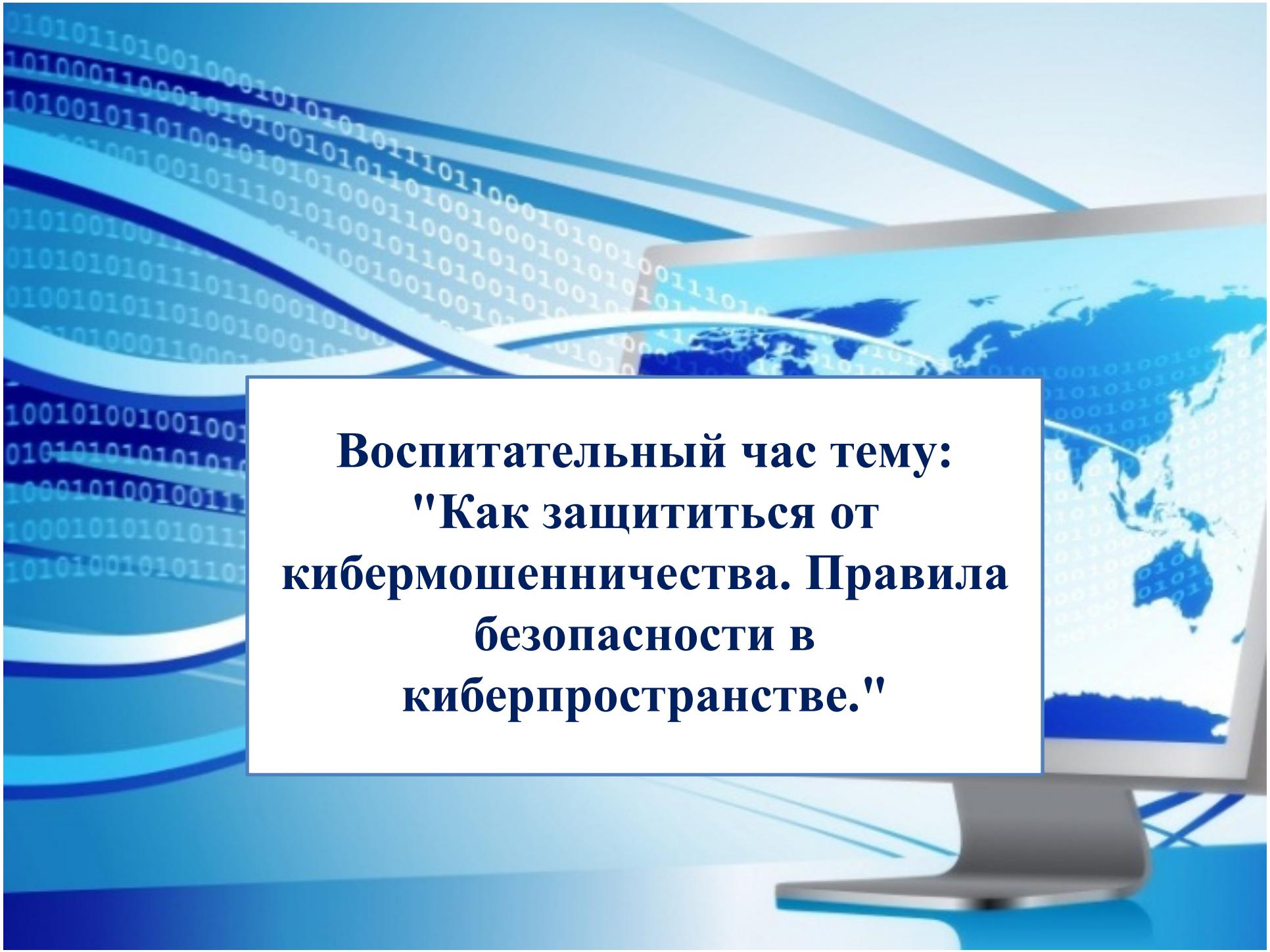

Воспитательный час тему:
"Как защититься от кибермошенничества. Правила безопасности в киберпространстве."

