МАУК «МКДЦ»
Центральная районная библиотека
Информационно-консультационное бюро

«СВОБОДА И ОТВЕТСТВЕННОСТЬ В ИНТЕРНЕТЕ»

Интернет — интересный и многогранный мир, который позволяет узнавать много нового, общаться с людьми на разных концах света, играть в игры и делиться с другими своими фотографиями.

Свобода – это выбор, иными словами добровольное решение творить добро или зло, совершать похвальные или дурные поступки, то есть быть добродетельным или преступным.

Ответственность - это способность отвечать миру, отвечать подлинно из глубины себя.

Интернет (англ. Internet) — это всемирная система объединённых компьютерных сетей для хранения и передачи информации.

С появлением в 1969 г. Интернета весь мир поделился на два понятия:

ОНЛАЙН (Интернет) и ОФФЛАЙН (обычная, традиционная жизнь).

Практически все, что есть в ОФФЛАЙНЕ, уже присутствует и в ОНЛАЙНЕ.

ВОЗМОЖНОСТИ СЕТИ ИНТЕРНЕТ

Электронная почта

Общение. Существует множество программ и интернет-сервисов, позволяющих общаться. Это программы для обмена сообщениями (ICQ, Mail.ru Агент), социальные сети (Facebook, В Контакте, Одноклассники), тематические форумы и многое-многое другое.

Поиск информации

Поиск людей

Развлечения

Обмен файлами

Обучение

Совершение покупок в интернет-магазинах

Просмотр видео информации

Заработок. Существует множество специализированных сайтов, размещающих вакансии работодателей и резюме соискателей. Кроме того, вы можете работать удаленно.

Роль интернета в жизни современного человека сложно переоценить. Он фиксирует и концентрирует в себе современную реальность, является почти незаменимым помощником в работе, общении и отдыхе. Через интернет мы совершаем покупки, общаемся с людьми, которые могут быть за тысячи километров от нас, находимся в курсе самых последних событий со всего мира.

ОПАСНОСТИ СЕТИ ИНТЕРНЕТ

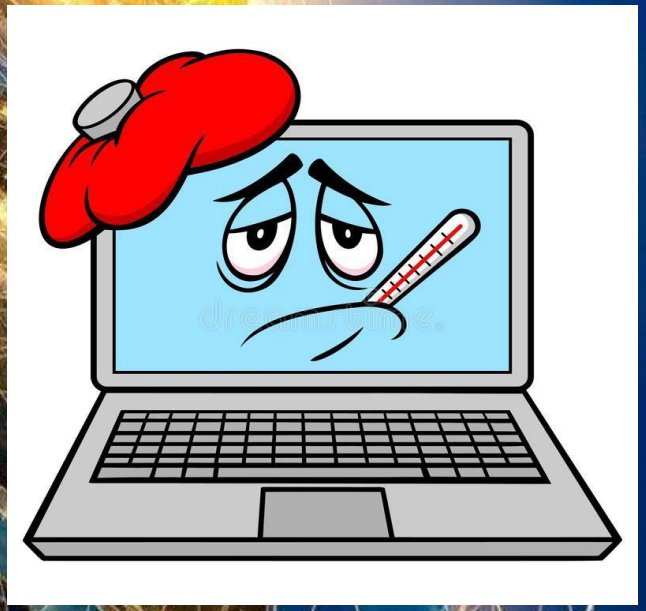
Угроза № 1. Вредоносные программы (Вирусы).

Вредоносная программа – это любая программа, которая наносит вред компьютеру или пользователю этого компьютера. Некоторые виды рекламы считаются вредоносными программами.

Сегодня вирусы пишутся с расчетом на коммерческую выгоду!

СИМПТОМЫ ЗАРАЖЕНИЯ ПК ВИРУСОМ

- ПК долго загружается и долго выключается;
- автоматическое открытие окон с незнакомым содержимым при запуске ПК;
- блокировка доступа к официальным сайтам антивирусных компаний;
- появление новых неизвестных процессов в окне «Процессы» диспетчера задач;
- запрет на изменение настроек компьютера в учётной записи администратора;
- невозможность запустить исполняемый файл (выдаётся сообщение об ошибке);
- появление всплывающих окон или системных сообщений с непривычным текстом;
- перезапуск компьютера во время старта какой-либо программы;
- случайное или беспорядочное отключение компьютера;
- случайное аварийное завершение программ.



Угроза № 2. Мошенничество.

