

# **«Безопасность детей в Интернет»**

**Правовые, психологические,  
технические аспекты безопасной  
работы в Интернет**

# Интернет — мир широких возможностей



## Интернет позволяет вам:

- общаться с друзьями, семьей, коллегами;
- получать доступ к информации и развлечениям;
- учиться, встречаться с людьми и узнавать новое.

# Защита и безопасность в Интернете

**Защита.** Необходимо защищать компьютеры при помощи современных технологий подобно тому, как мы защищаем двери в наших домах.

**Безопасность.** Наше поведение должно защищать от опасностей Интернета.



# Основные угрозы безопасности компьютера



## Вирусы и программы-черви

Программы, проникающие в компьютер для копирования, повреждения или уничтожения данных.



## Программы-трояны

Вирусы, имитирующие полезные программы для уничтожения данных, повреждения компьютера и похищения личных сведений.



## Программы-шпионы

Программы, отслеживающие ваши действия в Интернете или отображающие навязчивую рекламу.

# Основные угрозы безопасности детей в Интернете



## Киберхулиганы

И дети, и взрослые могут использовать Интернет, чтобы изводить или запугивать других людей.



## Хищники

Эти люди используют Интернет для того, чтобы заманить детей на личную встречу.



## Злоупотребление общим доступом к файлам

Несанкционированный обмен музыкой, видео и другими файлами может быть незаконным или повлечь загрузку вредоносных программ.



## Неприличный контент

Если дети используют Интернет без присмотра, они могут столкнуться с изображениями или информацией, от которой их желательно оградить.



## Вторжение в частную жизнь

Заполняя различные формы в Интернете, дети могут оставить конфиденциальные сведения о себе или своей семье.

# Основные угрозы личной безопасности в Интернете



## Кража идентификационных сведений

Преступление, связанное с похищением личных сведений и получением доступа к наличным деньгам или кредиту

## Фишинг

Сообщения электронной почты, отправленные преступниками, чтобы обманом вынудить вас посетить поддельные веб-узлы и предоставить личные сведения



## Мистификация

Сообщения электронной почты, отправленные, чтобы обманом вынудить пользователя отдать деньги



## Нежелательная почта

Нежелательные сообщения электронной почты, мгновенные сообщения и другие виды коммуникации

# Что вы можете предпринять



## Ваш компьютер

- Включите интернет-брандмауэр Windows.
- Используйте Центр обновления Microsoft для автоматической загрузки новейших обновлений Windows.
- Установите и регулярно обновляйте антивирусное программное обеспечение.
- Установите и регулярно обновляйте Защитник Windows (Microsoft Windows Defender)



## Ваша семья

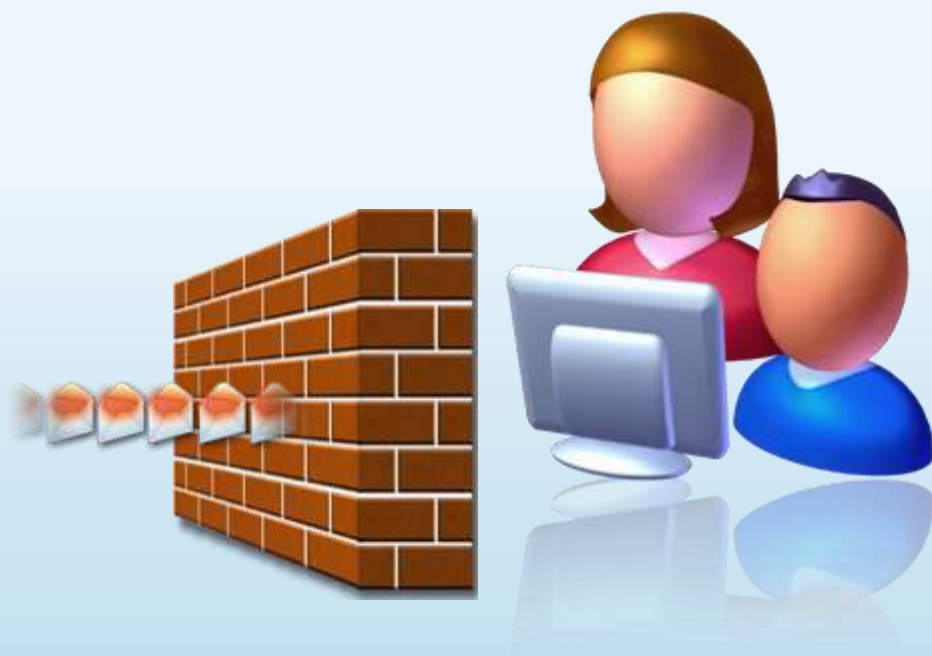
- Поговорите с детьми о том, что они делают в Интернете.
- Установите четкие правила использования Интернета.
- Держите личные сведения в секрете.
- Используйте настройки семейной безопасности в программном обеспечении Microsoft.



## Вы сами

- Выработайте линию поведения в Интернете, снижающую риски.
- Аккуратно обращайтесь с личными сведениями.
- Используйте технологии антифишинга и защиты от нежелательной почты, встроенные в Windows Vista, Windows XP SP2, Windows Live и Microsoft Outlook.

