*ТЕХНИЧЕСКИЕ РИСКИ В ИНТЕРНЕТЕ

- Создание паролей
- Вирусы в интернете
- Искусственный интеллект

*РИСКИ в ИНТЕРНЕТЕ

Алгоритм 1 создания сложных паролей:
Выбираем любое прилагательное. Например «отмороженный»
Выбираем любое существительное, логически не сочетающееся «камень»
Любую легко запоминающуюся цифру (г.р., последние цифры тел. и т.п.)
Любой знак препинания !
Запишем все без пробелов «отмороженныйкамень1998!»
Поменяем одну букву на прописную «отмороженныйКамень1998!»

Алгоритм 2
Для лучшего запоминания сделать начало, конец или середину всех паролей одинаковым «рп0!мИ»
К этим символам добавьте части, ассоциирующиеся с сервисами: рп0! мИcontact

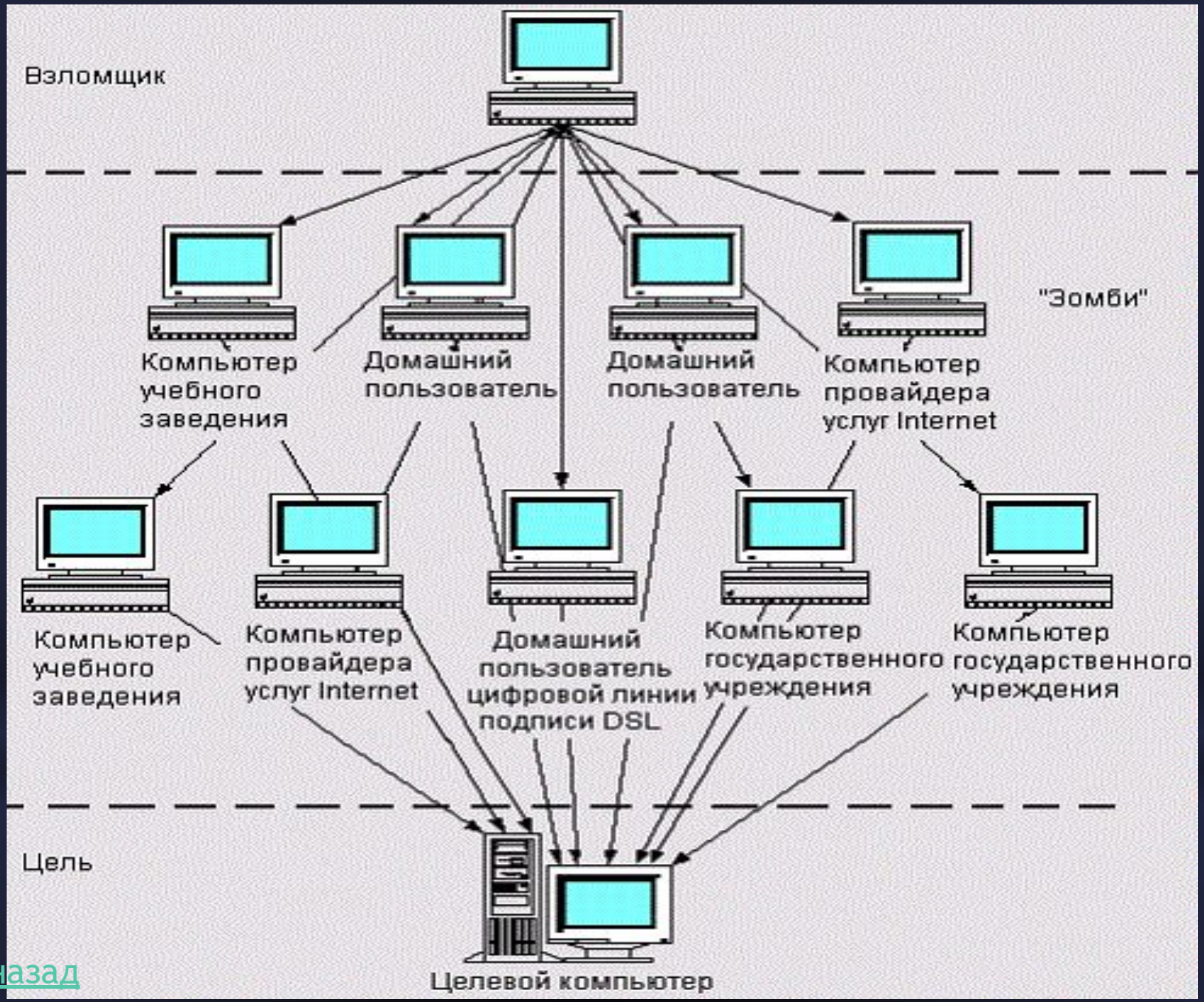
Алгоритм 3
Использовать только вам известное словосочетание «Моя мама готовит вкусные булочки по 12 штук». Взять первую букву каждого слова «Ммгвбп12ш».

