Как правильно использовать интернет.

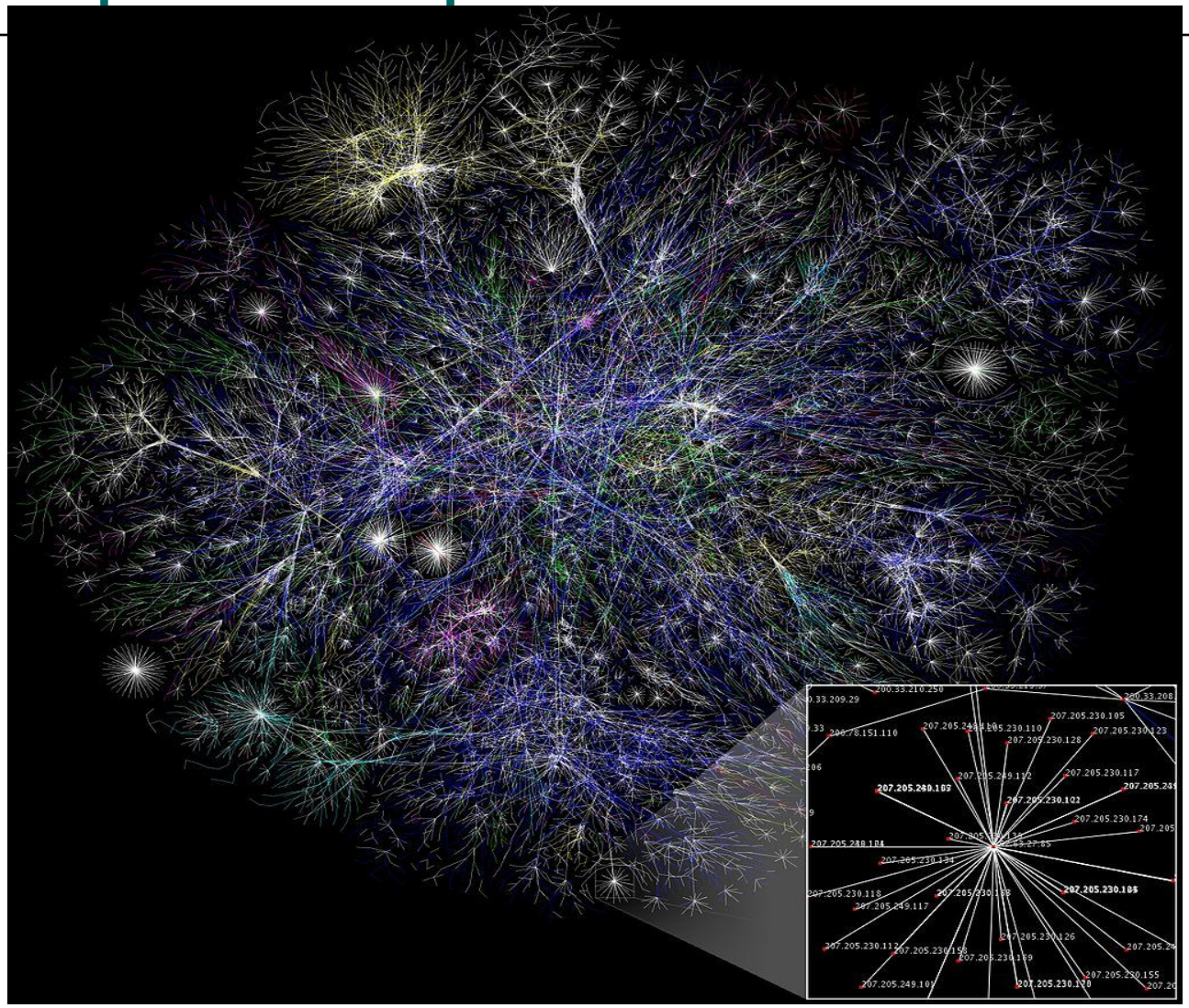
Работу выполнял: Патрушев Кирилл

"Презентация подготовлена для конкурса "Интернешка"

Что такое интернет и зачем он нужен?

- **Интерне́т** — всемирная система объединённых компьютерных сетей для хранения и передачи информации. Часто упоминается как **Всемирная сеть** и **Глобальная сеть**, а также просто **Сеть**. Построена на базе стека протоколов TCP/IP. На основе интернета работает Всемирная паутина (World Wide Web, WWW) и множество других систем передачи данных.

Карта интернета.