# Включите интернет-брандмауэр Windows



Интернет-брандмауэр  
создает защитный  
барьер между вашим  
компьютером и  
Интернетом

# Используйте автоматическое обновление для загрузки новейших обновлений программного обеспечения

- Устанавливайте все обновления, как только они становятся доступны
- Автоматическое обновление обеспечивает наилучшую защиту



## Установите и регулярно обновляйте антивирусное программное обеспечение



***Не позволяйте истечь  
сроку его действия***

- Антивирусное программное обеспечение помогает обнаруживать и удалять компьютерные вирусы, прежде чем они смогут навредить.
- Для эффективности антивирусного программного обеспечения регулярно обновляйте его.

## Установите и регулярно обновляйте антишпионское программное обеспечение



Используйте антишпионское программное обеспечение, такое как Защитник Windows (Microsoft Windows Defender), чтобы неизвестные программы не могли отслеживать ваши действия в сети и похищать ваши сведения.

# Другие способы защиты компьютера



**Архивируйте** регулярно Ваши данные

**Читайте** заявления о конфиденциальности на веб-узлах

**Закрывайте** всплывающие окна при помощи красной кнопки «X»

**Думайте**, прежде чем щелкнуть по ссылке

# Архивируйте свои файлы



- Сохраняйте их на компакт- или DVD-дисках, USB-накопителях или других внешних носителях
- Используйте веб-службы архивации

## Думайте, прежде чем щелкнуть по ссылке

- Будьте осторожны с вложениями и ссылками в сообщениях электронной почты
- Загружайте файлы только с веб-узлов, которым доверяете



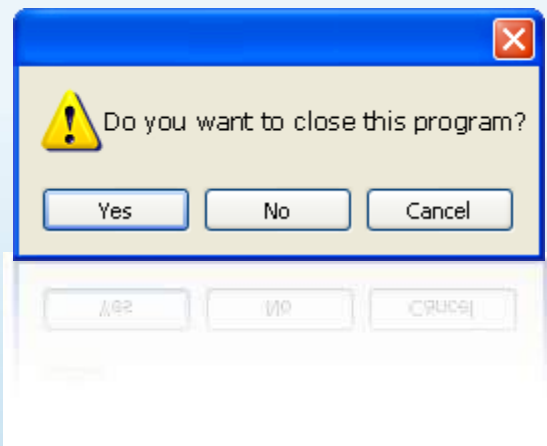
# Изучайте заявления о конфиденциальности

Старайтесь понять,  
на что Вы соглашаетесь,  
прежде чем подтвердить  
отправку или предоста-  
вить личные сведения

The image shows a document titled "Microsoft Online Privacy Notice Highlights" with a sub-header "(Get updated January 2006)". It features a "TRUSTE" logo and a photo of a woman. The document is organized into several sections with blue headers and "Additional Details" links:

- Scope:** The notice provides highlights of the full [Microsoft Online Privacy Statement](#). This notice and the full privacy statement apply to those Microsoft websites and services that display or link to this notice.
- Personal Information:**
  - When you register for certain Microsoft services, we will ask you to provide personal information.
  - The information we collect may be combined with information obtained from other Microsoft services and other companies.
  - We use cookies and other technologies to keep track of your interactions with our sites and services to offer a personalized experience.
- Your Choices:**
  - You can stop the delivery of promotional e-mail from a Microsoft site or service by following the instructions in the e-mail you receive.
  - To make proactive choices about how we communicate with you, follow the instructions listed in the [Communication Preferences](#) of the full privacy statement.
  - To view and edit your personal information, go to the [access section](#) of the full privacy statement.
- Uses of Information:**
  - We use the information we collect to provide the services you request. Our services may include the display of personalized content and advertising.
  - We use your information to inform you of other products or services offered by Microsoft and its affiliates, and to send you relevant survey invitations related to Microsoft services.
  - We do not sell, rent, or lease our customer lists to third parties. In order to help provide our services, we occasionally provide information to other companies that work on our behalf.
- Important Information:**
  - The full [Microsoft Online Privacy Statement](#) contains links to supplementary information about specific Microsoft sites or services.
  - The sign in credentials (e-mail address and password) used to sign in to most Microsoft sites and services are part of the [Microsoft Passport Network](#).
  - For more information on how to help protect your personal computer, your personal information and your family online, [visit our online safety resources](#).
- How to Contact us:** For more information about our privacy practices, go to the full [Microsoft Online Privacy Statement](#). Or write us using a [contact form](#).

# Закрывайте всплывающие окна только щелчком по красной кнопке (X)



- Всегда используйте красную кнопку (X) в углу всплывающего окна.
- Никогда не нажимайте «Да», «Принять» и даже «Отмена», поскольку это может привести к установке программы на компьютер.

