ГБОУ СОШ № 447 Курортного района Санкт-Петербурга

ОТКРЫТЫЙ СЕМИНАР ПО ТЕМЕ

# БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ

2019
Санкт-Петербург

**30 октября в России отмечают Всемирный день безопасности в сети Интернет.**

С целью обеспечения информационной безопасности пользователей при использовании ресурсов сети во многих образовательных организациях проводят открытые уроки и семинары.

Наш семинар призван привлечь дополнительное внимание студентов и преподавателей к проблеме подростковой безопасности в Интернете и развитию информационной грамотности студентов.

**Интернéт (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.

В связи с массовой популярностью сети Интернет важной проблемой сегодня является безопасность в глобальной сети. Касается данная проблема абсолютно всех, начиная от детей и заканчивая пенсионерами.

# ОПАСНОСТИ СЕТИ ИНТЕРНЕТ

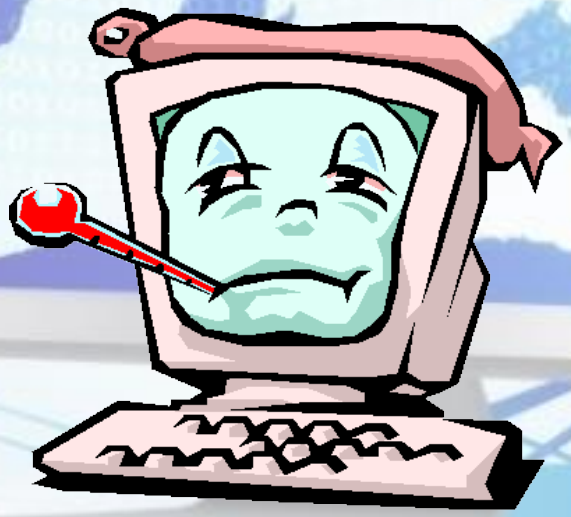
**Угроза № 1. Вредоносные программы (Вирусы).**

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.**

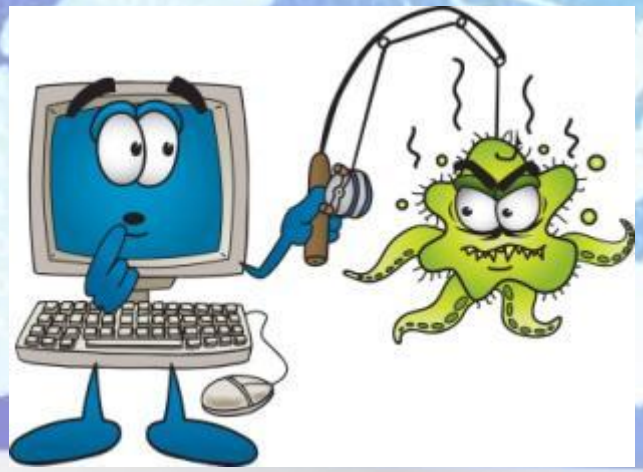
Мошенничество в Интернете приобретает все большие масштабы. Изобретаются новые уловки доступа злоумышленников к компьютерам пользователей с целью выкачивания у них денег.

