

Тема мероприятия:

Единый урок по безопасности в сети
«Интернет»
(Единый урок)

*“Безопасность есть предотвращение зла”
Платон, определения, стих 415*

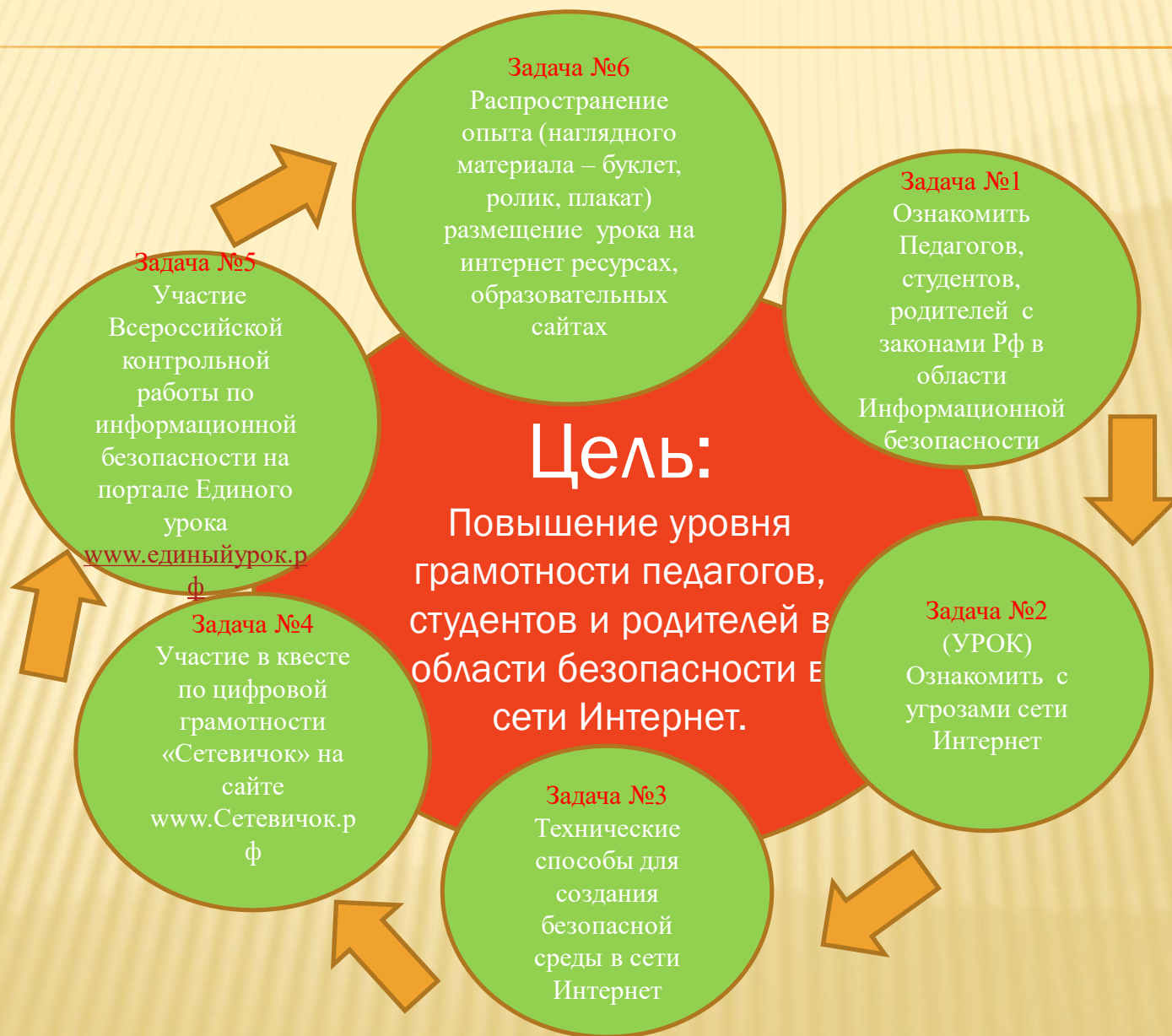
Традиционной Единый урок проходит в образовательных организациях в конце октября с 28 октября по 8 ноября, а дистанционные мероприятия проходят с 1 октября по 10 декабря 2019 года.

Обращаем внимание на то, что необходимо **привлечь** к участию всех обучающихся и педагогических работников профессиональных образовательных организаций не менее, чем в одном мероприятии Единого урока, и обеспечить максимальный охват родительской общности.

В соответствии с письмом члена Совета Федерации Федерального собрания РФ Л.Н.Боковой от 24.10.19 г. №1.6-01/14306 необходимо **до 6 декабря 2019** г. представить отчет по форме (приложение 2).

Цель мероприятия: Повышение уровня грамотности педагогов, студентов и родителей в области безопасности в сети Интернет.

Задачи поставленной цели:



Проблемы информационной безопасности

Основные понятия

Безопасность – отсутствие угроз, либо состояние защищенности от угроз.