# Действия, которые помогут защитить *вашу семью*

- 1** **Поговорите** с детьми о том, что они делают в Интернете
- 2** **Установите** четкие правила использования Интернета
- 3** **Держите** личные сведения в секрете
- 4** **Используйте** программные продукты для обеспечения семейной безопасности

# Обсудите с детьми опасности Интернета

- Открыто поговорите с детьми об опасностях Интернета, в том числе и о следующем.
  - Интернет-преступники
  - Недопустимый контент
  - Вторжение в частную жизнь
- Объясните им, как их собственное поведение может снизить угрозу и обеспечить безопасность в Интернете



# Уделите внимание тому, чем дети занимаются в Интернете

- Держите компьютер в центре внимания
- Узнайте, для чего Ваши дети используют Интернет
- Позвольте Вашим детям учить Вас
- Научите их доверять своим инстинктам
- Убедите их сообщать о любых неприятностях



# Держите личные сведения в секрете

- Научите детей советоваться с Вами, прежде чем предоставить личные сведения в Интернете
- Следите за деятельностью детей в Интернете
- Научите детей сообщать Вам о подозрительных действиях
- Помогите детям выбрать подходящие псевдонимы и адреса электронной почты



# Установите четкие правила использования Интернета

- Не открывайте файлы для общего доступа и не открывайте вложения
- Не щелкайте по ссылкам в сообщениях электронной почты
- Относитесь к другим так, как хотите, чтобы относились к вам
- Защищайте себя
- Уважайте собственность других людей
- Никогда не отправляйтесь на личную встречу с «другом» из Интернета



# Используйте программы для обеспечения семейной безопасности

- Эта возможность доступна в Windows Vista<sup>®</sup>, Windows Live<sup>™</sup> OneCare<sup>™</sup> Family Safety и Xbox 360<sup>®</sup>
- Помогает родителям управлять контентом, который просматривают дети, а также быть в курсе того, чем они занимаются и с кем общаются в Интернете



# Действия, которые помогут защитить *ваши личные сведения*

- 1** **Выработайте** линию поведения в Интернете, снижающую риски для вашей безопасности
- 2** **Обращайтесь** с личными сведениями аккуратно
- 3** **Используйте** технологии для снижения рисков и при необходимости поднимайте тревогу

## Выработайте линию поведения в Интернете, снижающую риски для вашей безопасности



- Удаляйте нежелательную почту, не открывая ее
- Остерегайтесь мошенничества в Интернете
- Используйте надежные пароли

Все говорят, что нельзя в качестве пароля использовать кличку собаки. Не знаю, а мне нравится, как зовут мою собаку:

**!gA4=u6\$rU%**

# Осторожно обращайтесь с личными сведениями



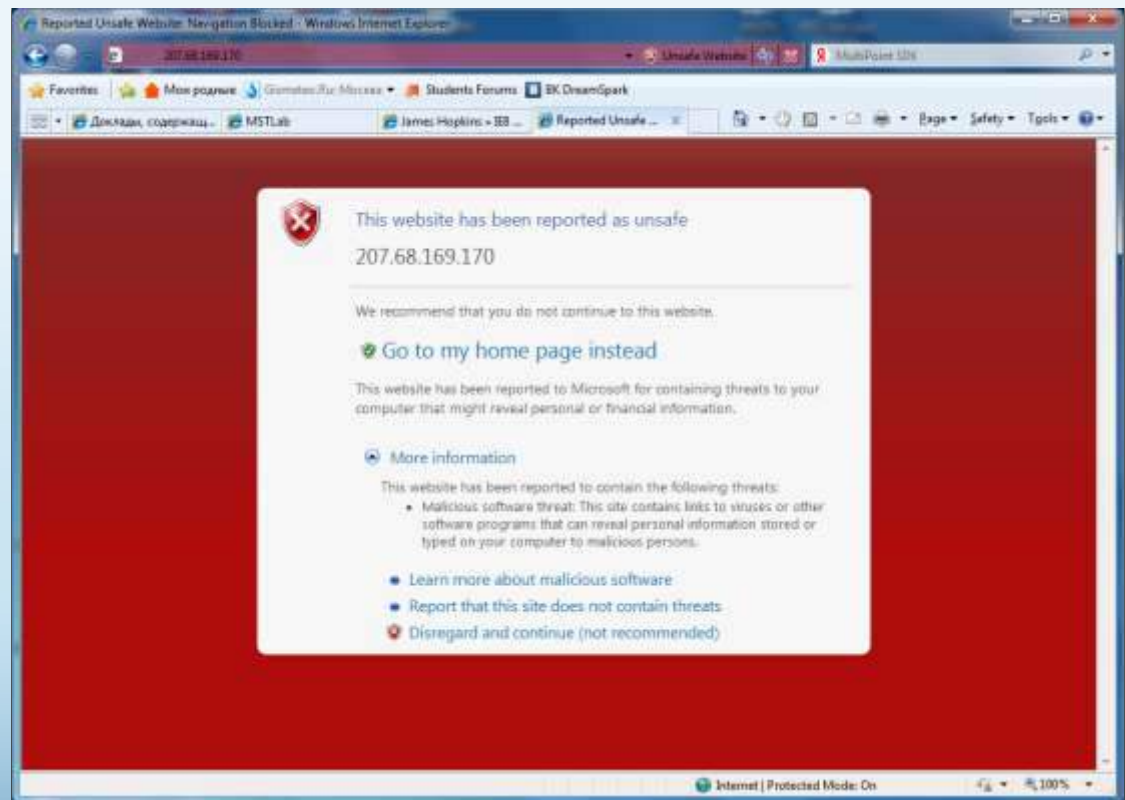
- Никогда не сообщайте личные сведения в мгновенных сообщениях или электронной почте
- Пользуйтесь только безопасными и надежными веб-узлами
- Убедитесь, что Вы попали именно туда, куда намеревались: веб-узлы могут быть поддельными
- Избегайте финансовых операций по беспроводным сетям
- В публичном месте сохраняйте конфиденциальность