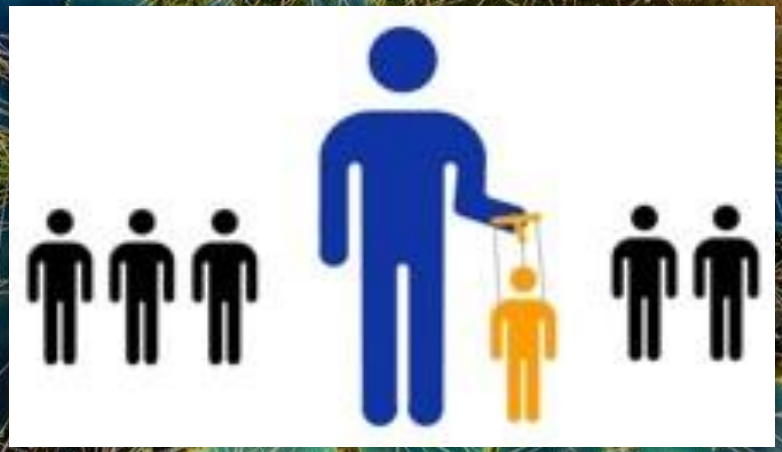
Мошенничество в Интернете приобретает все большие масштабы. Изобретаются новые уловки доступа злоумышленников к компьютерам пользователей с целью выкачивания у них денег.

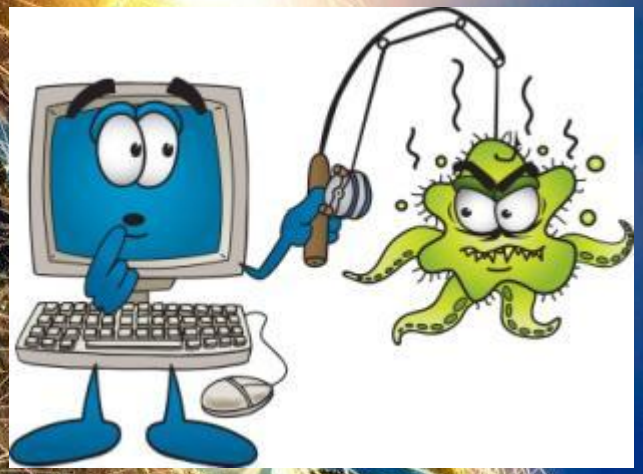
КАКИМ ОБРАЗОМ ЗЛОУМЫШЛЕННИКИ МОГУТ ПОЛУЧИТЬ ДОСТУП К ВАШЕМУ КОМПЬЮТЕРУ?

Первый приём. **Социальная инженерия**.

Это метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным.

Сегодня социальную инженерию зачастую используют в интернете для получения закрытой информации, или информации, которая представляет большую ценность. Благодаря использованию уловок и психологических приемов, вы открываете присланное хакерами письмо, содержащее вирус.





Второй приём. Фишинг («рыбалка»).

В интернете создаются подделки популярных сайтов и пользователи «клюют на эту наживку». Так вместо официальной страницы своего банка вы можете оказаться на его поддельной копии со всеми вытекающими последствиями.

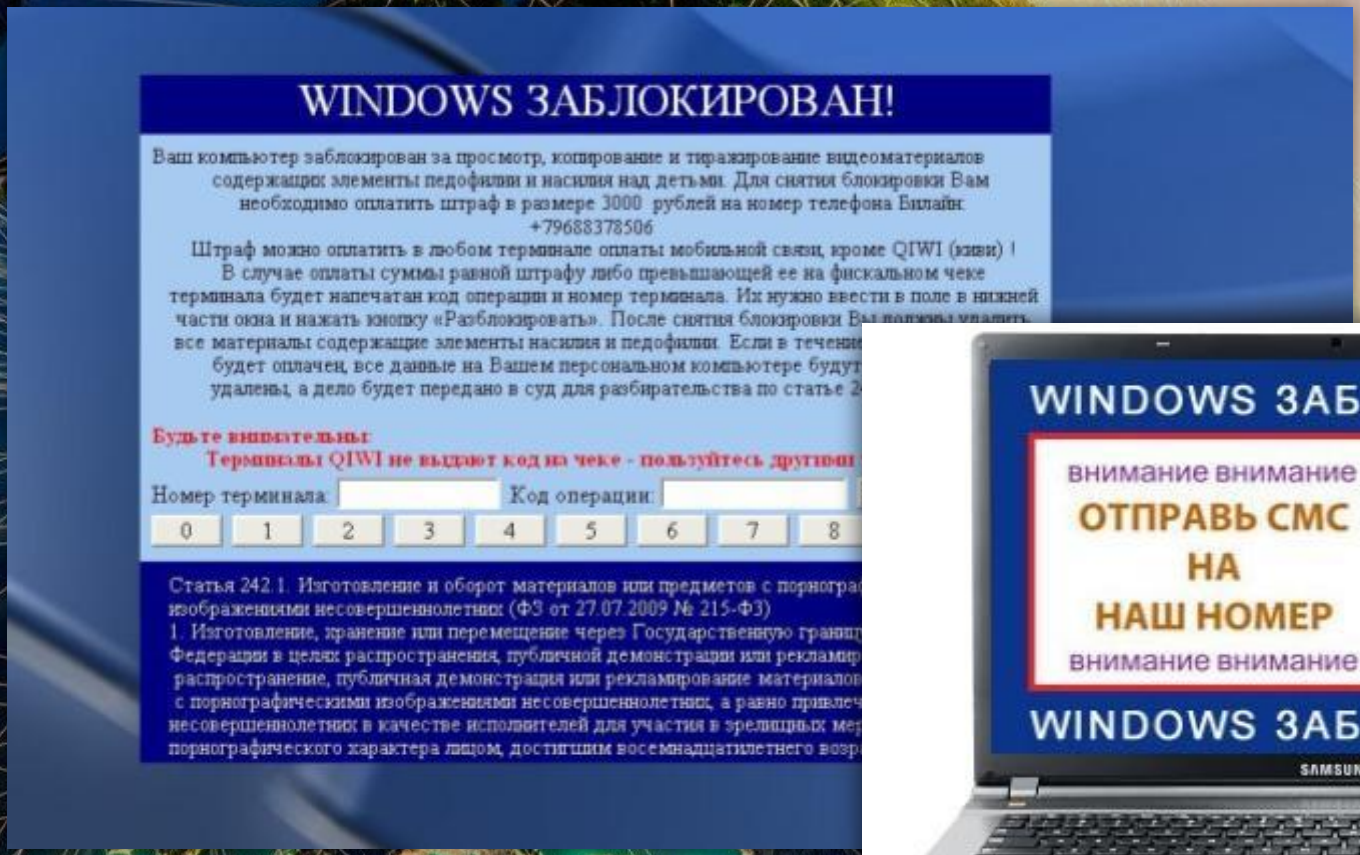
Третий приём. Предложение бесплатного программного обеспечения. Это как правило уловки, содержащие в себе множество вирусов и троянов.