# 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.

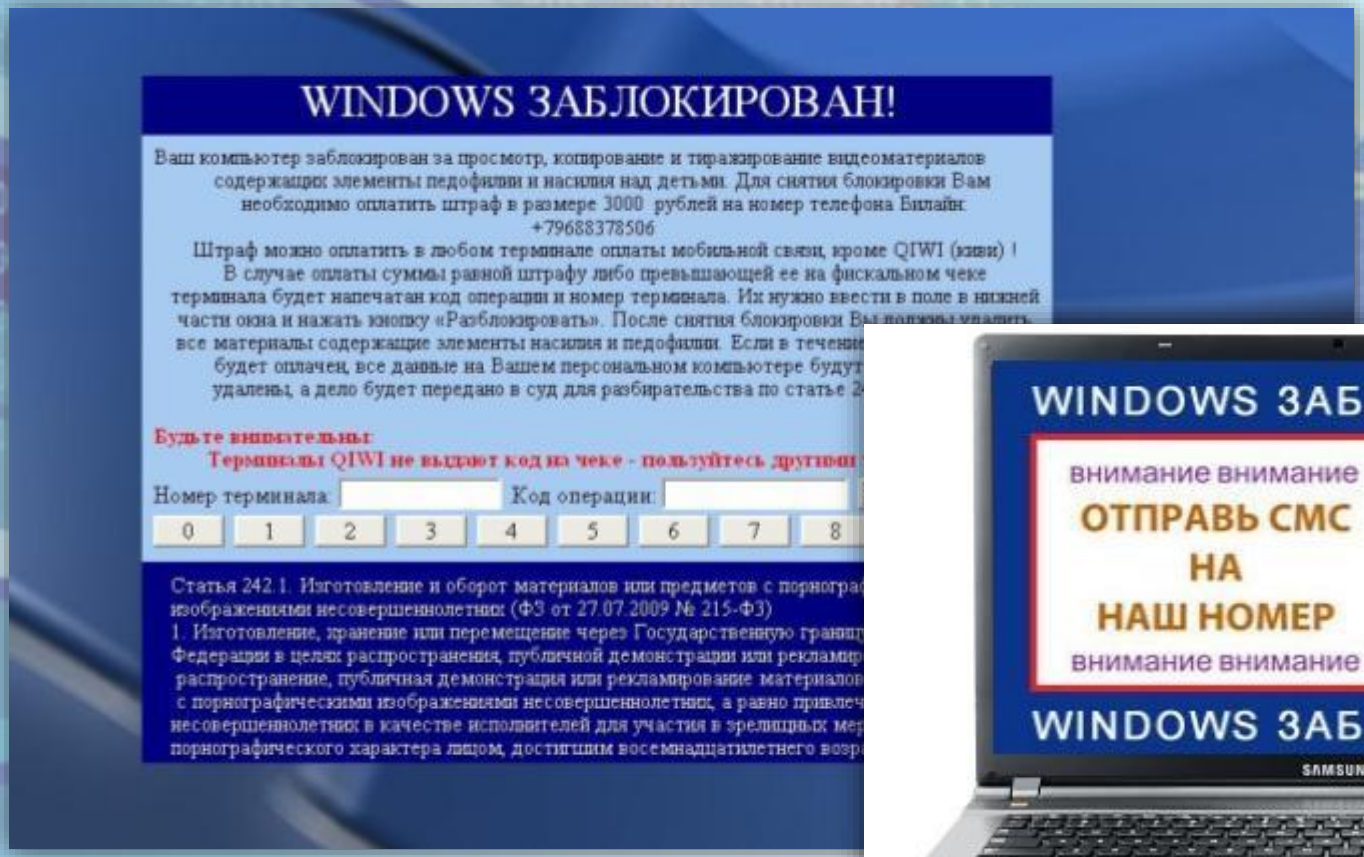
**Третий приём. Предложение бесплатного программного обеспечения**.
Это как правило уловки, содержащие в себе множество вирусов и троянов.

**Троя́нская 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.



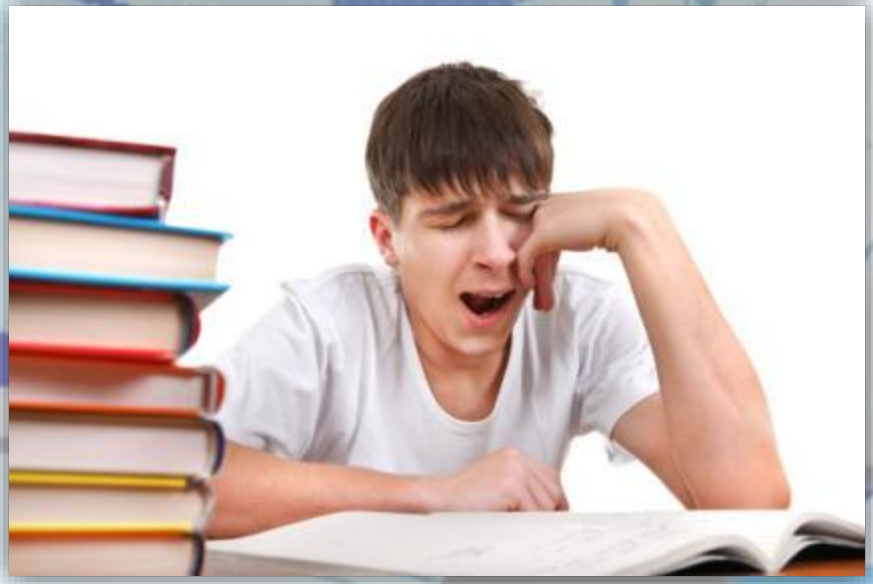

**Угроза № 3 . Интернет-зависимость.**

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.