Информация – сведения или сообщения.

Угроза информационной безопасности — совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства в информационной сфере.



Информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации.

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

(Федеральный закон от 29.12.2010 № 436-ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию").



Задача №1

Ознакомить Педагогов, студентов, родителей с законами Рф в области Информационной безопасности

К числу наиболее значимых нормативных правовых актов в области обеспечения информационной безопасности относятся следующие законы и подзаконные акты:

Конституция Российской Федерации <http://www.constitution.ru/> содержит нормы, которые определяют правовые основы информационной безопасности: основные положения правового статуса субъектов информационных отношений, принципы информационной безопасности (законности, уважения прав, баланс интересов личности, общества и государства), конституционный статус государственных органов, обеспечивающих информационную безопасность и др.

Конституция Российской Федерации устанавливает запрет на доступ к информации о частной жизни и передачу сообщений по линиям телефонной связи (ст.23).

Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» <http://pravo.gov.ru/proxy/ips/?docbody=&nd=102144301> закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

Закон определяет ключевые термины в области безопасности, которые применимы и для сферы информационной безопасности, принципы и систему безопасности, правовой статус и состав Совета Безопасности Российской Федерации.

Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» <http://kremlin.ru/acts/bank/32492> регулирует отношения, связанные с защитой детей от информации, причиняющей вред их здоровью и (или) развитию, в том числе от такой информации, содержащейся в информационной продукции.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» <http://kremlin.ru/acts/bank/24157> фиксирует базовые нормы для всей системы информационного законодательства, в т.ч. правового обеспечения информационной безопасности.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» <http://kremlin.ru/acts/bank/24154> регулирует деятельность по обработке (использованию) персональных данных.

Доктрина информационной безопасности Российской Федерации <http://kremlin.ru/acts/bank/41460> представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

Задача №2 (УРОК)

Ознакомить с угрозами сети Интернет

Угрозы, исходящие из Интернета

- * Мошенники
- * Вирусы
- * Недетский контент
- * Пропаганда наркотиков,
экстремизма, суицида



Интернет -

хищники используют социальные сети, чаты, мессенджеры, интернет - форумы и другие социальные средства коммуникации для общения с детьми и подростками с целью склонить их к незаконным действиям различного характера

Интернет – мошенники


Хищение конфиденциальных данных может привести к тому, что хакер незаконно получает доступ и каким -либо образом использует личную **информацию** пользователя, с целью получить материальную прибыль



КОМПЬЮТЕРНЫЕ ВИРУСЫ

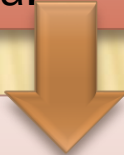


Троянская программа - вредоносная программа, проникающая на компьютер под видом безвредной.



Может:
Мешать работе пользователя
Шпионить за пользователем
Использовать ресурсы компьютера для какой-либо незаконной деятельности и т.д.

Spyware (шпионское программное обеспечение) - программа, которая скрытным образом устанавливается на компьютер с целью полного или частичного контроля за работой компьютера.



Может:
Собирать информацию о привычках пользования Интернетом и наиболее часто посещаемых сайтах.
Запоминать нажатия клавиш на клавиатуре, записывать скриншоты экрана и в дальнейшем отправлять информацию создателю spyware;
Несанкционированно и удалённо управлять компьютером;
Устанавливать на компьютер дополнительные программы;
Изменять параметры операционной системы;
Перенаправлять тебя в браузерах на сайты, которые заражены другими вирусами.

Руткит (Rootkit) - программа или набор программ, использующих технологии сокрытия системных объектов (файлов, процессов, драйверов, сервисов, ключей реестра, открытых портов, соединений и пр) посредством обхода механизмов защиты системы.