# Пользуйтесь технологиями антифишинга и защиты от нежелательной почты

- Множество поставщиков электронной почты, а также такие программы, как Windows Live Hotmail® и Microsoft Outlook®, отфильтровывают большинство сообщений с нежелательной почтой
- Антифишинг в Internet Explorer® блокирует и предупреждает о подозрительных веб-узлах



# Пользуйтесь технологиями антифишинга и защиты от нежелательной почты



Ф

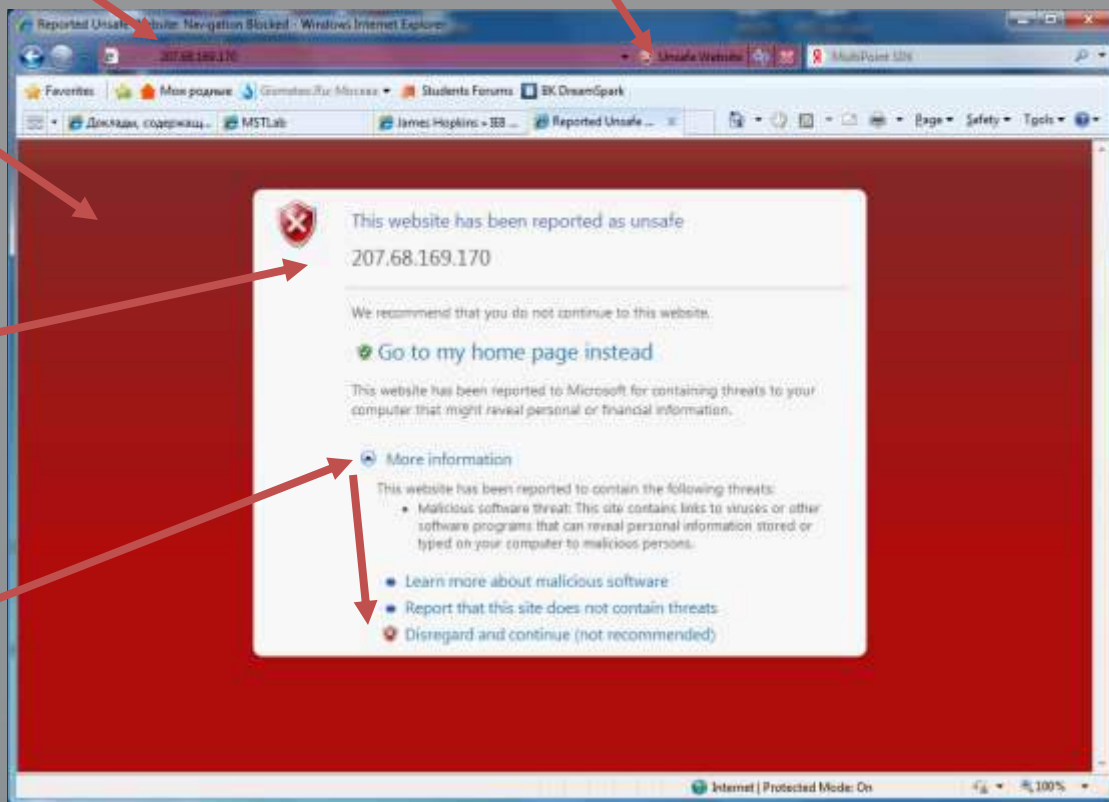
Предупреждение в адресной строке

Подсветка домена

Красный фон

Предупреждение на странице

Дополнительные действия для продолжения



# Если Ваши идентификационные сведения похищены

- Сообщите об этом
- Ведите записи
- Измените все пароли
- Заявите о мошенничестве в кредитных отчетах

Получите копию **кредитного отчета** и убедитесь, что ваш счет отмечен записями «Мошенничество» и «Заявление пострадавшего»

# Как Microsoft укрепляет защиту и безопасность?



## Сотрудничество

Сотрудничество с общественными организациями, технологическими компаниями и правительствами по всему миру для обеспечения безопасности в Интернете.



## Технологии

Разработка программных продуктов и средств повышения защиты и безопасности помогает снизить риски Интернета и сделать обдуманный выбор.



## Руководства

Предоставление полезных руководств, помогающих узнать об опасностях в Интернете и о том, как им противостоять.

# Дополнительные источники

Веб-узел "Безопасность дома" - Windows Internet Explorer  
http://www.microsoft.com/rus/protect/default.mspx

Веб-узел "Безопасность дома"

Чтобы установить Silverlight, щелкните здесь.