**Угроза № 4. Пренебрежение к учебе.**

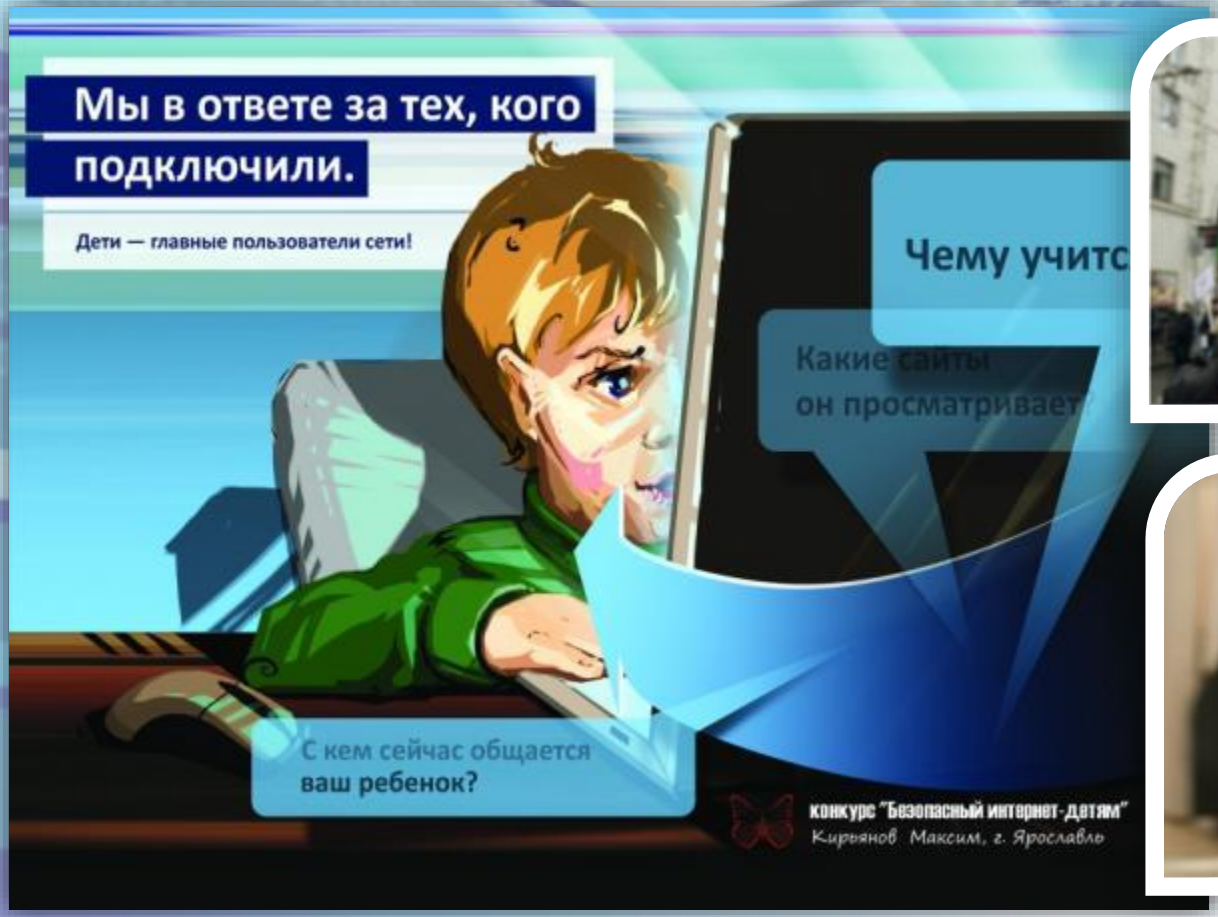
В Интернет много учебного материала, который становится доступным для студентов после процедуры скачивания, занимающей не более пяти минут. Подростки распечатывают нужный реферат и сдают его преподавателю, даже не удосужившись его прочитать. Таким образом, никакие знания получены не будут. Не в помощь студенту и «решебники» по любым дисциплинам. Студент, привыкший регулярно списывать, самостоятельно перестает учить, 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 молодые люди, которые имеют влияние на определенную аудиторию, 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 проходило 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.

