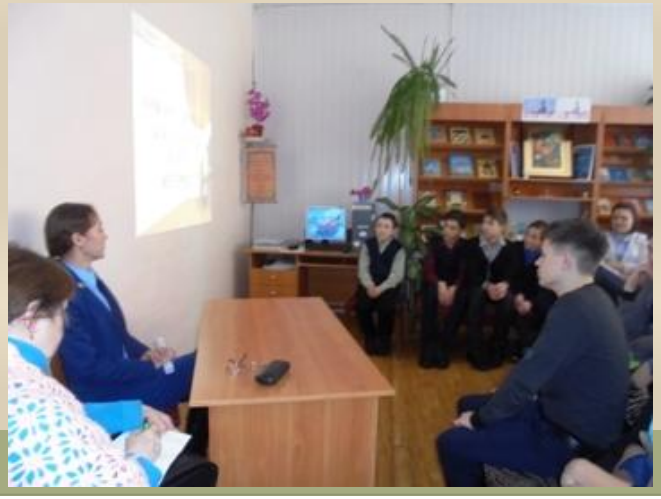
ПРАВОВОЙ ОНЛАЙН-ЛЕКТОРИЙ

Как вести себя в Интернете?

Безопасность в интернете – очень важная проблема нынешнего времени. И касается она всех, от детей до пенсионеров. Она становится все актуальнее в связи с массовым приходом в Интернет пользователей, почти, а то и совсем, не подготовленных к угрозам, их поджидающим.



Создание сети Интернет создавалась поэтапно. Проектирование и разработку сети возложили на четыре крупнейших научных заведения. Это Университеты штата Калифорния в Санта-Барбаре и Лос-Анджелесе, университет Юты и Стэндфордский исследовательский центр. В 1969 году их объединили между собой в сеть, которую назвали ARPANET (Арпанет). Тогда был проведен первый сеанс связи.

1971 г.	ЭЛЕКТРОННАЯ ПОЧТА
1973 г.	МЕЖДУНАРОДНАЯ СЕТЬ
1989 г.	КОНЦЕПЦИЯ ВСЕМИРНОЙ ПАУТИНЫ
1990 г.	ПЕРВЫЙ ДОМЕН (.SU)
1991 г.	ВСЕМИРНАЯ ПАУТИНА ДОСТУПНА В ИНТЕРНЕТЕ
1993 г.	ПЕРВЫЙ БРАУЗЕР
2010 г.	ИНТЕРНЕТ НА МКС
2011 г.	ООН: ИНТЕРНЕТ – БАЗОВОЕ ПРАВО ЧЕЛОВЕКА

Применительно к Интернету мы применяем слово «компетенция».

Компетенция –
способность решать задачи в определенной области.

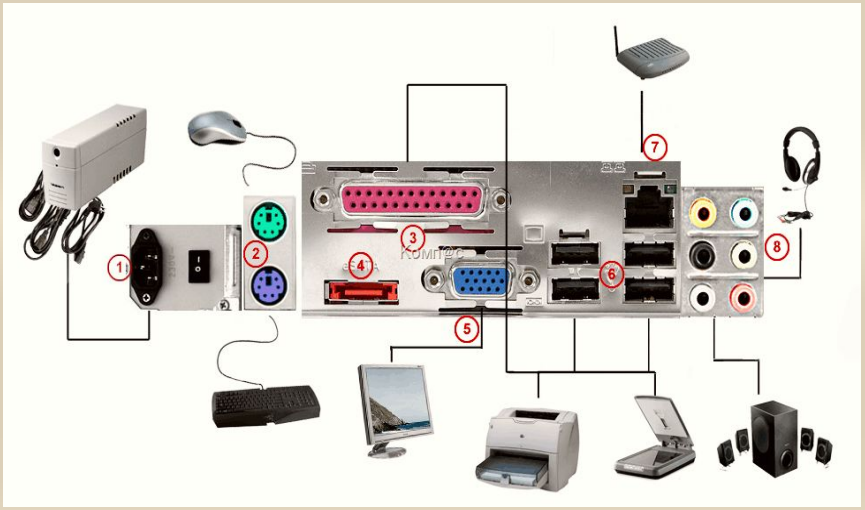
- ***ТЕХНИЧЕСКАЯ***
- ***ИНФОРМАЦИОННАЯ***
- ***КОММУНИКАТИВНАЯ***
- ***ПОТРЕБИТЕЛЬСКАЯ***

ИНТЕРНЕТ

ТЕХНИЧЕСКАЯ КОМПЕТЕНЦИЯ – способность использовать для работы в Интернете технические устройства и программы, базовое представление о каналах связи и рисках в этой области.