Троянская программа (также — **троя́н**, **троя́нец**, **троя́нский конь**) — это разновидность вредоносной программы, проникающая в компьютер под видом легального программного обеспечения, в отличие от *вирусов* и *червей*, которые распространяются самопроизвольно.

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: *сбор информации и её передачу злоумышленнику, её разрушение или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.*

Четвёртый приём. 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.



Угроза № 3 . Интернет-зависимость.

Детская и подростковая интернет-зависимость с каждым днем набирает все большие масштабы. Общение в социальных сетях заменяют общение с родителями и сверстниками, подвижные игры и физические занятия. Теряются коммуникационные навыки. Живые эмоции заменяются «веселыми смайликами».

Углубившись в виртуальное общение, человек перестает гулять на улице, встречаться с друзьями и мало двигается, как следствие, наступают проблемы со зрением, пищеварением, опорно-двигательным аппаратом, появляется повышенная утомляемость и головокружения.


Twitter
Windows
ВКОНТАКТЕ
internet

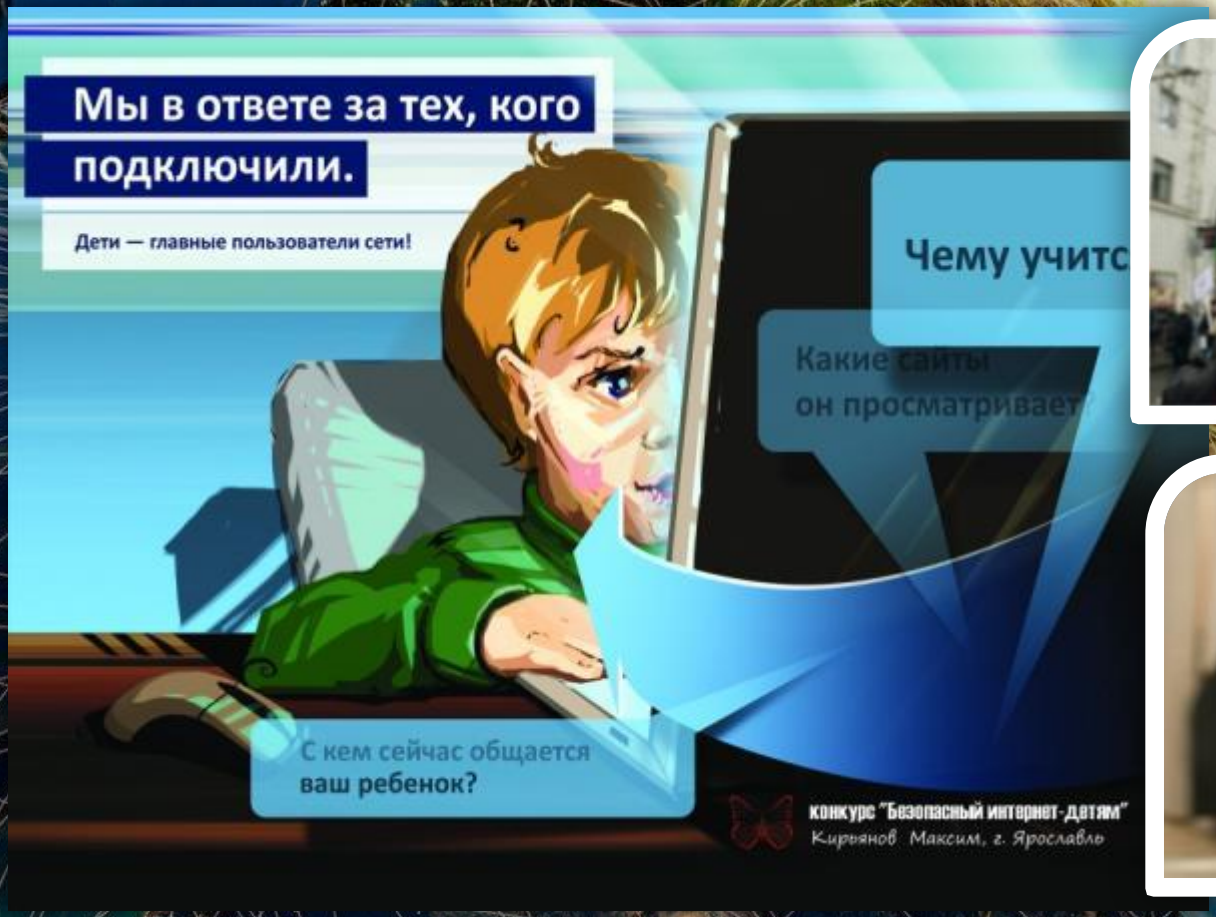
Угроза № 4. Пренебрежение к учебе.