# ОТВЕТСТВЕННОСТЬ ЗА ИНФОРМАЦИОННЫЕ ПРАВОНАРУШЕНИЯ

**Виды ответственности:**

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

## Ответственность за экстремистские действия в сети

- **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**

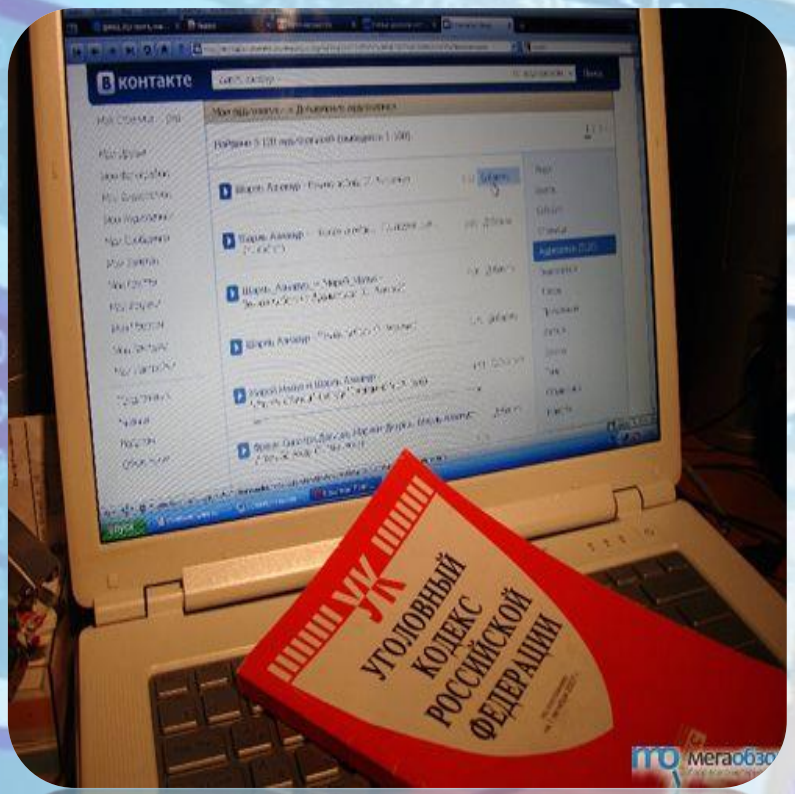
  **От штрафа до 300 тысяч рублей до лишения свободы на срок до 3 лет.**

- **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.

# Анкета

**Ваш возраст**

- до 18 лет
- более 18 лет

**1. С каких устройств вы чаще выходите в Интернет?**

a. Стационарный компьютер дома
b. Стационарный компьютер в колледже
c. Мобильные устройства (смартфон, планшет)
d. Ноутбук
e. Другое (укажите)

**2. Как часто вы обращаетесь к Интернету в поисках информации?**

a. Очень часто (несколько раз в день)
b. Довольно часто (почти каждый день)
c. Часто (несколько раз в неделю)
d. Редко (3-4 раза в месяц)
e. Очень редко (1-2 раза в месяц)

**3. Какое примерное количество сайтов вы посещаете за день? Ответ дайте в виде числа.**

**4. Какие сайты в Интернете вы считаете надежными?**

**Приведите название (не адрес!) одного сайта, информации которого вы доверяете.**

**5. Как вы думаете, будет ли ваша работа в будущем связана с деятельностью в Интернете?**

a. Да
b. Нет
c. Не знаю

**6. Чему Вы уделяют больше времени в Интернете?**

a. Учеба
b. Работа
c. Общение
d. Игры
e. Фильмы, музыка
f. Другое

**7. Где Вам проще общаться?**

a. В реальной жизни
b. В виртуальном пространстве Интернета (социальных сетях, на сайтах знакомств и пр.)

**8. Занятость родителей в Интернете. Чему уделяют больше времени в Интернете взрослые в вашей семье?**

a. Учеба
b. Работа
c. Общение
d. Игры
e. Фильмы, музыка
f. Другое

**9. Чем опасны социальные сети?**

a. Личная информация может быть использована кем угодно в разных целях
b. При просмотре неопознанных ссылок компьютер может быть взломан
c. Социальные сети не представляют опасности

**10. Какую информацию нельзя разглашать в Интернете?**

a. Свои увлечения
b. Свой псевдоним
c. Домашний адрес
d. Информацию о других без их согласия
e. Пароли, номера банковских карт и пр.