Интерне́т (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

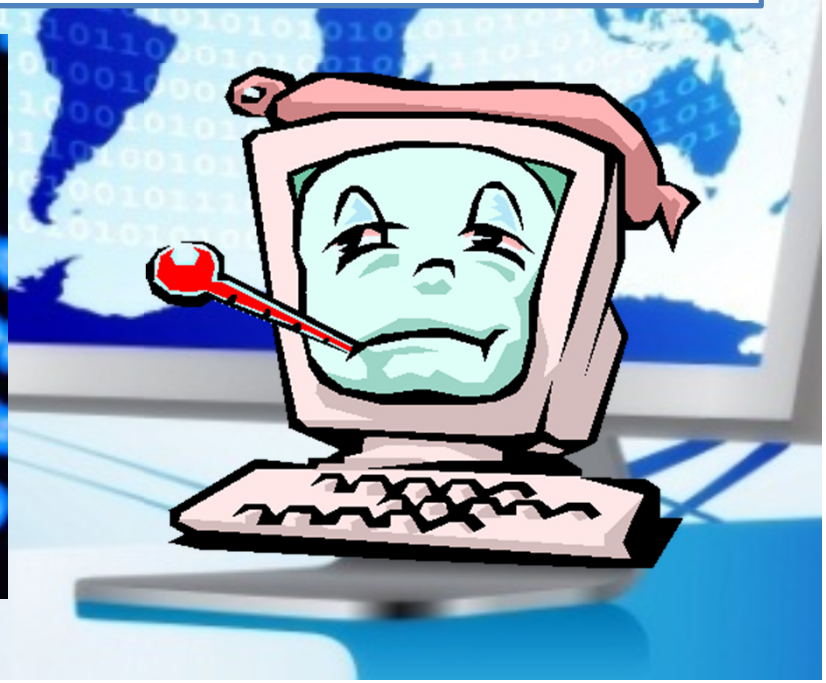
Угроза № 1. Вредоносные программы (Вирусы).

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

Сегодня вирусы пишутся с расчётом на коммерческую выгоду!