В Интернет много учебного материала, который становится доступным для пользователя после процедуры скачивания, занимающей не более пяти минут. Подростки распечатывают нужный реферат и сдают его преподавателю, даже не удосужившись его прочитать. Таким образом, никакие знания получены не будут. Не в помощь школьнику и «решебники» по любым дисциплинам. Дети, привыкшие регулярно списывать, самостоятельно перестают учиться, а значит усваивать материал и развиваться.

Угроза № 5. Доступ к сайтам, содержащим опасную информацию.

Путешествуя по просторам Интернета легко можно оказаться на сайтах, содержащих опасную для подростков информацию. Например: *порнография, суициды, сцены насилия и жестокости, призывы к экстремистским действиям и прочее.*

Отсечь доступ к сайтам с этим содержанием помогают поисковые фильтры, настройки приватности и программы «Родительский контроль".



Угроза № 6. Виртуальное общение.

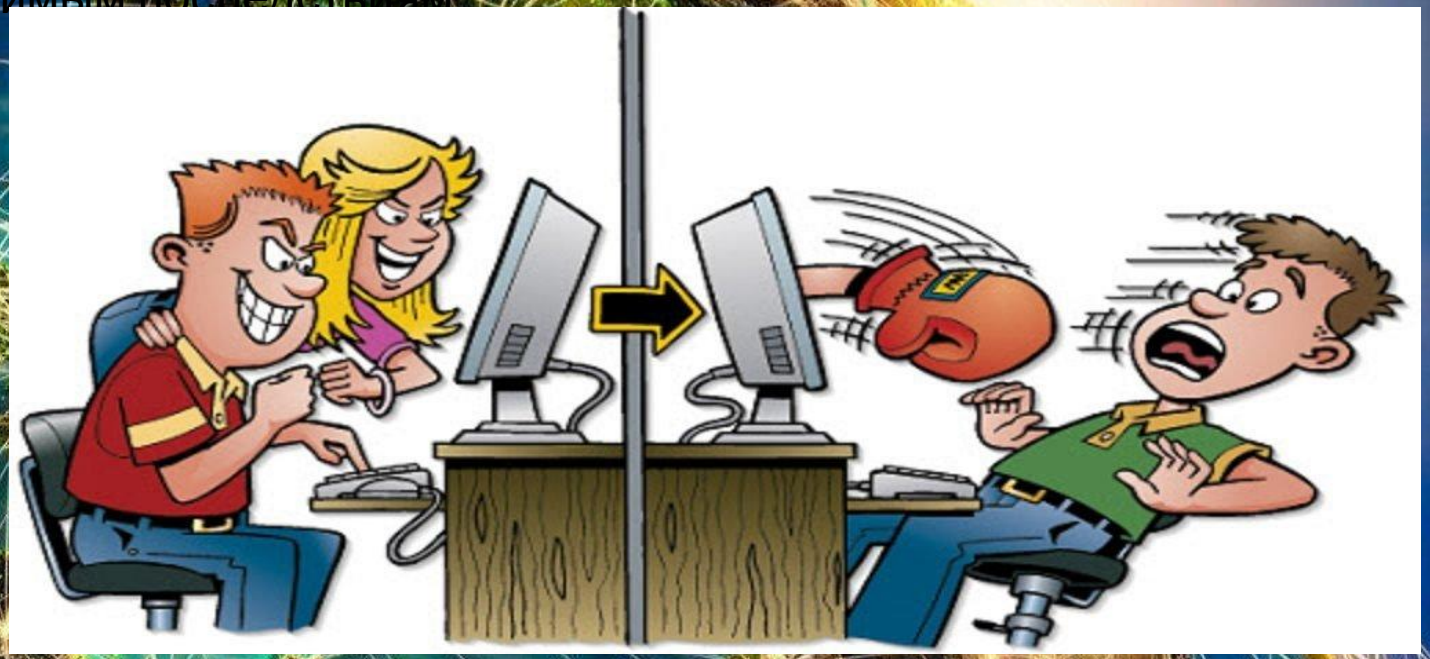
Виртуальное общение - это мир фантазий. Собеседник в Интернете может выдавать себя за кого-то другого. Здесь почти у каждого есть своя маска, свой тип поведения, причем он отличается часто от реальности. Почти каждый скрыт под аватарками, вымышленными именами и своими фантазиями.