*Надежные пароли

На большинстве персональных компьютеров нет никаких данных, используя которые злоумышленник может заработать деньги или нанести пользователю ущерб.

1. Если вы пользуетесь системами оплаты через Инет, то воспользовавшись вашим логином или паролем, злоумышленник украдет ваши деньги.
2. Злоумышленник может получать деньги за рассылку спама, организовать с вашего компьютера DDOS-атаку . Вы оплачиваете лишний траффик, миритесь с медленной работой компьютера, возможно общение со службой безопасности атакованной организации.
3. С вашего компьютера может распространяться вирус на компьютеры ваших знакомых, среди которых найдется тот, на ком можно заработать.

*Надежные пароли


Взломщик
"Зомби"
Компьютер учебного заведения
Домашний пользователь
Домашний пользователь
Компьютер провайдера услуг Internet
Компьютер учебного заведения
Компьютер провайдера услуг Internet
Домашний пользователь цифровой линии подписи DSL
Компьютер государственного учреждения
Компьютер государственного учреждения
Цель
Целевой компьютер

назад

Если на компьютер попадает вредоносная программа, то компьютер ломается.

Если просто просматривать веб-страницы и ничего не скачивать, невозможно поймать «вредоносную» программу. *Есть два способа заражения при просмотре страниц: уязвимость браузеров и через активные элементы страниц. Следует не только обновлять регулярно браузеры, но и ограничивать выполнение различных активных элементов (ActiveX, Java applet, VBS/Java script) при просмотре документов с ненадежных сайтов.*

Невозможно поймать вредоносную программу на сайтах крупных и уважаемых компаний «Яндекс», «Википедия» и т.п.

Если установить антивирус и регулярно его обновлять, ни один вирус компьютеру не страшен. *Любые обновления выходят ПОСЛЕ первых заражений новыми вирусами.*

*

Каждый день появляется около 200000 новых версий вредоносных программ: вирусов, троянов, червей и т.п. Наиболее часто встречаются:

Поддельная угроза вирусной атаки – всплывающие окна (иногда с характерным звуком) типа «Ваш компьютер заражен! Скачайте антивирус!» «Ваш аккаунт «В контакте» взломали!» и т.п. В панике пользователь кликает на ссылку, что приводит к мгновенному заражению, либо краже пароля.

Вредоносные ссылки - ссылки, рассылаемые с взломанных компьютеров друзей с призывом пройти по ним «Посмотри как ты получился на фото!», «Проголосуй за меня!», дальне как выше)))

Взлом легальных сайтов – установка вредоносных программ в невидимом режиме на легально посещаемых сайтах злоумышленниками.

*ВИРУСЫ

Избежать неприятностей помогает КОМПЛЕКС технических программ защиты, которые мы привыкли называть **АНТИВИРУСОМ.** Такая защита обновляется в режиме реального времени. Это лишь часть комплексного решения информационной безопасности. Его составляющие можно разделить на пять основных групп:

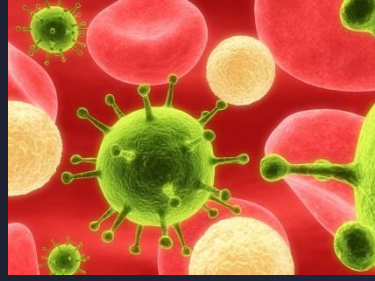
Классический антивирус – компьютерная программа, целью которой является обновить, предотвратить размножение и удалить вирусы и др. вредоносное ПО. Некоторые препятствуют несанкционированному проникновению на устройство.

Антишпион – для обнаружения и удаления spyware. Сейчас имеют дополнительные функции, позволяющие удалять агрессивную рекламу (add-ware).

Онлайн-сканер – обнаружение и удаление вирусов из файловой системы ПК, подключенного к Инету. Нет необходимости установки приложения, но обнаруживает только то, что уже проникло.

Сетевой экран – безопасность в локальных сетях и Инете. Контролирует и фильтрует сетевой трафик, защищает от несанкционированного доступа

*Антивирусы



- Регулярно обновляйте браузер и ОС.
- Внимательно смотрите за тем, какие веб-сайты вы посещаете
- Остерегайтесь всплывающих окон, которые вам предлагают установить ПО или устранить неполадки
- Добавляйте нужные сайты в закладки.
- Устанавливайте ПО только из надежных источников
- Обнаружив после загрузки любые подозрительные признаки(медленная работа ПК, всплывающие окна и т.п.) удалите ПО и проверьтесь антивирусом
- Сканировать ПК лучше с помощью нескольких антивирусов

*Защита от вирусов

Captcha – искаженное изображение с набором символов. Цель – предотвратить атаки автоматических систем на сайт.

http://www.youtube.com/watch?v=QvOlgob5njQ

*CAPTCHA