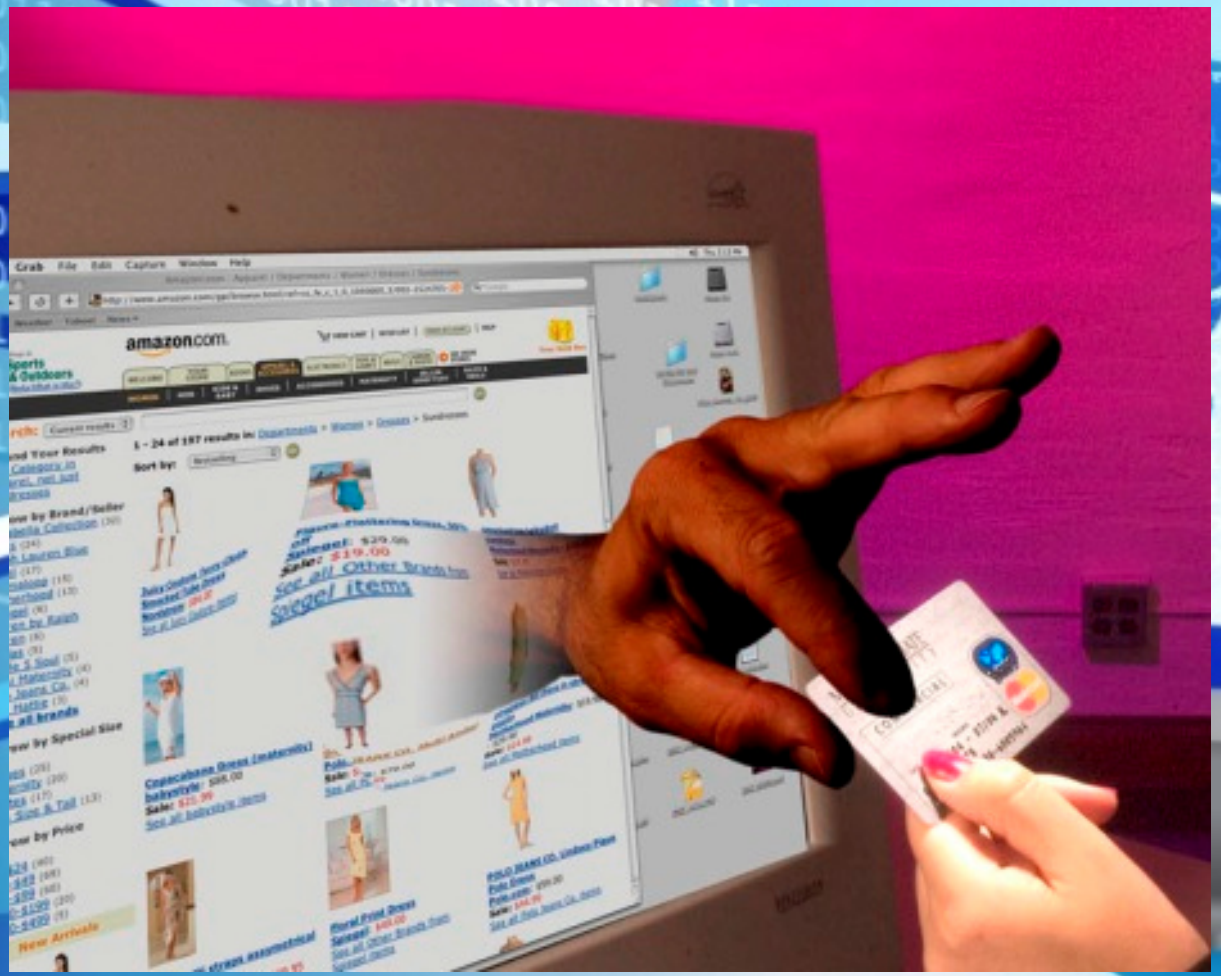
СИМПТОМЫ ЗАРАЖЕНИЯ ПК ВИРУСОМ

- 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.

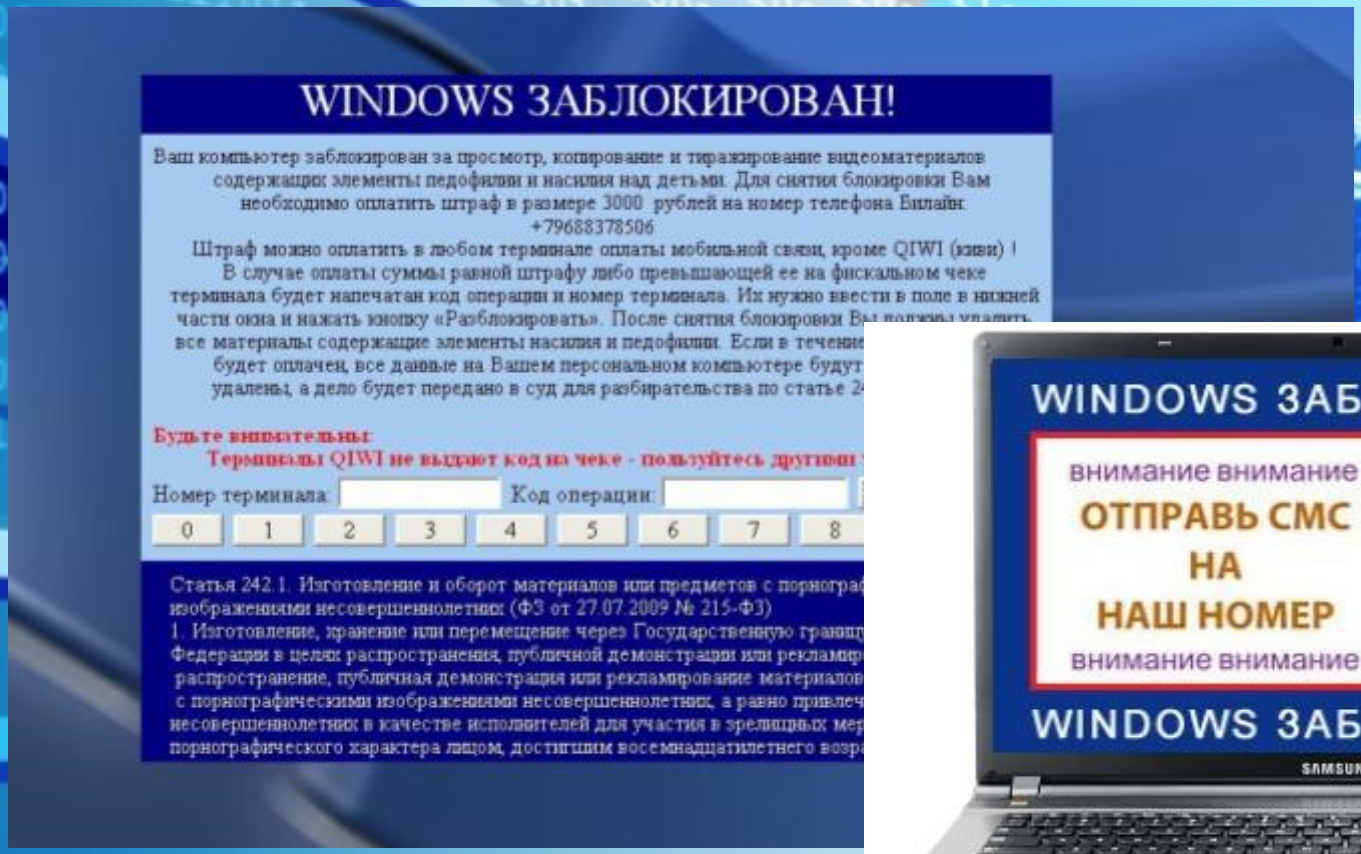
Третий приём. Предложение бесплатного программного обеспечения.
Это как правило уловки, содержащие в себе множество вирусов и троянов.