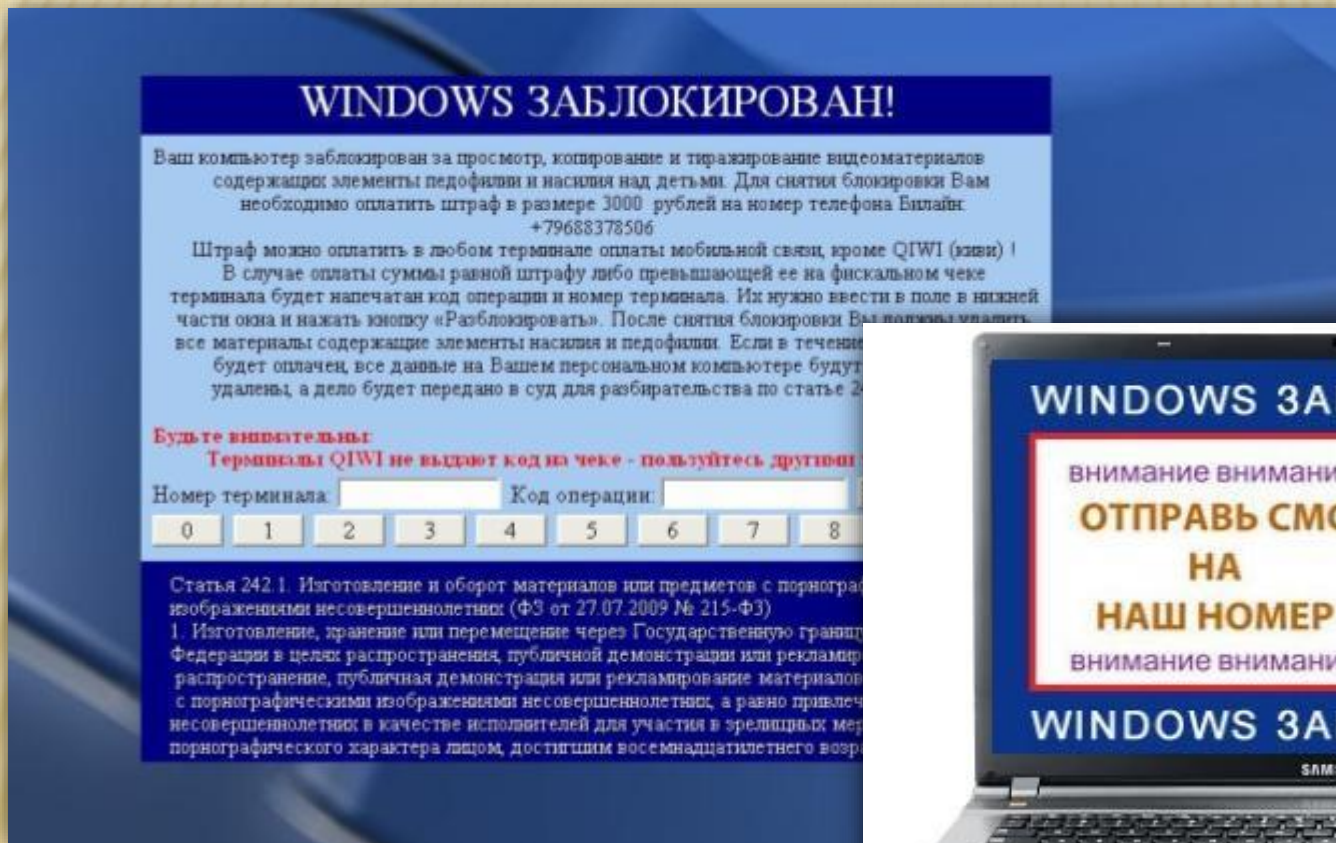


Признаки заражения этим вирусом:
Вывод на экран странных сообщений или изображений;
Подача странных звуковых сигналов;
Неожиданное открытие и закрытие лотка CD и DVD -ROM устройства;
Произвольный, без твоего участия, запуск на компьютере каких-либо программ.

Сетевой червь - разновидность самовоспроизводящихся компьютерных программ, распространяющихся в локальных и глобальных компьютерных сетях. Червь является самостоятельной программой.

Блокирование операционной системы.

Еще один простой вариант получить доступ к ПК пользователя и его деньгам – заблокировать операционную систему и потребовать некоторые сведения и некоторую сумму за ее разблокировку.



Термины

Кибербулинг (cyberbullying) – подростковый виртуальный террор

Бумицид – доведение ребенка до самоубийства путем психологического насилия

Флейм (от английского «flame») или виртуальная перепалка. Обмен эмоциональными репликами в открытом доступе.

- Интернет-ХАМЫ (Тролли) провоцируют на необдуманные поступки и необоснованную агрессию!
- Киберпреступники зачастую обманом похищают чужое имущество!
- Хакеры используют анонимность для распространения вредоносного программного обеспечения, завладения учётными данными, платёжными реквизитами, персональной информацией!

Кардинг

(от **англ.** *carding*) — вид **мошенничества**, при котором производится операция с использованием **платежной карты** или её реквизитов, не инициированная или не подтверждённая её держателем.

фíшинг (**англ.** *phishing* от *fishing* «рыбная ловля, выуживание»^[1]) — вид **интернет-мошенничества**, целью которого является получение **доступа к конфиденциальным данным пользователей** — **логинам** и паролям.

СОВЕТЫ ПО БЕЗОПАСНОЙ РАБОТЕ В СЕТИ ИНТЕРНЕТ



Задача №3

Технические способы для создания безопасной среды в сети Интернет

Вы защитите компьютер от большинства интернет-угроз, если будете соблюдать простые правила безопасности.

Обновляйте операционную систему

Скачайте последнюю версию браузера

Установите антивирус

Включите фаервол

Пользуйтесь учетной записью с ограниченными правами

Придумывайте сложные пароли

Выбирайте легальное ПО

Делайте резервные копии ценных данных

Брандмауэр - обладает более широким спектром функций. А именно : анализирует не только сетевую активность приложения, но и активность приложений

Термин брандмауэр (нем. *Brandmauer*, от *Brand* — пожар и *Mauer* — стена) — глухая противопожарная стена здания или его английский

эквивалент **файрвол** (англ. *firewall*; *fire* - огонь, *wall* – стена) используется также в значении «межсетевой экран».