Россия | Изменить | Все веб-узлы корпорации Майкрософт

**Microsoft**


Безопасность дома  
Новости  
Последние обновления  
Продукты для обеспечения безопасности  
Защитите свой компьютер  
Защитите себя  
Защитите свою семью  
Подпишитесь на наш информационный бюллетень  
Поддержка  
Учебные видеоматериалы  
Веб-узлы для других стран

**Безопасность дома**

Защитите свой компьютер →    Защитите себя →    Защитите свою семью →

**Кража личных данных**  
[Что такое фишинг-атаки?](#)  
Никогда не отвечайте на сообщения электронной почты от банка или компании, выпустившей кредитную карту, если в них запрашиваются личные сведения.  
[Проверьте надежность ссылок паролей](#)

**Программы-шпионы и вирусы**  
[Не допустите превращения компьютера в зомби](#)  
Если злоумышленники получают контроль над множеством компьютеров одновременно, образуются сети зомби, которые могут причинить вред другим компьютерам в Интернете.

**Полезные сведения**  
  
[Используйте родительский контроль в стиле Windows Vista на компьютере с системой Windows XP](#)  
Семейная безопасность OneCare — это бесплатная веб-служба для пользователей Microsoft Windows XP.

**Файлы для загрузки, продукты и услуги**

**Защитите свой компьютер** от программ-шпионов и прочих нежелательных программ

- [Средство проверки безопасности Windows Live OneCare](#)
- [Центр обновления Microsoft](#)
- [Internet Explorer 7](#)
- [Система Windows Vista](#)

**Защитите себя** от нежелательной почты, кражи личных сведений и прочего мошенничества

- [Антифишинг Microsoft](#)
- [Microsoft Office 2007](#)

**Защитите свою семью** от нежелательных содержимого и контактов

- [Семейные параметры Xbox](#)

http://www.microsoft.com/rus/protect/default.mspx    Internet | Protected Mode: On    100%



# Программа повышения квалификации

## «Здоровье и безопасность детей в мире компьютерных технологий и Интернет»



- Разработка программы сотрудниками АПК и ППРО при поддержке Microsoft в рамках инициативы «Партнерство в образовании»

**Идея создания**

**Актуальность**

- Формирование навыков поведения в информационном обществе с целью обеспечения информационной безопасности

**РУЦ - эксперты**

**Анализ**

- Декабрь 2008 г. – программа представлена на семинаре для РУЦ Microsoft «Академия учителей» в г.Москве

- Потребности школы и семьи



Программа  
направлена  
на:

Формирование  
навыков поведения  
в информационном  
обществе

с целью  
обеспечения  
информационной  
безопасности

Категории  
специалистов:

Дир. и зам.дир.по  
информатизации,  
учителям-  
предметникам и

педагогам доп.обр.  
детей, препод-м и  
тьюторам учр-й ПК

Построение  
программы:

Блочно -

модульное

# Структура программы

Модуль 1

- Психическое и физическое здоровье детей при работе за компьютером.

Модуль 2

- Социальный, эмоциональный и личностные аспекты занятий детей на компьютере.

Модуль 3

- Информационная этика и правовые аспекты защиты информации.

Модуль 4

- Безопасность детей в Интернете.

Модуль 5

- Технологии и средства защиты информации от разрушения и несанкционированного доступа.

Модуль 6

- Компьютерные вирусы и средства защиты.

# Результаты освоения программы

Осознание обучающимися значимости проблемы и ее решения для будущего общества, образования, педагогических кадров, школьников и эмоционально-положительное отношение к предлагаемому курсу, к программе как к потенциально эффективным инструментам решения обозначенной проблемы;

Знания в сфере проектирования безопасных информационно-методических сред образовательных учреждений, в области психолого-педагогического и здоровьесберегающего сопровождения образовательного процесса, персонала и школьников, использующих персональные компьютеры и Интернет в профессиональной, учебной и внеучебной деятельности;

Знания в области разработки программ информатизации школы, с учетом соблюдения принципов безопасности информации и жизнедеятельности, здоровьесбережения участников образовательного процесса;

Опыт проектирования названных объектов, условий, программ.