Важно знать, что по закону ответственность за содержание текста несёт не только автор, опубликовавший информацию, но и пользователь, распространивший её — поставивший отметку «Мне нравится» или скопировавший её на свою страницу.

Угроза № 7. Интернет-хулиганство.

Одна из проблем, с которой можно столкнуться в социальных сетях - это оскорбления - *троллинг.*

Иногда это выглядит как обычное развлечение, своеобразная переписка, но очень часто *тролль* (так называют таких людей) выходит за рамки дозволенного и давит на самые болевые точки. Очень часто «популярные» дети, которые имеют определеннное влияние в классе, начинают терроризировать человека через интернет. Порой это приводит к необратимым последствиям.



Троллинг – это способ общения в сети, целью которого является провоцирование других его участников к конфликтам, выведение их из душевного равновесия, снижение интереса пользователей к ресурсу, где проходит общение.

КАК ОБЕСПЕЧИТЬ ЗАЩИТУ ПК

Пользователь, который только что приобрел персональный компьютер, прежде чем начать покорять Интернет-просторы, должен:

- установить антивирус и антишпионское программное обеспечение. После установки обновить их и настроить автоматическое обновление. Лучше если обновление антивируса запускается автоматически вместе с операционной системой.
- проверять антивирусом любую устанавливаемую на ПК программу.

КАК ОБЕСПЕЧИТЬ ЗАЩИТУ ПК

1. Не открывать файлы, скачанные из непроверенных источников.
2. Сразу удалять письма подозрительного содержания.
3. Не обращать внимания на предложения легкого заработка, и уж тем более, не высылать никому своих логинов и паролей.
4. При регистрации использовать сложные пароли из символов, букв и цифр. Назначайте каждый раз новый оригинальный пароль.
5. Соблюдать осторожность, используя интернет в местах общего пользования.
6. С платежными системами безопаснее работать через специальные приложения, а не через официальный сайт.
7. Следить за интернет-трафиком. Резкое увеличение трафика безо всякой причины – серьезный повод для беспокойства.
8. Игнорировать сообщения о крупных выигрышах или получении наследства.
9. Использовать лицензионное ПО.
10. Использовать только проверенные варианты при совершении покупок в интернет – магазинах.

ПЯТЬ ПРАВИЛ БЕЗОПАСНОГО ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

1. Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их.

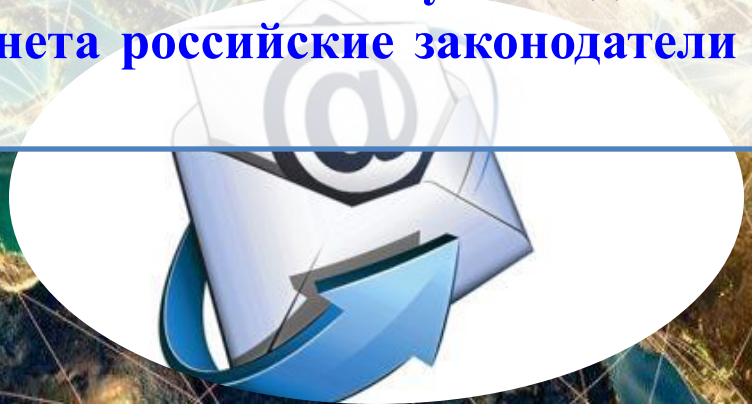
2. Никогда не отвечайте на спам.

3. Применяйте фильтр спама или программы работы с электронной почтой.

4. Создайте новый или используйте семейный адрес электронной почты для Интернет-запросов, дискуссионных форумов и т.д.

5. Никогда не пересылайте «письма счастья». Вместо этого сразу удаляйте их.

Раньше СМИ отвечали за каждое своё слово, а в Интернете царила свобода. Сегодня по количеству введённых запретов для пользователей Интернета российские законодатели перегнали многие развитые страны.