Брандмауэр или firewall – это программный комплекс, предназначенный для защиты компьютера от сетевых атак.

Следует отметить, что благодаря брандмауэрам увеличивается безопасность работы в сети, а также отражается большинство атак на компьютер путем фильтрации некоторых информационных пакетов. Поэтому настоятельно рекомендую Вам не отключать брандмауэр.

Включите файрвол

Файрвол проверяет данные, которыми обмениваются компьютер и интернет, и блокирует подозрительные соединения. Он дополнительно защищает операционную систему от вирусов.

Включите файрвол:

Фаервол, от англ. FireWall - стена огня. То есть метод защиты компьютера от подозрительной сетевой активности исходя только из правил : что пускать, а что не пускать.

Вы должны это знать:

❑ Когда ты регистрируешься на сайтах, старайся не указывать личную информацию
(номер мобильного телефона, адрес электронной почты, свое фото!)

❑ Используй *веб-камеру* только при общении с друзьями. Проследи, чтобы посторонние люди не имели возможности видеть ваш разговор, так как он может быть записан!



❑ Нежелательные письма от незнакомых людей называются «Спам». Если ты получил такое письмо, не отвечай на него. Если ты ответишь на подобное письмо, отправитель будет знать, что ты пользуешься своим электронным почтовым ящиком, и будет продолжать посылать тебе спам!



Фильтры электронной почты

Используйте фильтры электронной почты для блокирования спама и нежелательных сообщений



Что делать и чего не делать при работе в сети:

Не запускать файлы и не переходить по ссылкам, которые были получены из ненадежных источников.

Не скачивать файлы с непроверенных ресурсов в Интернет или локальной сети.

Чтобы минимизировать возможность заражения через браузер при просмотре веб-страниц, следует избегать переходов по подозрительным ссылкам и баннерам, особенно, если они рекламируют что-то противозаконное.

Если во время интернет серфинга вы попали на сайт, который изобилует рекламой, открывает множество окон без вашего ведома, или предлагает вам что-то скачать без вашей инициативы, то стоит его немедленно покинуть, т.к. это типичный рассадник вирусов.

*Используй функционал браузера:
«избранное», «закладки»!*

*Хорошо подумай, какую информацию
можно публиковать
в Интернете! Не публикуй
информацию
о своём местонахождении и (или)
материальных ценностях*

*При работе в Интернете будь вежлив
с другими пользователями Сети.*

Проверяй адрес сайта!

**Всегда помни
E-MAIL, ЛОГИН, ПАРОЛИ**

**И НЕ РЕГЕСТРИРУЙСЯ ВЕЗДЕ
БЕЗ НАДОБНОСТИ**

- Используйте надёжный пароль. Его нужно правильно создавать, аккуратно хранить и регулярно менять.



- Выясните, какие программные способы предлагает владелец сети для защиты данных.
- Не забывайте очищать историю и удалять сохраненный пароль после работы со своим аккаунтом с чужого компьютера.

**НЕ ПОСЕЩАЙТЕ
ПОДОЗРИТЕЛЬНЫЕ
САЙТЫ**

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ КОНТРОЛЯ ДЕТЕЙ В СЕТИ ИНТЕРНЕТ

Стандартные возможности **родительского контроля в ОС**

Контроль средствами **антивирусных программ**

Специальные программы для родительского контроля:

КиберМама - проследит за временем работы, предупредит ребенка о том, что скоро ему нужно будет отдохнуть и приостановит работу компьютера, когда заданное вами время истечет.

Time Boss - предназначена для ограничения времени, которое наши дети проводят за компьютером.

Интернет Цензор - программа предназначена для эффективной блокировки сайтов, которые могут представлять опасность для ребенка, когда он использует Интернет.

NetPolice - контентный фильтр, который позволит осуществлять комплексную защиту детей от Интернет-угроз

Детский браузер Гогуль это не отдельная программа, а дополнение (плагин) к браузеру **Mozilla Firefox**