**Проекты программ просветительской работы с родителями и общественностью.**

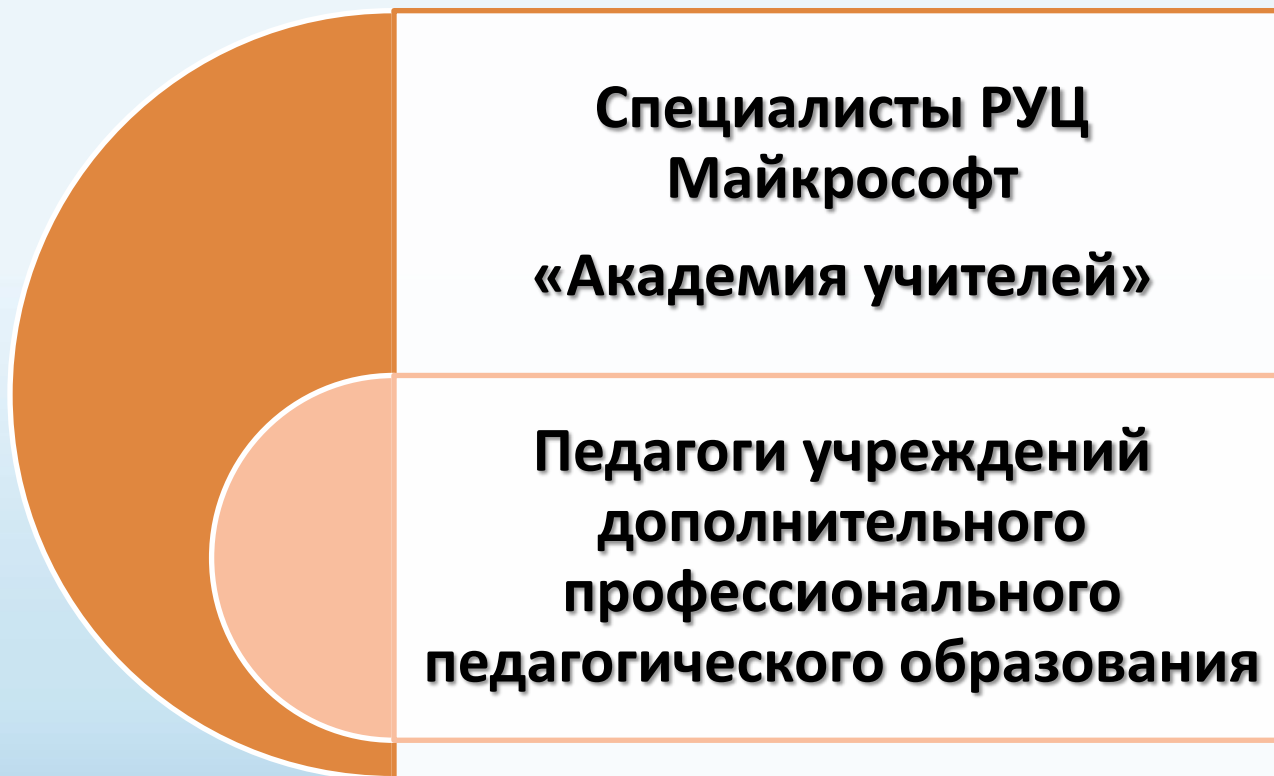


**Проекты учебных и методических занятий, в рамках которых рассматриваются вопросы здоровья и безопасности школьников и педагогического персонала в мире Интернет и компьютерных технологий.**

**Проекты разделов программ информатизации образовательных учреждений, информационно-методических сред, локальных вычислительных сетей школ, локальных нормативных актов.**

**Продукты,  
фиксирующие  
освоенность  
программы**

# Реализаторы программы



Ваш ребенок правильно сидит за компьютером?

Компьютерный класс оборудован согласно необходимым требованиям?



Знаете ли Вы как нужно эффективно отдыхать при работе на компьютере и после?

Что такое «компьютерный зрительный синдром»?

# Модуль 1 «Психическое и физическое здоровье детей при работе за компьютером»

**Постановка проблемы:**

Психологический и физический аспекты организации работы детей за компьютером

**Цель:**

Сформировать у учителя (управленца, родителя) умения использовать приемы по организации безопасной и здоровьесберегающей работы ребенка за компьютером

**Задачи:**

Изучение основ здоровьесберегающих технологий, применяемых при организации работы ребенка на компьютере.

Проверка и обеспечение соответствия помещений, компьютерного оборудования и режима работы учащихся гигиеническим требованиям к организации занятий.

Разработка и использование профилактической гимнастики и комплексов упражнений физкультурных минуток и пауз для предупреждения нарушений здоровья детей при работе за компьютером.

## Темы модуля «Психическое и физическое здоровье детей при работе за компьютером»:

Компьютеры и физическое здоровье детей.

Гигиенические требования к организации занятий с использованием новых информационно-компьютерных технологий.

Профилактика нарушений осанки и зрения при работе за компьютером.

## Что мы предлагаем при изучении модуля?

1

- Основы гигиенических требований к состоянию воздушной среды и к оформлению и размещению различных средств ТСО.

2

- Рекомендации по правильной организации рабочего места ребенка.

3

- Рекомендации по профилактике нарушений осанки при работе за компьютером различных категорий учащихся.

4

- Инструкции по правильной посадке за компьютером.

5

- Комплексы упражнений для профилактики нарушений зрения, снижения утомления глаз.

6

- Комплексы физкультминуток на занятиях с детьми школьного и дошкольного возраста.
- «Золотые» правила при работе за компьютером.



# Модуль 1 «Психическое и физическое здоровье детей при работе за компьютером»

**Формы работы с модулем:**

**Теоретические и практические занятия, круглые столы и дискуссии**



**Итог работы:**

**Тест**



## Ребенок имеет склонность к депрессии?

**Симптомы «отстраненного»  
поведения, следствие зависимости  
от компьютерных игр?**

**«Синдром компьютерного стресса»  
- что это такое?**

**Какие признаки  
характерны для игромана?**

## Модуль 2 «Социальный, эмоциональный и личностные аспекты занятий детей на компьютере»

**Постановка проблемы:**

Влияние компьютера на развитие интеллекта и психику ребенка

**Цель:**

Научить учителя (управленца, родителя) правильному использованию компьютерных игр и снижению стрессовых ситуаций при работе детей с компьютером

**Задачи:**

Изучение влияния виртуального взаимодействия и видеоигр на развитие интеллекта и эмоциональный фон ребенка.