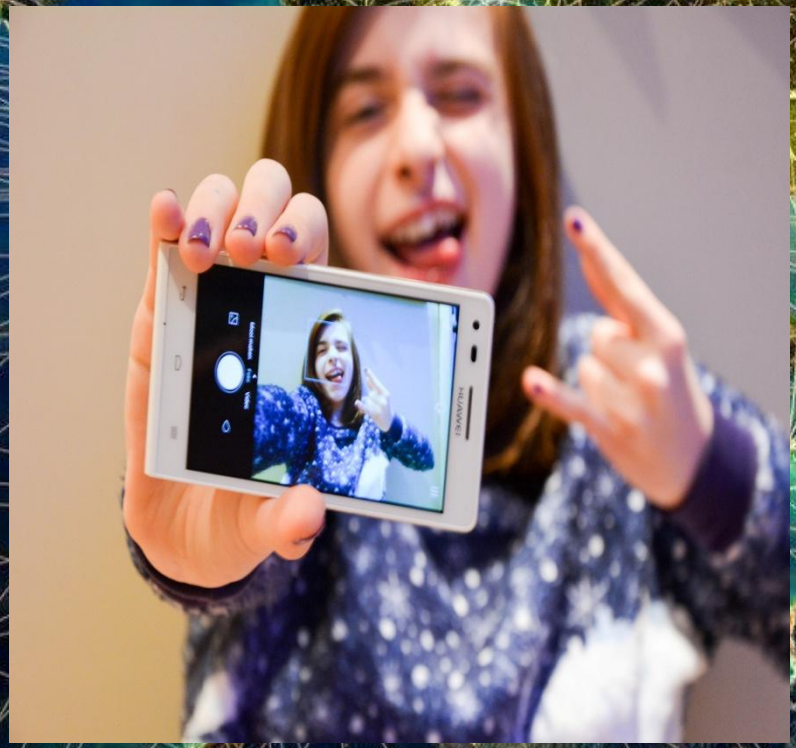


ПРОФИЛАКТИКА ИНТЕРНЕТ-ЗАВИСИМОСТИ

- Активизировать воспитательную работу в семье и учебных заведениях.
- Сократить время, которое вы проводите в Интернет.
- Вести активный, здоровый образ жизни, распределяя время для спорта, учёбы и развлечений.
- Расширить круг общения со сверстниками.
- Поддерживать доброжелательные отношения с родителями и друзьями.

ПРАВИЛА БЕЗОПАСНОГО ПОВЕДЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

- Не заполняйте все поля вашего профиля.
- Не нужно выкладывать в социальных сетях откровенные фотографии.



- Не регистрируйтесь под чужими данными. Если хотите сохранить инкогнито – прибегните к вымышленному имени.
- Не используйте чужие изображения без разрешения этих людей.
- Никогда не используйте социальную сеть или иной подобный сервис в качестве основного хранилища информации.

- 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 участвуйте в сомнительных акциях.
- НИКОГДА не переходите по длинным ссылкам, это чаще всего путь к зараженному вирусом файлу.
- Соблюдайте культуру общения в сети.

- Не пишите в ленте о своих сомнительных с точки зрения закона «подвигах».
- Не добавляйте в друзья всех подряд.
- Не вступайте в сомнительные сообщества, куда вас приглашают непонятные люди.

К федеральным законам, обеспечивающим интернет безопасность детям можно отнести:

- Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" (в ред. от 23.12.2010).
- Федеральный закон от 27 июля 2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации".
- Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" от 29.12.2010 N 436-ФЗ .

Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" регулируются отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами (далее - государственные органы), органами местного самоуправления, иными муниципальными органами (далее - муниципальные органы), юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий (операций), совершаемых с персональными данными с использованием средств автоматизации, то есть позволяет осуществлять в соответствии с заданным алгоритмом поиск персональных данных, зафиксированных на материальном носителе и содержащихся в картотеках или иных систематизированных собраниях персональных данных, и (или) доступ к таким персональным данным.

Цель настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Сфера действия Федеральный закон "Об информации, информационных технологиях и о защите информации"

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим Федеральным законом.

Федеральный закон "О защите детей от информации, причиняющей вред их здоровью и развитию" 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, а также предусматривающий отнесение информационной продукции к одной из пяти категорий, и запрещающий её распространение среди детей в зависимости от их возраста.

1) информационная продукция для детей, не достигших возраста шести лет;

2) информационная продукция для детей, достигших возраста шести лет;

3) информационная продукция для детей, достигших возраста двенадцати лет;

4) информационная продукция для детей, достигших возраста шестнадцати лет;

5) информационная продукция, запрещенная для детей (информационная продукция, содержащая информацию, предусмотренную частью 2 статьи 5 настоящего Федерального закона).

К информации, запрещенной для распространения среди детей, относится информация:

1) побуждающая детей к совершению действий, представляющих угрозу их жизни и (или) здоровью, в том числе к причинению вреда своему здоровью, самоубийству, либо жизни и (или) здоровью иных лиц, либо направленная на склонение или иное вовлечение детей в совершение таких действий;

2) способная вызвать у детей желание употребить наркотические средства, психотропные и (или) одурманивающие вещества, табачные изделия, никотинсодержащую продукцию, алкогольную и спиртосодержащую продукцию, принять участие в азартных играх, заниматься проституцией, бродяжничеством или попрошайничеством;

3) обосновывающая или оправдывающая допустимость насилия и (или) жестокости либо побуждающая осуществлять насильственные действия по отношению к людям или животным, за исключением случаев, предусмотренных настоящим Федеральным законом;

3.1) содержащая изображение или описание сексуального насилия;

4) отрицающая семейные ценности, пропагандирующая нетрадиционные сексуальные отношения и формирующая неуважение к родителям и (или) другим членам семьи;

5) оправдывающая противоправное поведение;

6) содержащая нецензурную брань;

7) содержащая информацию порнографического характера;

8) о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), включая фамилии, имена, отчества, фото- и видеоизображения такого несовершеннолетнего, его родителей и иных законных представителей, дату рождения такого несовершеннолетнего, аудиозапись его голоса, место его жительства или место временного пребывания, место его учебы или работы, иную информацию, позволяющую прямо или косвенно установить личность такого несовершеннолетнего.

