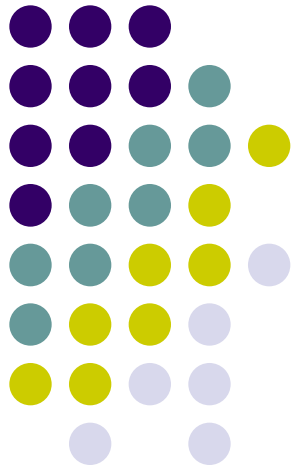
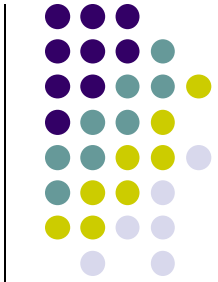
Безопасность в сети Интернет

БПОУ ВО «ВКС»
Преподаватель
Белехова Н.Н.



Цель: изучить опасные угрозы сети Интернет и методы борьбы с ними



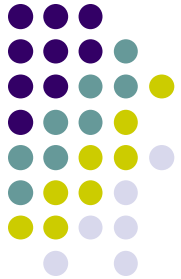
Задачи:

- Познакомиться с понятием «Интернет», «Вирус», изучить приемы безопасности при работе в сети Интернет;
- Познакомиться с ответственностью за компьютерные преступления.

Интернет -

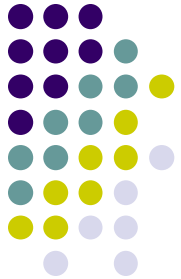
это объединенные между собой компьютерные сети, глобальная мировая система передачи информации с помощью информационно-вычислительных ресурсов

Возможности сети Интернет

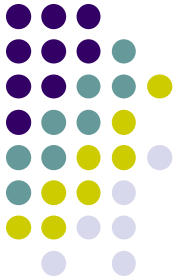


- учеба;
- поиск информации;
- перевод денежных средств;
- Интернет – заказы;
- социальные сети и многое другое.

Количество людей, пользующихся компьютером и сотовым телефоном, имеющим выход в Интернет, постоянно растет. Значит, возрастает возможность обмена данными между ними по электронной почте и через Всемирную сеть. Это приводит к росту угрозы заражения компьютера вирусами, а также порчи или хищения информации чужими вредоносными программами, ведь основными источниками распространения вредоносных программ являются электронная почта и Интернет. Правда, заражение может также произойти через дискету илиUSB-носитель.

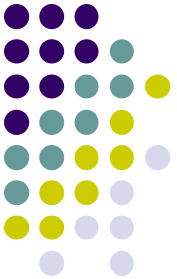


Рейтинг самых опасных угроз в сети Интернет



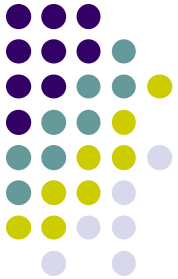
- Вредоносные программы;
- Кража информации;
- Финансовое мошенничество,
- Спам.

1. Вредоносные программы
Компьютерный вирус -



разновидность компьютерных программ или вредоносный код, отличительной особенностью которых является возможность к размножению

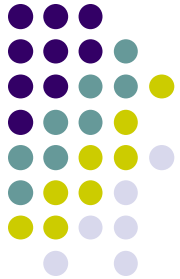
Классификация вирусов:



1. По поражаемым объектам:

- Файловые вирусы – вирусы, которые при распространении своих копий изменяют содержимое исполняемых файлов;
- Загрузочные вирусы – вирусы, записывающиеся в первый сектор жесткого диска и выполняющиеся при перезагрузке
- Скриптовые вирусы – требуют наличие одного из скриптовых языков (Javascript, VBScript)
- Макровирусы – разновидность вирусов, разработанных на макроязыках, встроенных в такие ППП, как Microsoft Office

Классификация вирусов:



2. По поражаемым ОС и платформам:

-DOS;

-Microsoft Windows;

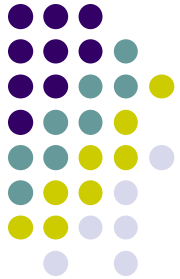
-Unix;

-Linux.