Детский браузер Гогуль

Федеральная программа безопасного детского интернета

Официальный сайт
<http://www.gogul.tv>

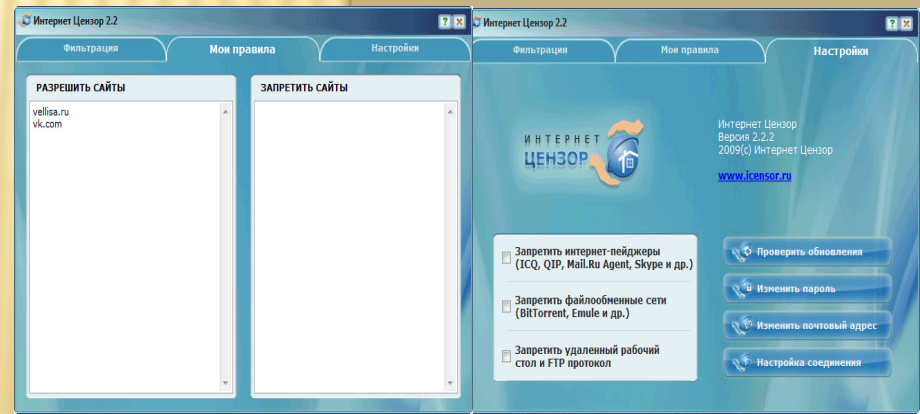


Интернет Цензор

Официальный сайт
<https://vellisa.ru/internet-tsenzor>

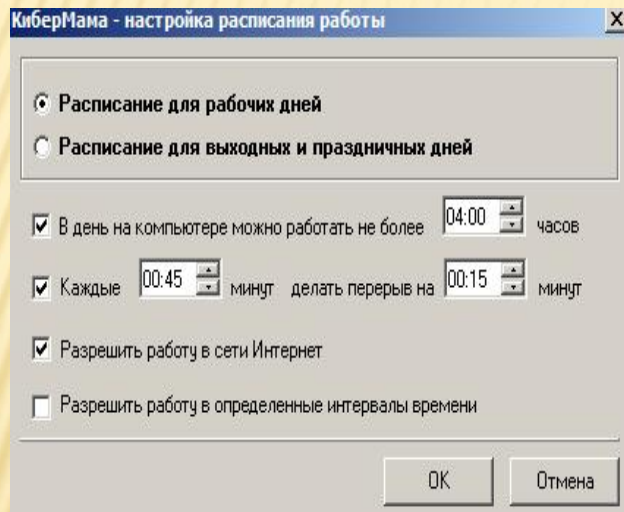
Интернет Цензор —
бесплатная программа для
осуществления
родительского контроля.
Программа предназначена
для эффективной
блокировки сайтов, которые
могут представлять
опасность для ребенка, когда
он использует Интернет.

- Безопасность ребёнка в Интернете обеспечивается за счёт наличия собственного каталога проверенных детских сайтов.
- Гогуль ведёт статистику посещённых сайтов для контроля родителями, а также может ограничивать время пребывания ребёнка в интернете.
- Детский браузер Гогуль позволяет составить расписание доступа, то есть программирование ограничения продолжительности использования ребёнком Интернета по дням недели.



КИБЕРМАМА

HTTP://WWW.CYBERMAMA.RU/

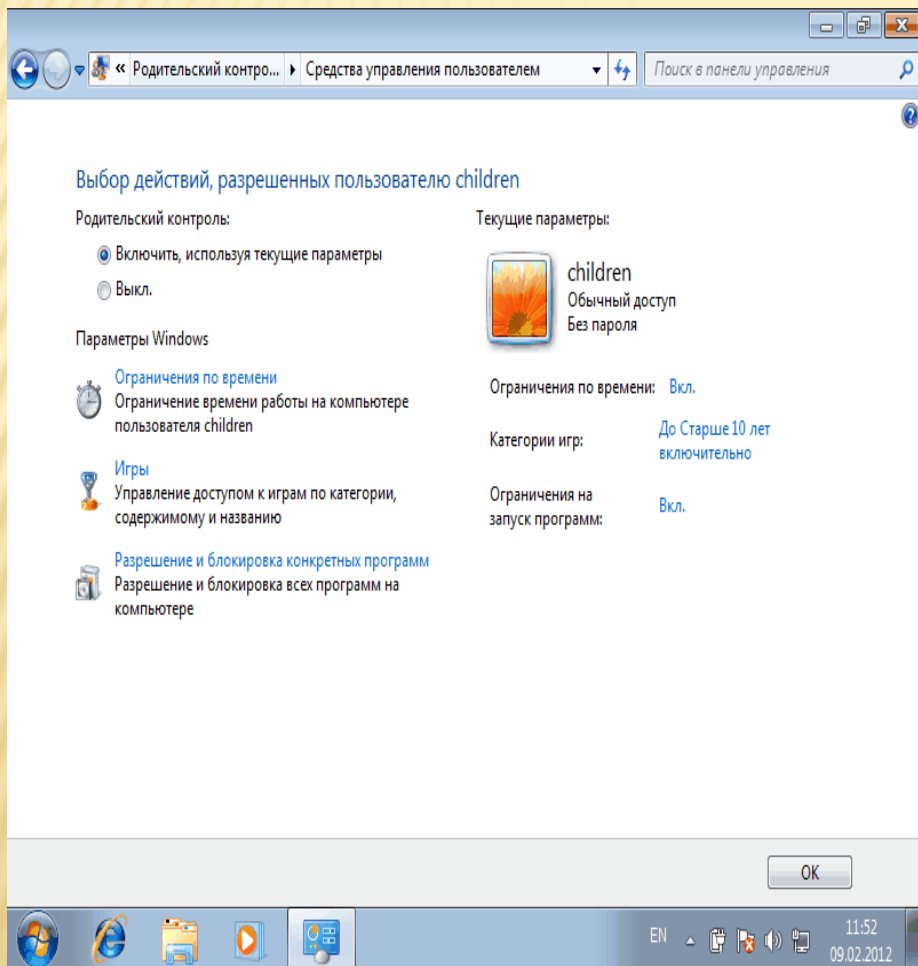


КиберМама проследит за временем работы, предупредит ребенка о том, что скоро ему нужно будет отдохнуть и приостановит работу компьютера, когда заданное вами время истечет.