Что такое контентная фильтрация?

Контентная фильтрация — это способ распознавания и ограничения нежелательного контента.

Контент-фильтр нужен не только коммерческим организациям для защиты от входа в социальные сети или другие отнимающие время сотрудников сайты. Контент-фильтры особенно нужны там, где есть дети. Проблема воровства персональных данных или вовлечения на небезопасные сайты являются одной из наиболее острых. Организации, которые предоставляют детям выход в интернет, должны особенно тщательно следить за «чистотой» посещаемых сайтов. Основные виды опасности выхода в Интернет – это травля, информация о наркотиках, алкоголе и общение с незнакомцами. И это лишь часть того, с чем подросток может столкнутся, лишь выйдя в сеть.

За отсутствие контент-фильтрации или некачественную фильтрацию интернета образовательной организации предписываются штрафы и судебные разбирательства.

ЗАКОН N 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»

ЗАКОН N 114-ФЗ «О противодействии экстремистской деятельности»

Traffic Inspector Inspector Next Generation – отечественное решение сетевой безопасности, основанное на открытом коде OPNsense. Решение предоставляет IT-специалистам мощный набор инструментов для защиты локальной сети от внешних атак.

Traffic Inspector – сертифицированное комплексное решение информационной безопасности.

SkyDNS Школа — облачный сервис для контентной фильтрации доступа в интернет, требующий минимальных сетевых настроек.

Яндекс.DNS — это бесплатный рекурсивный DNS-сервис. Сервера Яндекс.DNS находятся в России, странах СНГ и Западной Европе. Запросы пользователя обрабатывает ближайший дата-центр, что обеспечивает высокую скорость соединения.

Интернет Цензор — бесплатная программа для осуществления родительского контроля

ОТВЕТСТВЕННОСТЬ ЗА ИНФОРМАЦИОННЫЕ ПРАВОНАРУШЕНИЯ

Виды ответственности:

- Административная ответственность;
- Уголовная ответственность;
- Дисциплинарная ответственность;
- Гражданско-правовая ответственность.

Ответственность за экстремистские действия

- **Публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма**

  От штрафа в размере до 500 тысяч рублей до лишения свободы на срок от 2 до 5 лет.

- **Распространение личной или семейной тайны человека**

  От возмещения морального ущерба до лишения свободы на срок до 2 лет.

- **Реабилитация нацизма**

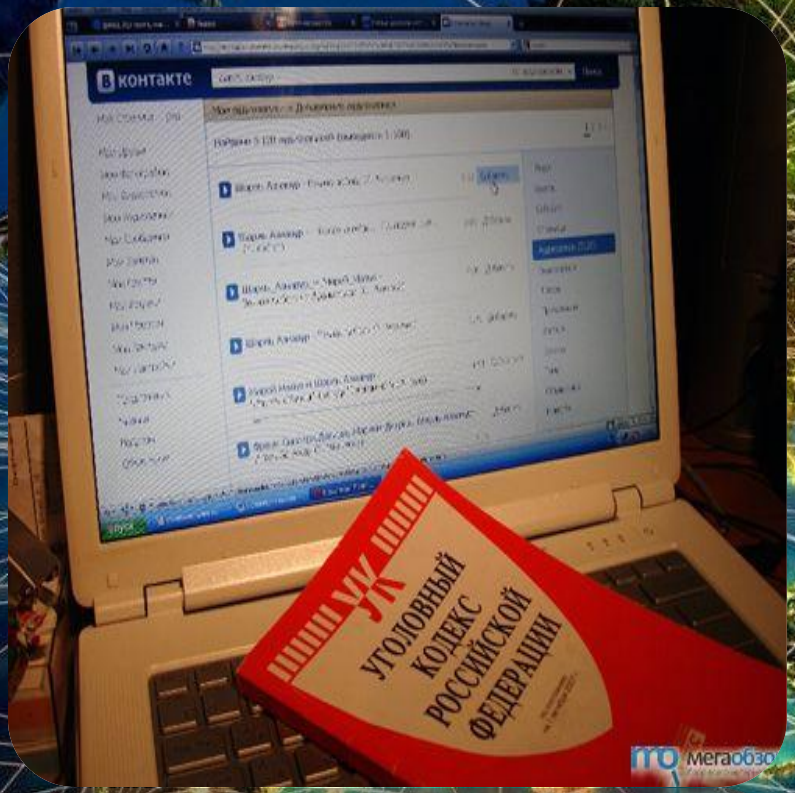
  От штрафа до 300 тысяч рублей до лишения свободы на срок до 3 лет.

- **Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности России**

  От штрафа в размере от 100 до 300 тысяч рублей до лишения свободы на срок до 5 лет.

Список экстремистских материалов опубликован на сайте Минюста. http://minjust.ru/ru/extremist-materials.