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.



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.

- 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.

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**

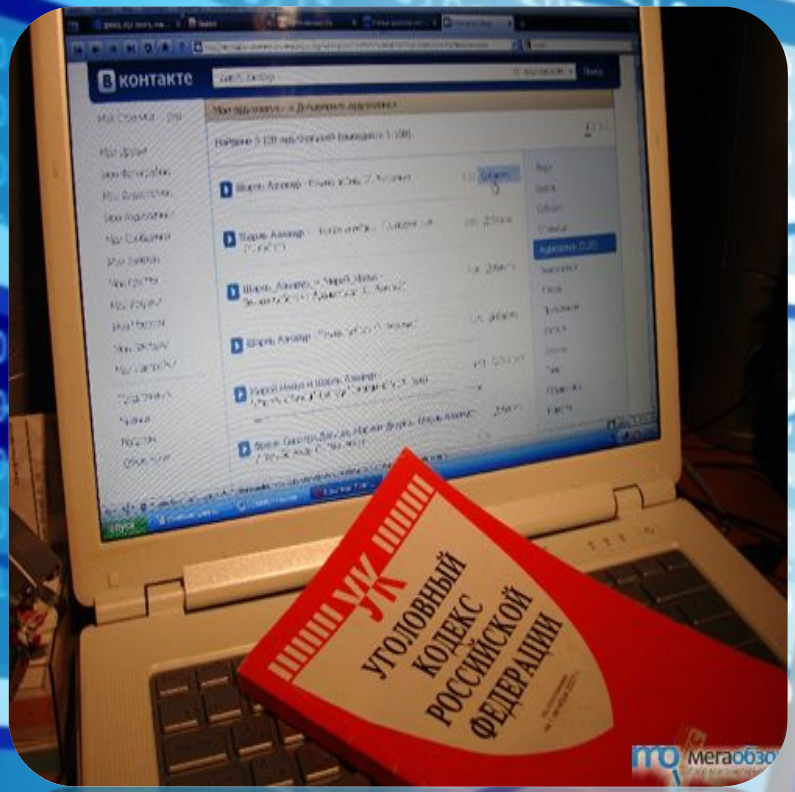
  От штрафа до 300 тысяч рублей до лишения свободы на срок до 3 лет.

- **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.


Спасибо за внимание!