влечение” – больше 9, но меньше 12 баллов и/или шкала “утрата контроля” – больше 9, но меньше 12 баллов, шкала “абстинентный синдром” – меньше 12 баллов, шкала “рост толерантности и поглощенность” – меньше 12 баллов.

Ответ 2. В результате тестирования по шкале оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему, у вашего ребенка не выявлено достоверных признаков интернет–аддикции, однако имеется значительный риск ее формирования. Пожалуйста, обратитесь с ребенком к врачу, на данном этапе возможна успешная профилактика дальнейшего развития зависимости.

Вариант 3. Шкала “влечение” – больше 12 баллов и/или шкала “утрата контроля” – больше 12 баллов, шкала “абстинентный синдром” – меньше 12 баллов, шкала “рост толерантности и поглощенность” – меньше 12 баллов.

Ответ 3. В результате тестирования по шкале оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему, у вашего ребенка с высокой вероятностью имеется интернет–зависимость, предположительно I стадии. Пожалуйста, обратитесь с ребенком к врачу для верификации диагноза и разработки индивидуальной программы лечения и реабилитации.

Вариант 4. Шкала “влечение” – больше 12 баллов и/или шкала “утрата контроля” – больше 12 баллов, шкала “абстинентный синдром” – больше 12, но меньше 18 баллов и/или шкала “рост толерантности и поглощенность” – больше 12, но меньше 18 баллов.

Ответ 4. В результате тестирования по шкале оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему, у вашего ребенка с высокой вероятностью имеется интернет–зависимость, предположительно I стадии с намечающимся переходом во II стадию. Пожалуйста, обратитесь с ребенком к врачу для верификации диагноза и разработки индивидуальной программы лечения и реабилитации.

Вариант 5. Шкала “влечение” – больше 12 баллов и/или шкала “утрата контроля” – больше 12 баллов, шкала “абстинентный синдром”

– больше 18 баллов и/или шкала “рост толерантности и поглощенность” – больше 18 баллов.

Ответ 5. В результате тестирования по шкале оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему у вашего

ребенка с высокой вероятностью, имеется интернет–зависимость, предположительно II стадии. Пожалуйста, обратитесь с ребенком к врачу для верификации диагноза и разработки индивидуальной программы лечения и реабилитации.

Вариант 6. Шкала “влечение” – меньше 12 баллов и шкала “утрата контроля” – меньше 12 баллов, шкала “абстинентный синдром”– больше 12 баллов и/или шкала “рост толерантности и поглощенность” – больше 12 баллов.

Ответ 6. В результате тестирования по шкале оценки зависимости от персонального компьютера, Интернета и мобильных устройств, обеспечивающих доступ к нему, относительно состояния вашего ребенка получены противоречивые данные, не поддающиеся интерпретации. Пожалуйста, понаблюдайте за ребенком внимательно несколько дней и повторите тестирование или обратитесь с ребенком к врачу для очной консультации.

## ЛИТЕРАТУРА


1. Департамент образования Администрации г. Перми Муниципальное бюджетное учреждение «Центр психолого-педагогической, медицинской и социальной помощи» г. Пермь, 2022.
2. Пережогин, Л.О. Интернет-зависимость : предпосылки формирования, клиническая картина, лечение и профилактика : методические рекомендации / Л. О. Пережогин, А. А. Федонкина. - М.:ФГБУ “НМИЦ ПН им. В.П. Сербского» Минздрава России, 2024. – 33 с.
3. Цветкова, М.С. Информационная безопасность. 2–11 классы : методическое пособие для учителя / М. С. Цветкова. — М.: БИНОМ. Лаборатория знаний, 2020. — 64с.— ISBN 978-5-9963-5730-7.
4. Методический сборник для подготовки и проведения классного часа для школьников по вопросам информационной безопасности / А. К. Балагурова. – Чита: ГУ ДПО «ИРО Забайкальского края», 2022. – 42 с.


## ИНТЕРНЕТ-РЕСУРСЫ


1. Безопасный Интернет : материалы для учащихся начальных классов к «Уроку безопасного Интернета» : [презентация] // Лига безопасного Интернета : [сайт]. –URL:https://ligainternet.ru/wp-content/uploads/2022/10/materialy-dlya-uchashhixsya-nachalnyx-klassov-k-uroku-bezopasnogo-interneta.pdf(дата обращения: 19.08.2024)
2. Методические рекомендации по проведению уроков безопасного Интернета в школах : [презентация] // Лига безопасного Интернета : [сайт].–URL: https://ligainternet.ru/wp-content/uploads/2022/10/metodicheskie-rekomendacii-po-provedeniyu-urokov-bezopasnogo-interneta-v-shkolax.pdf (дата обращения:

19.08.2024)