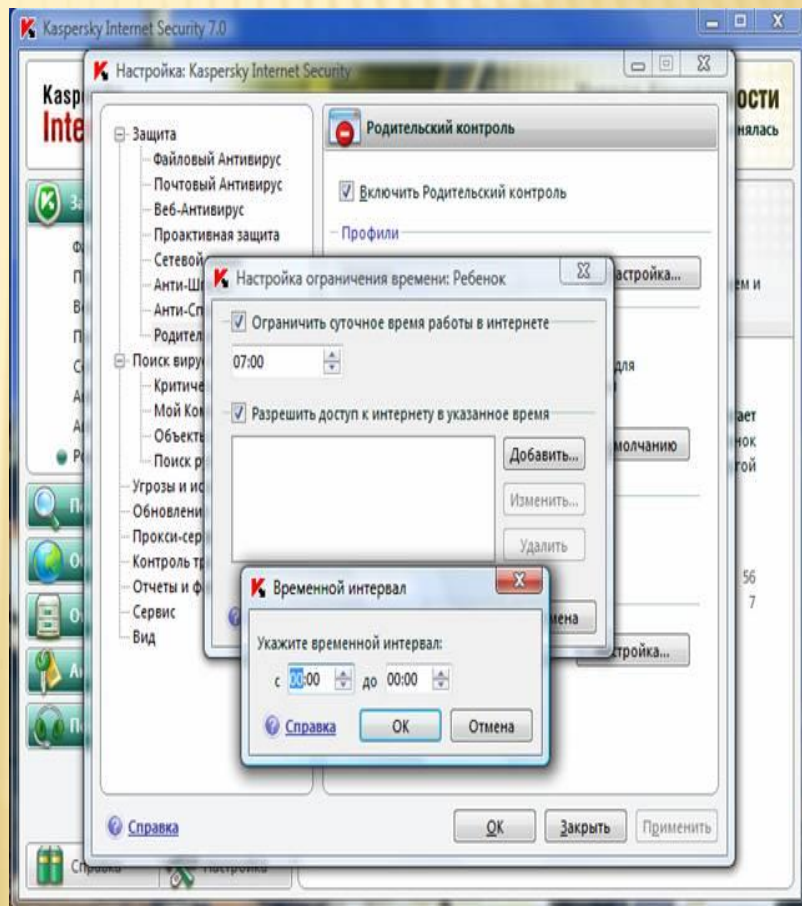
КиберМама поддерживает следующие возможности:

- Ограничение по суммарному времени работы
- Поддержка перерывов в работе
- Поддержка разрешенных интервалов работы
- Возможность запрета интернета
- Возможность запрета игр/программ

Родительский контроль в ОС



Родительский контроль в Kaspersky Internet Security



ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Антивирусная программа (антивирус) — программа для обнаружения компьютерных вирусов и лечения инфицированных файлов, а также для профилактики — предотвращения заражения файлов или операционной системы вредоносным кодом

Proxy-servers (proxy — доверенность, доверенное лицо)

Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью — маршрутизация как таковая отсутствует, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом обращения из глобальной сети в локальную становятся невозможными в принципе

Этот метод не дает достаточной защиты против атак на более высоких уровнях — например, на уровне приложения (вирусы, код Java и JavaScript)

Межсетевые экраны (брандмауэры или фаерволы — от нем. *Brandmauer*, англ. *firewall* — «противопожарная стена»)

- **Антивирус** — программа, которая знает вирусы «в лицо»
- **Межсетевой экран** — защищает от внешних непрошенных подключений

САМЫЕ ЭФФЕКТИВНЫЕ АНТИВИРУСНЫЕ ПРОГРАММЫ

- ✗ Антивирус лаборатории Касперского
- ✗ Доктор Web
- ✗ NOD 32
- ✗ AVAST



Примечание. Если устройство подключено к интернету, антивирусы будут обновляться автоматически.

Задача №4

Участие в квесте по цифровой грамотности «Сетевичок» на сайте www.Сетевичок.рф

Интернет

Проверка знаний студентов по основам информационной безопасности (тест): Сетевичок.ру (сайте www.Сетевичок.рф)

The screenshot shows the 'Викторина' (Quiz) page on the website. The main heading is 'Техническая компетенция' (Technical Competence). Below it, there is a short text: 'Кирилл скачивает программы, как с сайтов официальных разработчиков, так и других сайтов. Он считает, что везде архивы одинаковые и это безопасно.' (Kirill downloads programs, both from official developer websites and other websites. He believes that everywhere archives are the same and this is safe.)