Расширение представлений о формировании внимания и мотивации ребенка и влиянии на них компьютера.

Формирование представлений об изменении психического здоровья детей при интенсивном использовании компьютера и Интернета.

Информирование о влиянии компьютерных игр на поведение детей.

Изучение стрессовых факторов при работе с компьютером.

## Темы модуля «Социальный, эмоциональный и личностные аспекты занятий детей на компьютере»:

Развитие интеллекта и стили общения в цифровом мире.

Влияние компьютера на внимание, мотивацию.

Негативное воздействие компьютера на психическое здоровье детей.

## Что мы предлагаем при изучении модуля?

1

- Примеры влияния компьютерных видеоигр на интеллект и психику ребенка (например: «уход от реальности»).

2

- Отличительные признаки «игромана».
- Пример агрессивного поведения, как следствия жестоких игр.

3

- Советы по выбору и использованию видеоигр.
- Практические рекомендации по улучшению внимания и мотивации у детей.

4

- Способы профилактики стресса при работе с компьютером.

5

- Игры и упражнения на снижение агрессии и ослабление негативных эмоций, возникших при работе с компьютером.

6

- Тест «Шкала оценки личностной тревожности» (по Ч.Спилбергеру и Ю.Л.Ханину).
- Практические советы по снятию стресса.

## Модуль 2 «Социальный, эмоциональный и личностные аспекты занятий детей на компьютере»

### Формы работы с модулем:

Теоретические и практические занятия, круглые столы и дискуссии

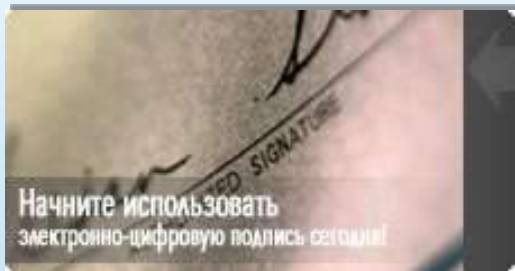


### Итог работы:

Ролевая игра или проект внеклассного мероприятия

# Что такое информационная безопасность?

Электронно-цифровая подпись –  
зачем она нужна?



Каковы преступления в  
сфере компьютерной  
информации?

Какие средства защиты  
информации существуют?

## Модуль 3 «Информационная этика и правовые аспекты защиты информации»

### Постановка проблемы:

Недостаточная осведомленность о проблемах информационной безопасности в образовательных учреждениях

### Цель:

Сформировать у учителя (управленца, родителя) представление о правовых и технологических аспектах информационной безопасности

### Задачи:

**Изучение основ информационной безопасности.**  
**Изучение основных законов РФ в области компьютерного права.**

## Темы модуля «Информационная этика и правовые аспекты защиты информации»

**Информационная этика и право.**

**Основные законы Росси в области компьютерного права.**

## Что мы предлагаем при изучении модуля?

1

- Терминологический аппарат по информационной безопасности.

2

- Угрозы и уровни информационной безопасности, направления защиты компьютерной безопасности.

3

- Защита аутентификации и целостности электронных документов с помощью цифровой подписи.

4

- Перечень ряда Федеральных законов в области компьютерного права.

5

- Ситуационные задачи по правовым вопросам.

## Модуль 3 «Информационная этика и правовые аспекты защиты информации»

### Формы работы с модулем:

Теоретические и практические занятия, круглые столы и дискуссии



### Итог работы:

Контрольные вопросы и тест

Какие опасности таят в себе социальные сети?

Что такое Интернет-зависимость?



В контакте

МОЙ МИР@mail.ru  
национальная социальная сеть

Как защитить ребенка от негативного контента в сети Интернет?

Как осуществить контроль за ребенком при его работе за компьютером?

## Модуль 4 «Безопасность детей в Интернете»

### Постановка проблемы:

Увеличивающееся негативное влияние на детей при использовании ими Интернета

### Цель:

Помочь учителю (управленцу, родителю) в организации обеспечения безопасности детей в Интернете

### Задачи:

- Информирование о существующих опасностях с которыми дети могут столкнуться в сети Интернет.
- Разработка норм и правил поведения детей в сети Интернет.
- Формирование понятий о синдроме Интернет-зависимости.
- Изучение проблем безопасности при навигации по Интернет-ресурсам и при работе с электронной почтой.
- Изучение основ блокировки доступа к опасному содержимому.

## Темы модуля «Безопасность детей в Интернете»

Опасности, с которыми дети могут столкнуться в сети.

Безопасное общение детей в Интернете.

Профилактика Интернет-зависимости у учащихся.

Технологии безопасной работы в сети.

## Что мы предлагаем при изучении модуля?

1

- Перечень рисков, подстерегающих ребенка в сети Интернет.
- Рекомендации по грамотному использованию электронной почты.

2

- Технологии безопасного общения в средах мгновенного обмена сообщениями.
- Инструкции по безопасному общению в чатах.

3

- Советы по профилактике и преодолению Интернет-зависимости.
- Тест на определение Интернет-зависимости (Кимберли Янг).