Безопасность в интернете

- **Вирусы** - компьютерные вирусы, сетевые и почтовые черви могут распространяться самостоятельно. Например, если вам приходит подозрительное электронное письмо с вложением – весьма высока вероятность того, что оно содержит компьютерный вирус, который может заразить некоторые файлы на вашем компьютере, испортить или украсть какие-нибудь данные. Троянские программы самостоятельно не распространяются, хотя они могут распространяться с помощью компьютерных вирусов. Их основные цели

- **Неосторожное поведение пользователя** - неосторожность пользователя – это серьезная проблема, которая ставит под удар даже самую защищенную систему, даже данные, которые расположены на отключенном от Интернета компьютере. Например, задавая слишком простой пароль для почтового ящика, вы делаете его взлом сравнительно легким, неприятны последствия случайного удаления

Функции вирусов

- 1)Кража паролей от ваших электронных кошельков, почтовых ящиков, icq, сайтов, аккаунтов в различных сервисах и т. д. К сожалению, случаи, когда открыв в один прекрасный день свой кошелёк webmoney, пользователь обнаруживает в нём ноль, не редкость, причём установить, куда и кем были переведены деньги, в таких случаях весьма затруднительно. Украв пароль от почтового ящика, вредоносная программа может от вашего имени разослать по имеющимся в вашей адресной книге адресам письма с вложенными в них троянами или вирусами и т. д.

- 2)Достаточно прибыльным "бизнесом" в наше время является организация DDoS-атак, которые могут направляться на любой сайт или сервер, даже не имеющий каких-либо существенных уязвимостей. В результате таких атак сервер перегружается запросами, идущими с многочисленных компьютеров в разных регионах мира и сайт, на который направлена атака, таким образом отключается. Многочисленные случаи DDoS-атак на различные сайты были бы невозможны, если бы в распоряжении организаторов этих атак не находилось большое количество компьютеров обычных ничего не подозревающих пользователей, заражённых троянами, которые по сигналу извне начинают все вместе посылать запросы на сервер, выбранный в качестве жертвы.

- 3)Организация массовых рекламных рассылок также является, к сожалению, прибыльным бизнесом, и для таких целей также практикуется заражение компьютеров обычных пользователей троянами.
- 4)Перечисленные цели являются наиболее типичными, но, в принципе, цели могут быть ограничены лишь фантазией автора троянов и вирусов. Троян может зашифровать, например, некоторые из имеющихся на вашем компьютере файлов и затем требовать плату за восстановление информации, заставлять ваш модем звонить на платные телефонные номера и т. д. Последние 2 года были отмечены эпидемией т. н. "блокировщиков" Windows, когда попавшие на компьютер вирусы блокировали работу компьютера и требовали отправить платную смс для его разблокировки.

Источники опасностей

1) социальная инженерия - метод основанный на психологических приёмах, который существует и эффективно используется с самого начала развития компьютерных сетей и которому не грозит исчезновение. Список уловок, придуманных хакерами в расчёте на доверчивость пользователей, огромен. Вам могут прислать письмо от имени администрации сервиса с просьбой выслать им якобы утерянный пароль или письмо, содержащее безобидный, якобы файл, в который на самом деле спрятан троян, в расчёте на то, что из любопытства вы сами его откроете и запустите вредоносную программу.
2) трояны и вирусы могут быть спрятаны в различных бесплатных, доступных для скачивания из интернета программах, которых огромное множество или на пиратских дисках, имеющихся в свободной продаже.

3) взлом вашего компьютера может быть произведён через дыры в распространённом программном обеспечении, которых, к сожалению, довольно много и всё новые уязвимости появляются регулярно. Хакеры, в отличие от большинства пользователей, не следящих за уязвимостями и часто не скачивающих устраняющие их патчи, за обнаружением новых уязвимостей следят и используют их в своих целях. Для того, чтобы компьютер, имеющий уязвимости, был заражён, достаточно, например, всего лишь зайти на определённую страничку (ссылку на эту страничку хакер может прислать в письме, оставить на форуме и т. д.).
4) в последнее время получил распространение фишинг - создание поддельных сайтов, копирующих сайты известных фирм, сервисов, банков и т. д. Заманить вас на такой поддельный сайт могут разными способами, а цель - украсть данные вашего аккаунта (т. е. логин и пароль), которые вы обычно вводите на странице настоящего сайта.

Спасибо за внимание

- Я думаю все эти знания помогут вам в пользовании интернетом. ☺