ПРАВИЛА БЕЗОПАСНОСТИ И ЭКСПЛУАТАЦИИ

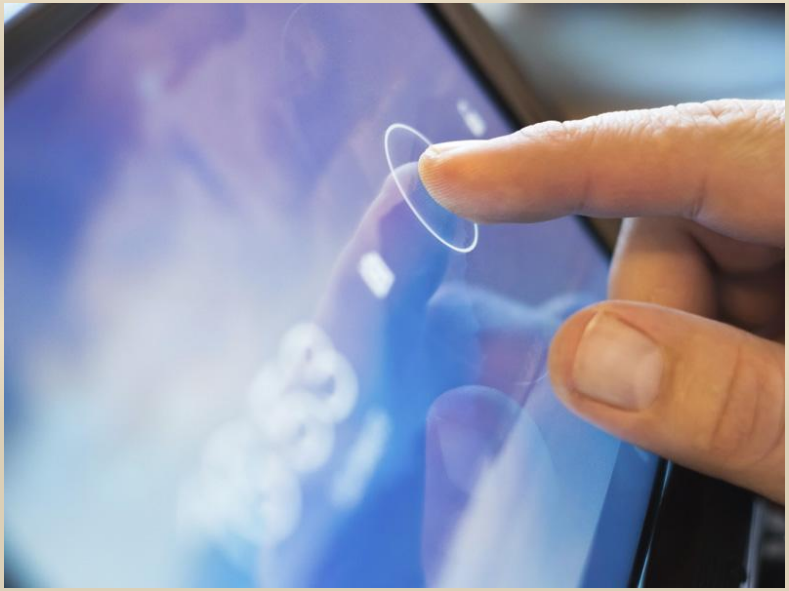
ПРАВИЛЬНО ПОДКЛЮЧАЙ УСТРОЙСТВА



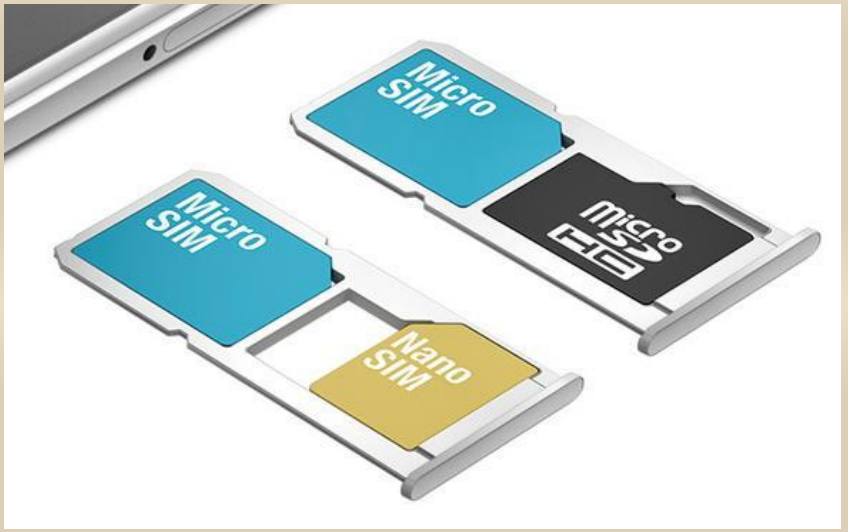
СВОЕВРЕМЕННО ЗАРЯЖАЙ АККУМУЛЯТОРЫ

ПРАВИЛА БЕЗОПАСНОСТИ И ЭКСПЛУАТАЦИИ

УЧИТЫВАЙ УСЛОВИЯ ЭКСПЛУАТАЦИИ



СЛЕДИ ЗА СОХРАННОСТЬЮ УСТРОЙСТВ



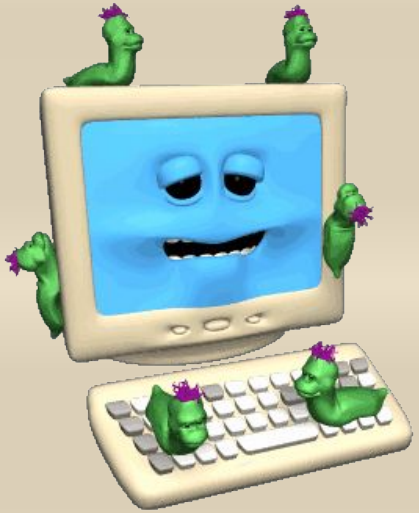
ПРОГРАММЫ

В программах нужно уметь работать. Большинство программ имеют удобный интерфейс. Очень часто бывает так, что наши программы содержат в себе ошибки, которые не влияют на работоспособность устройства и вы их даже не замечаете. Но они дают возможность злоумышленникам и хакерам воспользоваться ими в корыстных целях. Они создают программные вирусы, которые попадают на ваш компьютер (могут попасть) через эти дырки и ошибки программного кода. И это дает им возможность украсть важную для вас информацию: пароли, контакты, реквизиты банковских карт, писать за вас сообщения в социальных сетях.

УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ
(в ред. Федерального закона от 07.12.2011 N 420-ФЗ)