3. По технологиям, используемым вирусом

- Полиморфные вирусы(при заражении новых файлов шлифует свой собственный код)
- Стелс-вирусы(вирус, скрывающий свое присутствие, путем перехвата сообщений к ОС)
- Руткит(программа для скрытия следов преступления)

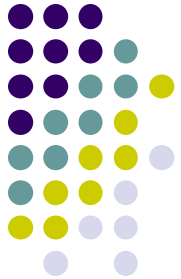
Классификация вирусов:



4. По дополнительной вредоносной функциональности:

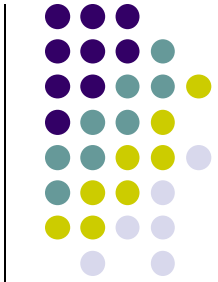
- Бэкдоры. Программы которые устанавливает взломщик на компьютере после получения первоначального доступа с целью повторного доступа
- Шпионы – собирают информацию о конфигурации компьютера
- Ботнеты – используется для нелегальной деятельность (рассылка спама)

Спам -(англ. *spam*)



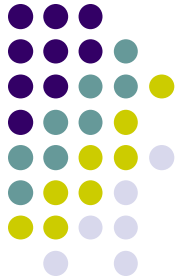
— массовая рассылка коммерческой, политической и иной рекламы или иного вида сообщений лицам, не выражавшим желания их получать. Легальность массовой рассылки некоторых видов сообщений, для которых не требуется согласие получателей, может быть закреплена в законодательстве страны. Например, это может касаться сообщений о надвигающихся стихийных бедствиях, массовой мобилизации граждан и т. п. В общепринятом значении термин «спам» в русском языке впервые стал употребляться применительно к рассылке электронных писем.

Кража информации



Кража конфиденциальной информации, это преступление, которое становится, с каждым днем, все популярней и популярней. Интерес для преступников представляет не только информация «важная и дорогая», достаточно часто происходит взлом компьютеров и кража конфиденциальной информации, которая содержится на компьютерах обычных, среднестатистических пользователей.

Финансовое мошенничество



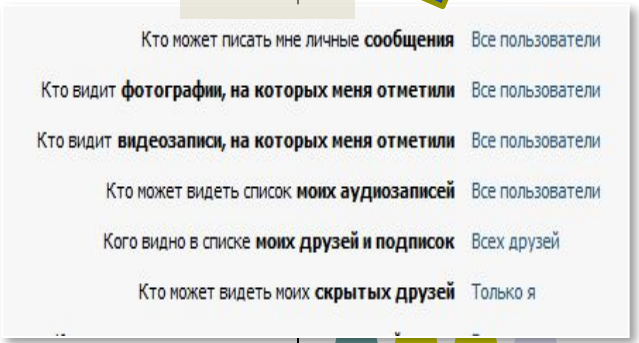
- **Мошенничества, связанные с Интернет-магазинами**
- **Фишинг** (от англ. fishing - рыбная ловля, выуживание) - вид интернет-мошенничества, цель которого - получить данные, содержащиеся на вашей пластиковой карте.
- **Интернет-попрошайничество**
- **Мошенничества в отношении иностранных граждан (брачные аферы).**

Персональные данные и личная информация в Интернете

Персональные данные – твоя частная собственность, прежде чем публиковать их и (или) передавать третьим лицам, подумай, стоит ли?

Персональные данные охраняет Федеральный Закон № 152 – ФЗ «О персональных данных»

- 80% преступников берут информацию в соц. сетях.
- Личная информация используется для кражи паролей.
- Личная информация используется для совершения таких преступлений как: шантаж, вымогательство, оскорбление, клевета, киднеппинг , хищение!



При регистрации в социальных сетях следует использовать только Имя или Псевдоним (ник)!

Настрой приватность в соц. сетях и других сервисах

Не публикуй информацию о своём местонахождении (или) материальных ценностях!

Хорошо подумай, какую информацию можно публиковать в Интернете!

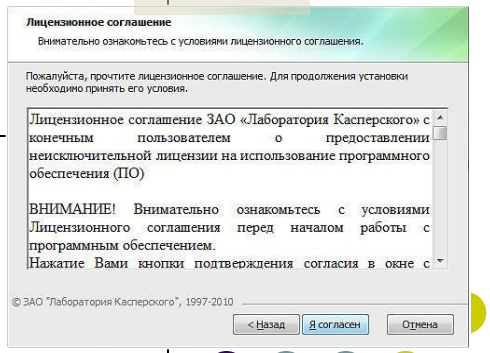
Не доверяй свои секреты незнакомцам из Интернета!