- Скачивать нужно только с официального сайта разработчика
- Можно скачать с сайта не разработчика, но проверить достоверность его хеша (например, в Kaspersky Application Advisor)
- Скачивать можно с любого сайта

At the bottom, there is a section for joining a social network: 'Присоединяйся к нам в социальной сети Вконтакте' (Join us on the social network VKontakte). It mentions support from the Federal Agency for Mass Information and Communications and the 'Страна молодых' (Young Country) movement.

The screenshot shows the user profile page on the website. The main heading is 'Сообщение' (Message) with a sub-heading 'Вы успешно вошли на сайт' (You have successfully logged in to the site). There is a 'Выйти' (Logout) button.

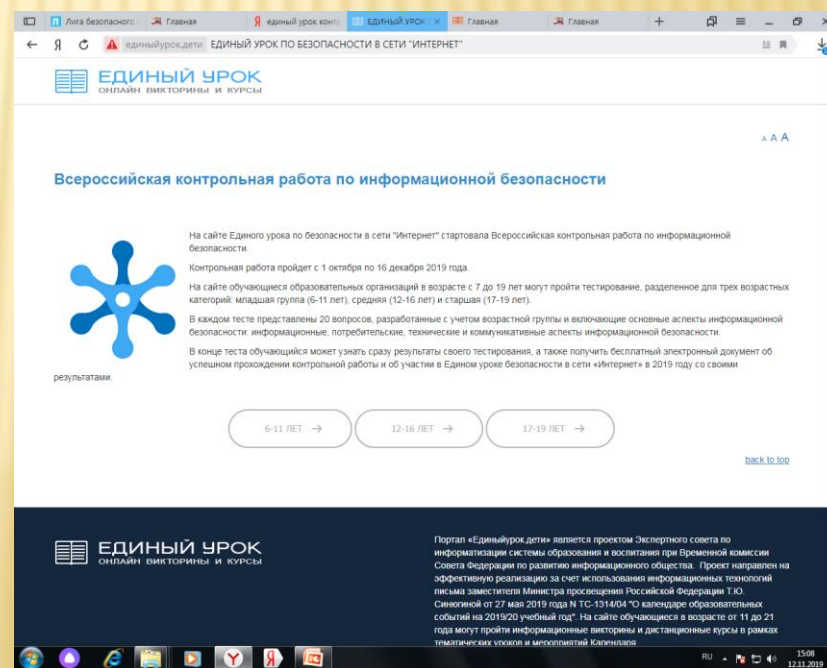
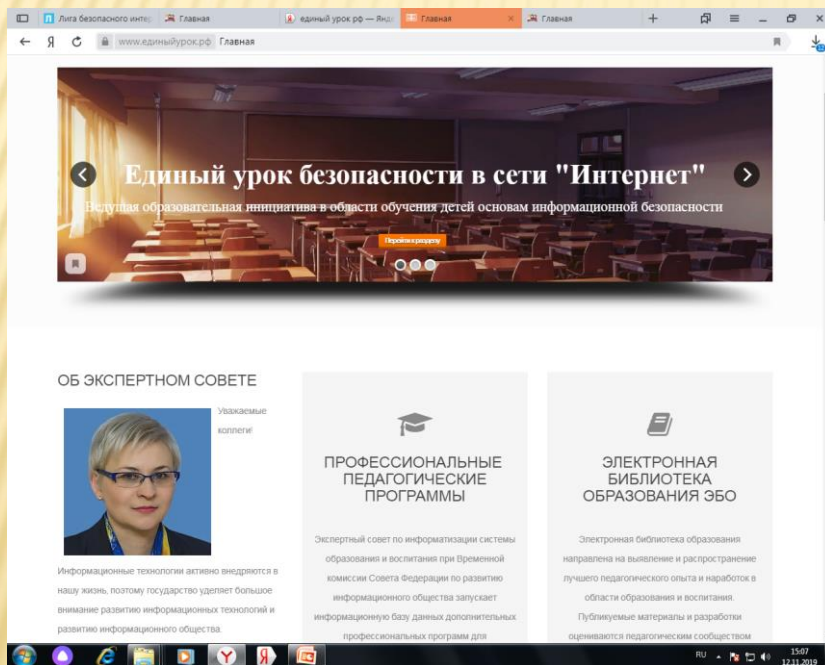
Below the message, there is a section for 'Твои данные' (Your data) with three tabs: '1 задание', '2 задание', and '3 задание'. The data is as follows:

Имя пользователя	Оля0911
IP адрес	-
Укажи свой возраст	Учащийся 9-11 класс (студент СПО)
Фамилия	Туровская
Имя	Ольга
Отчество	Витальевна
Твой субъект Федерации или страна	Тамбовская область
Твой муниципалитет	ГО город Тамбов

On the right side, there is a 'Приветствуем Вас, Оля0911' (Welcome you, Olya0911) section with a profile picture and a 'Выйти' (Logout) button. Below that, there is a 'Мой рейтинг' (My rating) section showing a score of 250.00. At the bottom right, there is a section for 'Активация купона за опрос и Премия' (Coupon activation for survey and Prize) with a 'Получить баллы' (Get points) button and a note: '(код купона можно получить, пройдя опрос и приняв участие в судействе)' (coupon code can be obtained by completing the survey and participating in the judging).