Количество случаев привлечения к уголовной ответственности пользователей социальных сетей в России за последние годы увеличилось более чем вдвое.



Большинство подобных дел связаны со статьями Уголовного кодекса РФ, устанавливающими ответственность за экстремизм, оскорбление и клевету.

Гл. 28 «Преступления в сфере компьютерной информации» Уголовного Кодекса РФ

Статья 272. Неправомерный доступ к компьютерной информации

Т.е. информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ или их сети, то предусматривается наказание от

штрафа в размере до 200 000 до лишения свободы на срок до 2 лет.

То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, - наказывается:

штрафом в размере от 100 000 до 300 000 р. либо лишением свободы на срок до 5 лет.

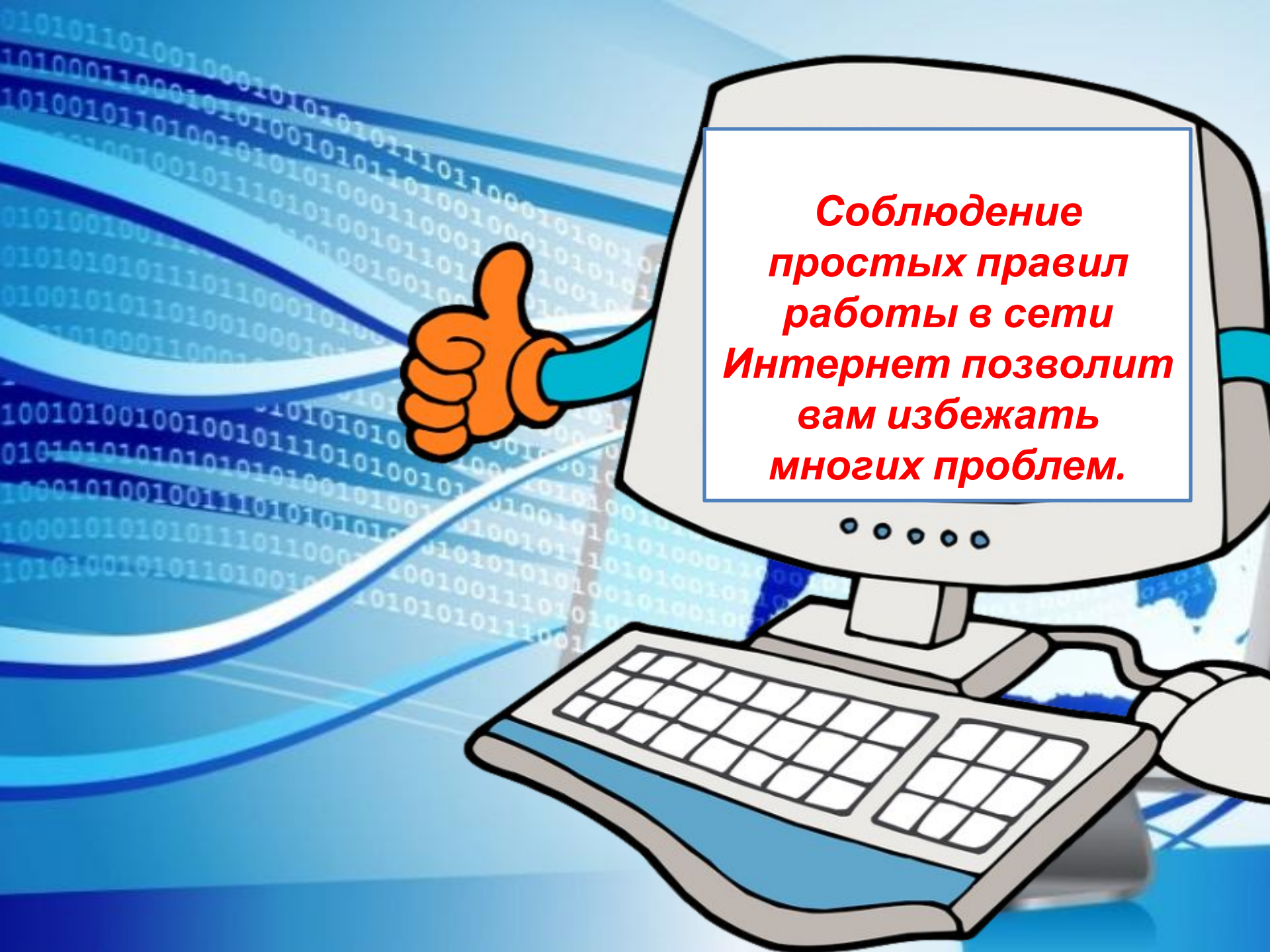
или штраф в размере зар. платы или иного дохода осужденного за период от 1 года до 2-х лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

Заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети наказываются:

лишением свободы на срок до 3-х лет со штрафом в размере до 200 000 р.;

Те же деяния, повлекшие по неосторожности тяжкие последствия, наказываются лишением свободы на срок от 3 до 7 лет.


Соблюдение простых правил работы в сети Интернет позволит вам избежать многих проблем.


Спасибо за внимани