Условия использования программного продукта

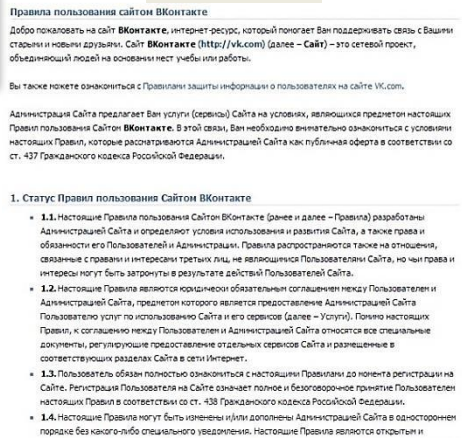
Любая услуга в Интернете имеет лицензионное соглашения и (или) условия использования. При установке программных продуктов (особенно от неизвестных производителей) следует внимательно читать тексты соглашений, ведь после принятия соглашения вся ответственность и последствия использования программного продукта ложатся на тебя!

Подтверждая соглашение «вслепую» ты можешь:

1. Оформить платные подписки/услуги;
2. Предоставить приложению/программе обширные права;
3. Лишиться персональных данных, хранящихся на электронном устройстве;
4. Стать звеном СПАМ сети;
5. Стать жертвой мошенников.



ПОМНИ: любые соглашения об использовании программных продуктов и услуг, даже от проверенного производителя, требуют внимательного изучения!



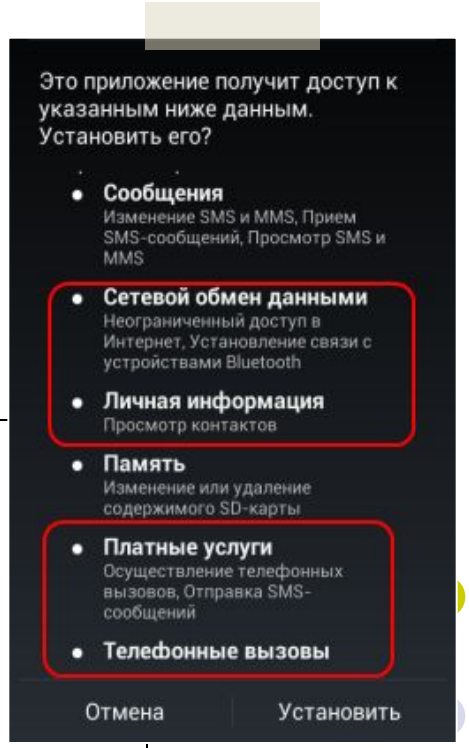
Чтобы не стать жертвой злоумышленников:

- *Использовать лицензионные продукты проверенного производителя;*
- *Внимательно знакомиться с лицензионным соглашением;*
- *Не использовать подозрительное ПО.*

Мобильные устройства/Мобильный интернет

Знай:
Современный мобильный телефон/планшет - это не просто средство связи или красивая игрушка, а полноценное коммуникационное устройство не уступающее по производительности и функционалу персональному компьютеру.

Внимание! Персональные данные!
Сегодня мобильные устройства содержат важную информацию:
- *Список контактов;*
- *Личные фотографии/видеозаписи;*
- *Данные доступа к электронной почте и иным аккаунтам в сети;*
- *Данные о банковских картах/платежах;*
- *Имеют привязку к балансу сим-карты оператора связи.*



Соблюдай простые правила использования мобильных устройств:

- *установи мобильную версию антивируса на своё мобильное устройство;*
- *установи приложения, шифрующие твои данные - они защитят личные файлы;*
- *устанавливай приложения только из проверенных источников, внимательно читай отзывы пользователей*

- *отключи функцию автоподключения к открытым Wi-Fi сетям*
- *используй только защищённые Wi-Fi сети;*
- *обязательно правильно завершай работу с публичным Wi-Fi;*