1. СОЗДАНИЕ, РАСПРОСТРАНЕНИЕ ИЛИ ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНЫХ ПРОГРАММЛИБО ИНОЙ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ, ЗАВЕДОМО ПРЕДНАЗНАЧЕННЫХДЛЯ НЕСАНКЦИОНИРОВАННОГО УНИЧТОЖЕНИЯ, БЛОКИРОВАНИЯ, МОДИФИКАЦИИ, КОПИРОВАНИЯ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ИЛИ НЕЙТРАЛИЗАЦИИ СРЕДСТВ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

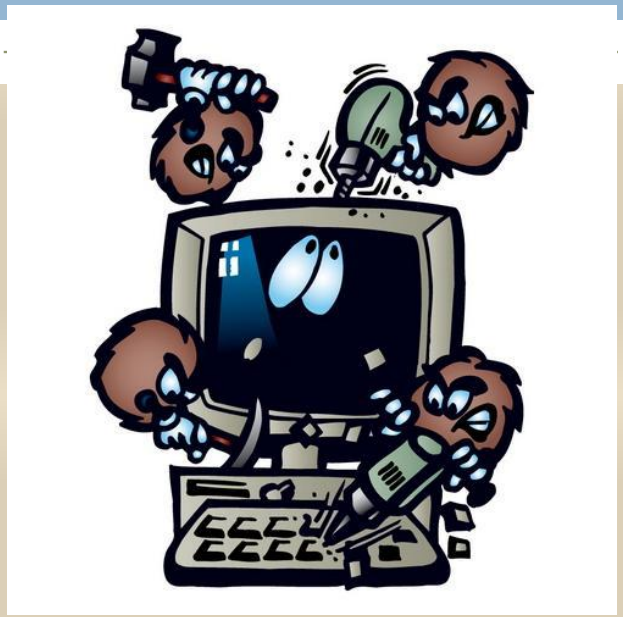
ВРЕДОНОСНЫЕ ПРОГРАММЫ



вирусы

сетевые черви

ВРЕДОНОСНЫЕ ПРОГРАММЫ



руткиты

шпионские программы

ВРЕДОНОСНЫЕ ПРОГРАММЫ МОГУТ:

- Похищают логины, пароли, данные банковских карт
- Рассылают спам
- Делают скрытые скриншоты
- Рассылают сообщения и звонки на платные номера
- Отправляют данные злоумышленникам
- Включают удаленное управление компьютером

ГЛАВНЫЕ ИСТОЧНИКИ ВИРУСОВ:

- Непроверенные ссылки
- скачивание файлов с непроверенных ресурсов
- программы непроверенного разработчика
- сомнительные и зараженные сайты
- опасные баннеры
- зараженные файлы
- нарушение правил работы на компьютере

Признаки заражения компьютера:

Вывод на экран странных сообщений и изображений

произвольный запуск каких-либо программ

подача странных звуковых сигналов

неожиданная перезагрузка и завершение программ

неожиданное открытие и закрытие лотка дисковода

повышенная нагрузка и «зависание» устройства

КАК ИЗБЕЖАТЬ ЗАРАЖЕНИЯ КОМПЬЮТЕРА

Использовать современные операционные системы

Использовать антивирус с обновлениями

Ограничить физический доступ к своему компьютеру

Своевременно обновлять программы

Работать под учетной записью

Проверенные внешние носители

Не открывать файлы из ненадежных источников

Для профессиональной борьбы с вирусами созданы, так называемые **антивирусники.** Эти программы в режиме реального времени оценивают все файлы, которые расположены на вашем компьютере, ищут спрятанные там вирусы. Они имеют обширные базы, энциклопедии, в которых подробно описаны все в мире антивирусные программы. Поэтому регулярное обновление антивирусников очень важно. Антивирусник может просто не узнать, что на ваш компьютер установились новые вирусы.

Wi-Fi – это не интернет как таковой, а современный стандарт обмена данными между устройствами, оснащенными специальными радиомодулями.

.

Сегодня сети Вай-фай особо популярны. Многие торговые точки устанавливают бесплатный точки доступа для привлечения своих клиентов. Это, конечно, нам очень нравится. Но нельзя забывать и об осторожности.


СВОБОДНЫЙ
Wi-Fi
ДОСТУП

Основные правила использования Wi-Fi в общественных местах

- ДЛЯ НАЧАЛА НУЖНО УДОСТОВЕРИТЬСЯ, ЧТО ВЫ ПОДКЛЮЧАЕТЕСЬ К ОФИЦИАЛЬНОЙ СЕТИ WI-FI ЗАВЕДЕНИЯ, В КОТОРОМ ВЫ НАХОДИТЕСЬ. ОБЫЧНО ТАКИЕ СЕТИ ИМЕЮТ ПАРОЛЬ ИЛИ ТРЕБУЮТ МИНИМАЛЬНУЮ АВТОРИЗАЦИЮ;

- ПРОВЕРИТЬ ПОЧТУ ИЛИ ОСТАВИТЬ КОММЕНТАРИЙ НА ФОРУМЕ МОЖНО, НО ТОЛЬКО ЕСЛИ ВЫ УВЕРЕНЫ В БЕЗОПАСНОСТИ ПОДКЛЮЧЕНИЯ;

- НЕ ПРОВОДИТЕ ЧЕРЕЗ ПУБЛИЧНУЮ СЕТЬ НИКАКИХ ФИНАНСОВЫХ ОПЕРАЦИЙ НА САЙТАХ ИЛИ ПРИЛОЖЕНИЯХ.

МЕРЫ БЕЗОПАСНОСТИ В СЕТИ WI-FI В ОБЩЕСТВЕННЫХ МЕСТАХ

Не передавай свою личную информацию через общедоступную сеть

Обращай внимание на значок безопасного соединения

Отключи функцию «Общий доступ к файлам и принтерам»

В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически»

В домашней сети Wi-Fi используй надежные пароли и отключи ненужные функции сети

.

СОЦИАЛЬНЫЕ СЕТИ

ЧТОБЫ ОБЕЗОПАСИТЬ СЕБЯ В СОЦИАЛЬНЫХ СЕТЯХ, НЕОБХОДИМО:

- УКАЗЫВАЙТЕ МЕНЬШЕ ЛИЧНОЙ ИНФОРМАЦИИ;
- НЕ УКАЗЫВАТЬ МЕСТА, ГДЕ ВЫ БЫЛИ, ПРИ ПОМОЩИ ГЕОЛОКАЦИИ;
- НЕ СТОИТ АФИШИРОВАТЬ СВОЕ ФИНАНСОВОЕ СОСТОЯНИЕ;
- НЕ УКАЗЫВАЙТЕ НОМЕР СВОЕЙ БАНКОВСКОЙ КАРТЫ;
- НЕ КАЖДЫЙ ВЛОЖЕННЫЙ ФАЙЛ В СООБЩЕНИИ СЛЕДУЕТ ОТКРЫВАТЬ;
- КОНФИДЕНЦИАЛЬНОСТЬ.