**11. Действуют ли правила этикета в Интернете?**

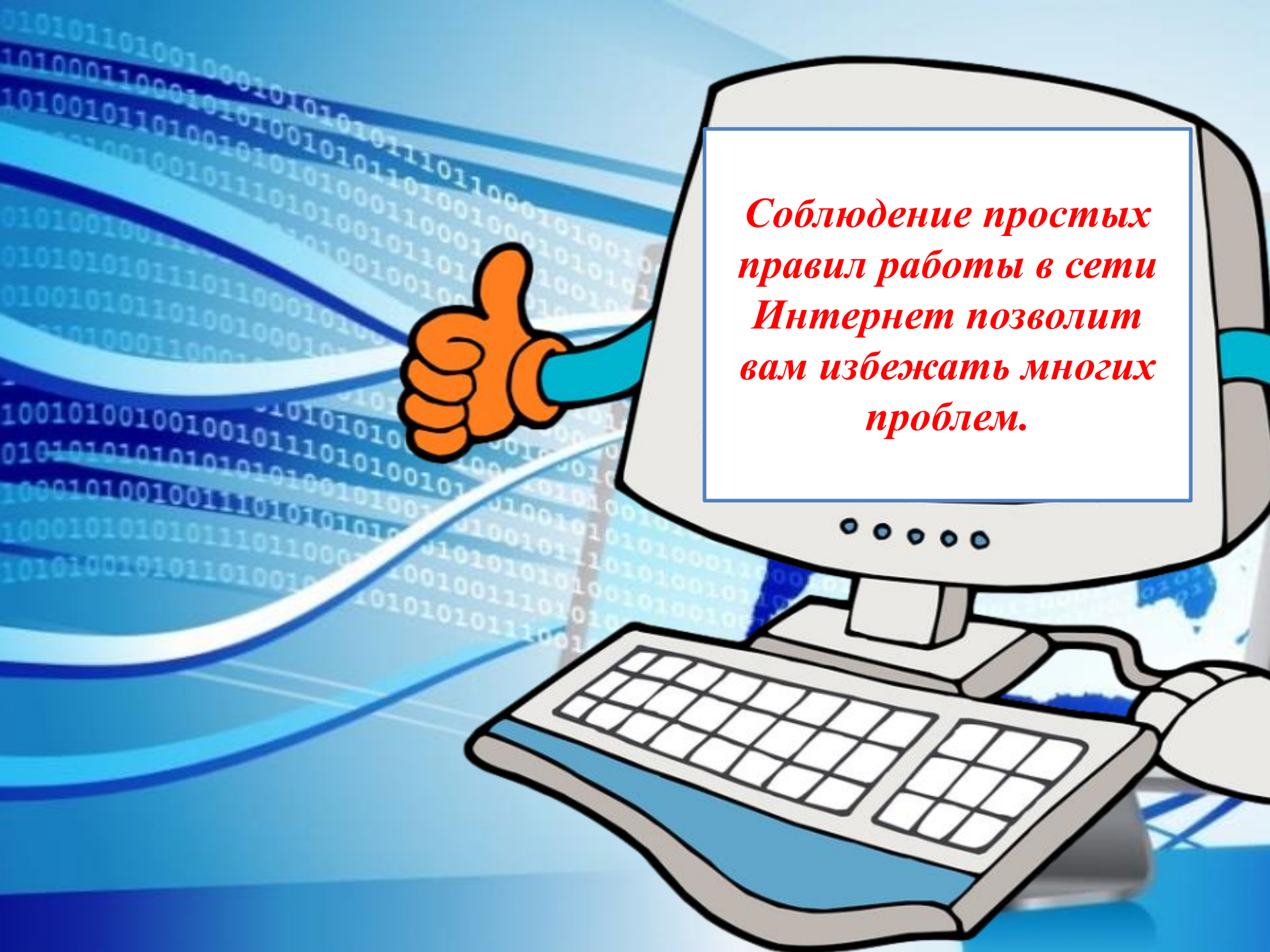
a. Интернет - пространство свободное от правил
b. В особых случаях
c. Да, как и в реальной жизни

**12. Использование Интернета является безопасным, если:**

a. защитить свой компьютер в Интернете и соблюдать все правила информационной безопасности
b. разглашать личную информацию
c. регулярно обновлять операционную систему
d. создавать резервные копии документов
e. регулярно обновлять антивирусную базу данных
f. посещать непроверенные сайты

**13. Что в Интернете запрещено законом?**

a. Размещать информацию о себе
b. Призывать к суициду
c. Размещать информацию о других без их согласия
d. Общаться
e. Копировать файлы для личного использования
f. Вести экстремистскую деятельность
g. Осуществлять неправомерный доступ к закрытой информации
h. Совершать покупки
i. Создавать, использовать и распространять вредоносное ПО
j. Участвовать в онлайн-опросах


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

# Использованные Интернет-источники


https://ru.wikipedia.org/wiki/

http://bezwindowsa.ru/internet-i-seti/bezopasnost-v-seti-internet.html

www.chmtt.inf

http://www.consultant.ru

https://yandex.ru/images/

# Спасибо за внимание!