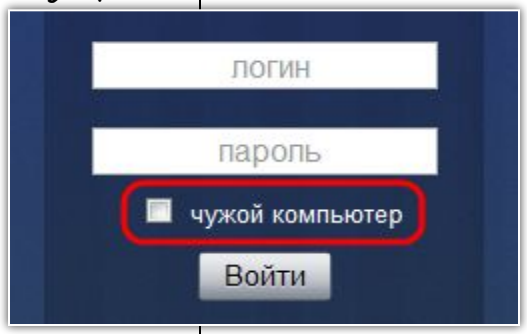
- *внимательно изучай права, запрашиваемые мобильными приложениями;*
- *используй только проверенные мобильные сервисы.*

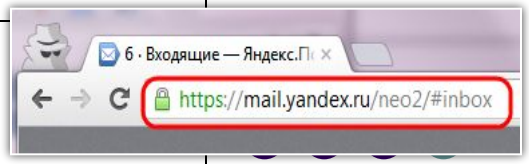
Открытые сети, чужая техника

Небрежное отношение к личной информации может привести к её утере!

ПОМНИ :

1. Будь осторожен в открытых и небезопасных сетях. Подключение к ложной сети может моментально лишить тебя всей персональной информации, хранящейся в твоем электронном устройстве: преступнику станут доступны пароли, и другая информация.
2. Опасно оставлять свои учётные данные на устройстве, которое тебе не принадлежит, этими данными могут воспользоваться в преступных целях.



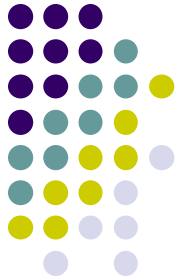


1. *При работе с публичным устройством используй пункт «чужой компьютер».*
2. *Используй режим «приватного просмотра» в браузере.*
3. *Всегда используй кнопку «выйти» при завершении работы с ресурсом.*
4. *Отказывайся от сохранения пароля при работе на «чужом компьютере».*

1. *Используй безопасное соединение с почтой и сервисами (безопасное соединение обозначено замком с зелёным текстом).*
2. *Не оставляй без присмотра устройства доступа в сеть (телефон, планшет, ноутбук).*

1. *Используй шифрованные хранилища данных, которые помогут защитить твои личные файлы.*
2. *Используй сложные пароли, состоящие из прописных и заглавных латинских букв и цифр, а также символов.*
3. *Используй только открытые сети в надежности которых ты уверен.*

Ответственность за компьютерные преступления



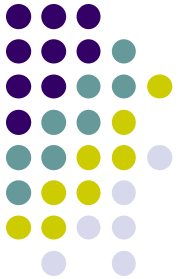
Каждый день появляются все новые и новые вирусы. Создание и распространение вредоносных программ (в том числе вирусов) преследуется в России согласно УК РФ (глава 28, статья 273)

Как ВИРТУАЛЬНАЯ сеть может влиять на РЕАЛЬНУЮ жизнь

ПОМНИ: за ВИРТУАЛЬНЫЕ преступления отвечают по РЕАЛЬНОМУ закону

- ст. 272 УК РФ - Неправомерный доступ к компьютерной информации (до 5 лет лишения свободы);
- ст. 273 УК РФ – Создание, использование и распространение вредоносных программ для ЭВМ (5 лет лишения свободы);
- ст. 274 УК РФ – Нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (до 5 лет лишения свободы);
- ст. 129 – Клевета (до 5 лет лишения свободы);
- ст. 130 – Оскорбление (до 3 лет лишения свободы);
- ст. 159 – Мошенничество (до 10 лет лишения свободы);
- ст. 165 – Причинение имущественного ущерба путем обмана или злоупотребления доверием (до 5 лет лишения свободы);
- ст. 146 – Нарушение авторских и смежных прав (до 10 лет лишения свободы);

Обязательные элементы информационной безопасности



1. Установка комплексной системы защиты
2. Пользуйтесь браузерами Mozilla Firefox, Google Chrome, Apple Safari.
3. Обновляйте ОС Windows.
4. Не отправляйте SMS-сообщения неизвестным пользователям
5. Пользуйтесь лицензионным ПО
6. Используйте сложные пароли
7. Делайте резервные копии файлов