4

- Общие правила по безопасности детей в Интернете.

5

- Советы по безопасности при работе на общедоступном компьютере.

6

- Практические работы: по установке и использованию программ-фильтров; по настройке компьютера с помощью средства проверки безопасности Windows Live OneCare; по отключению функции сохранения паролей и удалению временных файлов Интернета; по удалению прочих файлов, сохраненных корпоративными порталами, например Sharepoint Portal Server; по повышению уровня безопасности в Интернете с помощью Internet Explorer.



## Модуль 4 «Безопасность детей в Интернете»

### Формы работы с модулем:

Теоретические и практические занятия, круглые столы и дискуссии



### Итог работы:

Проект проведения внеклассного мероприятия

Зачем нужны пароли при работе на компьютере?

Электронная почта - есть опасность?

Ваша школьная сеть защищена?



# Модуль 5 «Технологии и средства защиты информации от разрушения и несанкционированного доступа»

**Постановка проблемы:**

Активное распространение мошенничества в Интернете

**Цель:**

Ознакомить учителя (управленца, родителя) с комплексом мер по обеспечению защиты компьютеров (локальных и сетевых) при работе в сети Интернет и научить проектированию комплекса мер в конкретном ОУ

**Задачи:**

Изучение основ защиты информации от несанкционированного доступа, утечки.

Создание условий для защиты информации на ПК.

Обеспечение безопасности информации в сетях и защиты поддерживающей инфраструктуры.

Обеспечение защиты сетевых сервисов.

Обеспечение безопасной работы на форумах.

## Темы модуля «Технологии и средства защиты информации от разрушения и несанкционированного доступа»

Цели совершения преступления. Меры и уровни защиты информации.

Установка паролей на ПК и папка. Меры безопасности при работе с электронной почтой.

Безопасность работы в локальной сети.

Безопасность работы на форумах.

## Что мы предлагаем при изучении модуля?

1

- Основные понятия в области защиты информации от разрушения и несанкционированного доступа по ГОСТ Р 50922-96.

2

- Рекомендации по установке паролей на папки, ПК.

3

- Общие рекомендации по защите компьютеров.

4

- Практические советы по работе на форумах.



## Модуль 5 «Технологии и средства защиты информации от разрушения и несанкционированного доступа»

**Формы работы с модулем:**

Теоретические и практические занятия, круглые столы и дискуссии



**Итог работы:**

Мероприятие круглого стола

Что такое вирус ?



Почему так важно знать как  
переносится компьютерный вирус?

А как Вы застрахованы от  
вирусов?

Какие антивирусные  
программы существуют?

## Модуль 6 «Компьютерные вирусы и средства защиты»

**Постановка проблемы:**

Повсеместное распространение огромного количества вирусов

**Цель:**

Сформировать у учителя (управленца, родителя) опыт создания защиты от распространения вирусных программ и вирусов на компьютерах в образовательных учреждениях и домашних условиях

**Задачи:**

Расширение представлений о вирусах и методах борьбы с ними.

Использование работы антивирусных программ.

## Темы модуля 6 «Компьютерные вирусы и средства защиты»

Обзор и способы классификации компьютерных вирусов.

Программная защита информации.

## Что мы предлагаем при изучении модуля?

1

- Классификация вирусов.

2

- Обзор самых известных вирусов и упражнения по их распознаванию на компьютере.

3

- Меры защиты от проникновения и распространения вирусов.

4

- Обзор антивирусных программ.

5

- Тесты на определение вирусов.

6

- Практически работы по: определению оптимизации времени работы антивирусной программы; визуальному определению вероятности появления вируса; примеру работы программы рассылки спама; проверке файла на заражение вирусом; знакомству с антивирусными программами.



## Модуль 6 «Компьютерные вирусы и средства защиты»

**Формы работы с модулем:**

**Теоретические и практические занятия, круглые столы и дискуссии**



**Итог работы:**

**Проект внеклассного мероприятия**



© Корпорация Microsoft, 2009 Все права защищены.

Microsoft, Hotmail, OneCare, Outlook, Windows, Windows Vista, Xbox, Xbox 360, Xbox LIVE и другие названия продуктов являются товарными знаками и охраняемыми товарными знаками корпорации Microsoft в США и других странах.

Сведения, содержащиеся в настоящей презентации, представлены исключительно для ознакомительных целей; они отражают текущую позицию корпорации Microsoft на момент ее публикации.

Поскольку корпорация Microsoft должна реагировать на изменение рыночных условий, данный документ не может рассматриваться как обязательство с ее стороны и корпорация Microsoft не гарантирует точности сведений, представленных после даты публикации.

**КОРПОРАЦИЯ MICROSOFT НЕ ПРЕДОСТАВЛЯЕТ НИКАКИХ ГАРАНТИЙ, ЯВНЫХ, ПОДРАЗУМЕВАЕМЫХ ИЛИ ПРЕДУСМОТРЕННЫХ ЗАКОНОМ, ОТНОСИТЕЛЬНО СВЕДЕНИЙ, СОДЕРЖАЩИХСЯ В ДАННОЙ ПРЕЗЕНТАЦИИ.**