Задача №5

Участие Всероссийской контрольной работы по информационной безопасности на портале Единого урока www.единыйурок.рф



Задача №6

Распространение опыта (наглядного материала – буклет, ролик, плакат) размещение урока на интернет ресурсах, образовательных сайтах



НЕКОТОРЫЕ РЕКОМЕНДАЦИИ РОДИТЕЛЯМ

- ☑ **КиберМама** - проследит за временем работы, предупредит ребенка о том, что скоро ему нужно будет одождать и приостановит работу компьютера, когда заданное вами время истечет.
- ☑ **Time Boss** - предназначена для ограничения времени, которое наши дети проводят за компьютером.
- ☑ **Интернет Цензор** - программа предназначена для эффективной блокировки сайтов, которые могут представлять опасность для ребенка, когда он использует Интернет.
- ☑ **NetPolice** - контентный фильтр, который позволяет осуществлять комплексную защиту детей от Интернет-угроз.
- ☑ **Детский браузер Егудя** это не отдельная программа, а дополнение (додатки) к браузеру Mozilla Firefox.
- ☑ **Родительский контроль в Kaspersky Internet Security**.
- ☑ **Для проверки знаний по информационной безопасности в сети Интернет студенты, родители и педагоги приглашаются**
- ☑ **Порталом информационной безопасности www.единныгрок.рф**



РЕСУРСЫ СЕТИ ИНТЕРНЕТ

1. Сайт ТОГБПОУ «Колледж торговли, общественного питания и сервиса» - <http://ktpois.68edu.ru/>
2. Азбука безопасности для детей и подростков <http://azben.com/safety/internet>
3. Дети России он-лайн / «Премия Рунета 2011» Ресурсы для детей и родителей и мн.др. <http://detonline.com>
4. Лига безопасного интернета Горячая линия по приёму сообщений о противоправном контенте в сети Интернет <http://www.ligainternet.ru/>
5. Статья для родителей «Обеспечение безопасности детей при работе в Интернет». Рекомендации по программе «Родительский контроль» Компьютерный информационный портал <http://www.ozzone.net/6213/>
6. Сайт www.Сетевычок.рф
7. Портал информационной безопасности в сети интернет для детей родителей и педагогов. www.единныгрок.рф

ТОГБПОУ «Колледж торговли, общественного питания и сервиса»

2019г.



*Единый урок
по безопасности в сети
«Интернет»*

**ПРАВИЛА
БЕЗОПАСНОСТИ В
СЕТИ ИНТЕРНЕТ ДЛЯ
СТУДЕНТОВ,
ПРЕПОДАВАТЕЛЕЙ,
РОДИТЕЛЕЙ**

Приложение 2

Информация об итогах Единого урока по безопасности в сети «Интернет» в 2019 году

наименование организации

	Показатели	Профессиональные образовательные организации
1.	Общее количество детей в организации	
2.	Общее количество родителей (законных представителей) детей в организации	
3.	Общее количество педагогических работников в организации	
4.	Количество вовлеченных детей в проведение Единого урока	
4.1	Количество участников Всероссийской контрольной работы по информационной безопасности на портале Единого урока www.Единыйурок.дети	
4.2	Количество участников международного квеста по цифровой грамотности «Сетевичок» на сайте www.Сетевичок.рф	
5.	Количество вовлеченных родителей (законных представителей) детей в проведение Единого урока	
5.1	Количество проведенных родительских собраний	
5.2	Количество родителей (законных представителей) детей, принявших участие в исследовании «Образ жизни подростков в сети»	
5.3	Количество родителей (законных представителей) детей, прошедших образовательные программы в области безопасности и развития детей в сети «Интернет»	
6.	Количество вовлеченных педагогических работников в проведение Единого урока	
6.1	Количество педагогических работников, прошедших программы повышения квалификации по вопросам обеспечения безопасности и развития детей в информационном пространстве в образовательных организациях дополнительного профессионального образования	
6.2	Количество педагогических работников, прошедших программы повышения квалификации по вопросам обеспечения безопасности и развития детей в информационном пространстве в рамках Всероссийской конференции по формированию цифрового детского пространства «Сетевичок»	
7	Количество образовательных организаций, в которых организовано обучение детей основам информационной безопасности на системном уровне	

1] Организация обучения работников образовательных организаций по образовательным программам повышения квалификации, включенным в программу Всероссийской конференции по формированию цифрового детского пространства «Сетевичок», на сайте Экспертного совета по информатизации системы образования и воспитания при Временной комиссии Совета Федерации по развитию информационного общества по адресу www.единыйурок.рф (в разделе «Проекты», пункт «Конференция по формированию цифрового детского пространства «Сетевичок»). Бесплатное обучение по денным образовательным программам включает изучение лекционного материала и получение документов об обучении.