Защита собственной информации от несанкционированного доступа

Презентация подготовлена
для конкурса "Интернешка
http://interneshka.org/

Что такое «несанкционированный доступ»?

Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети, сопровождающийся нарушением системы защиты ,влекущий к изменению, уничтожению, блокированию информации или вывод из строя компьютерного оборудования (проще говоря - ***взлом*** компьютера, личных данных в сети)

Источники угроз информационной безопасности

Человеческий фактор

- Внешние угрозы (действия хакеров, мошенников)
- Внутренние угрозы (действия пользователей ПК)

Технический фактор

- Некачественное оборудование
- Сбои внешних носителей, ПО

Стихийный фактор

- Стихийные бедствия
- Природные катаклизмы

Виды угроз информационной безопасности

Виды угроз информационной безопасности

Очень часто мошенниками используются именно эти типы вредоносных программ:

1.Червь использует уязвимости операционной системы и программ для распространения на другие компьютеры. Он использует сети, электронную почту и т.д., вследствие чего обладает высокой скоростью распространения.

2.Вирусы проникают в программы и изменяют их исходный код, добавляя свой, чтобы получить управление при запуске данной программы.

3.Трояны способны удалять файлы, воровать личную информацию и т.д. Их действия способны привести к зависанию компьютера.

Виды угроз информационной безопасности

4.Баннерная реклама

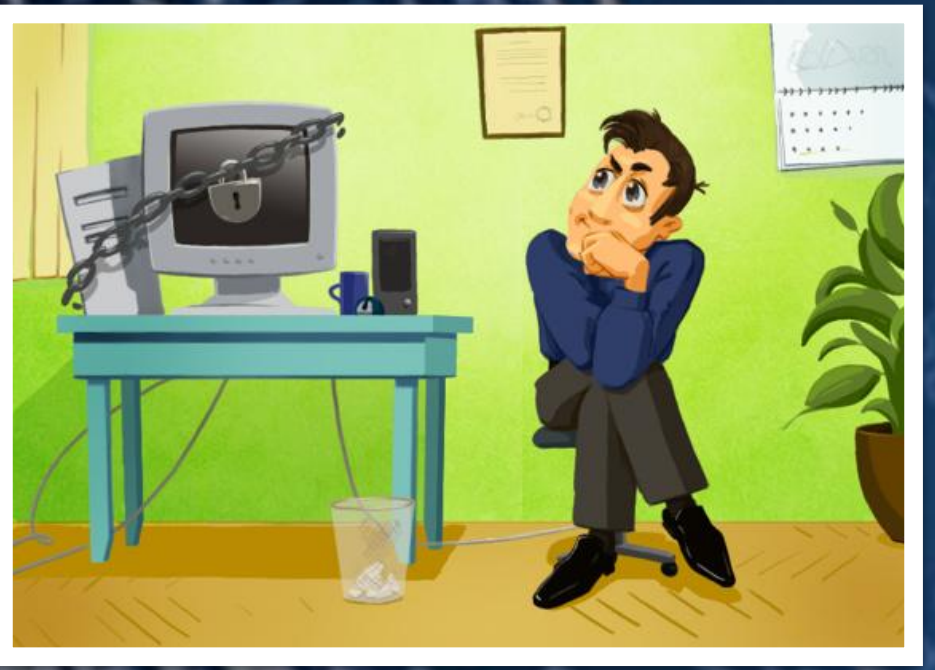
1. Баннерная реклама, которая появляется в браузере при пользовании интернетом или распространяется встроенной в ПО. Данный баннер использует огромное количество трафика.

2. Баннерная реклама, которая встраивается в операционную систему и при запуске пользователь видит баннер с требованием заплатить деньги, чтобы разблокировать баннер.

Все эти баннеры собирают информацию о пользователе и передают ее своему разработчику.

Виды угроз информационной безопасности

6.Программы-шпионы собирают всю информацию о пользователе. Обычно целью программ-шпионов является отслеживание действий пользователя на компьютере, программного обеспечения установленного на компьютере, способе подключения к интернету и т.д.



7.Потенциально опасные приложения - это программы, которые содержат бреши и ошибки в безопасности. Злоумышленники способны воспользоваться этими ошибками и проникнуть на ваш компьютер с целью получить вашу индивидуальную информацию.

Виды угроз информационной безопасности

8.**Программы-шутки**. Их использовали не только хакеры, но и обычные пользователи ради забавы. Однако и эти программы-шутки представляют опасность в руках хакера.
Например, программа-шутка, которая сообщает о форматировании диска, хотя никакого форматирования не будет.

9.Программы-маскировщики мешают антивирусным программам определять вредоносные программы. Также эти программы изменяют операционную систему, чтобы скрыть свое собственное присутствие.
К прочим опасным программам относятся программы взлома паролей, конструкторы вирусов, программы взлома сетевых ресурсов и т.д.

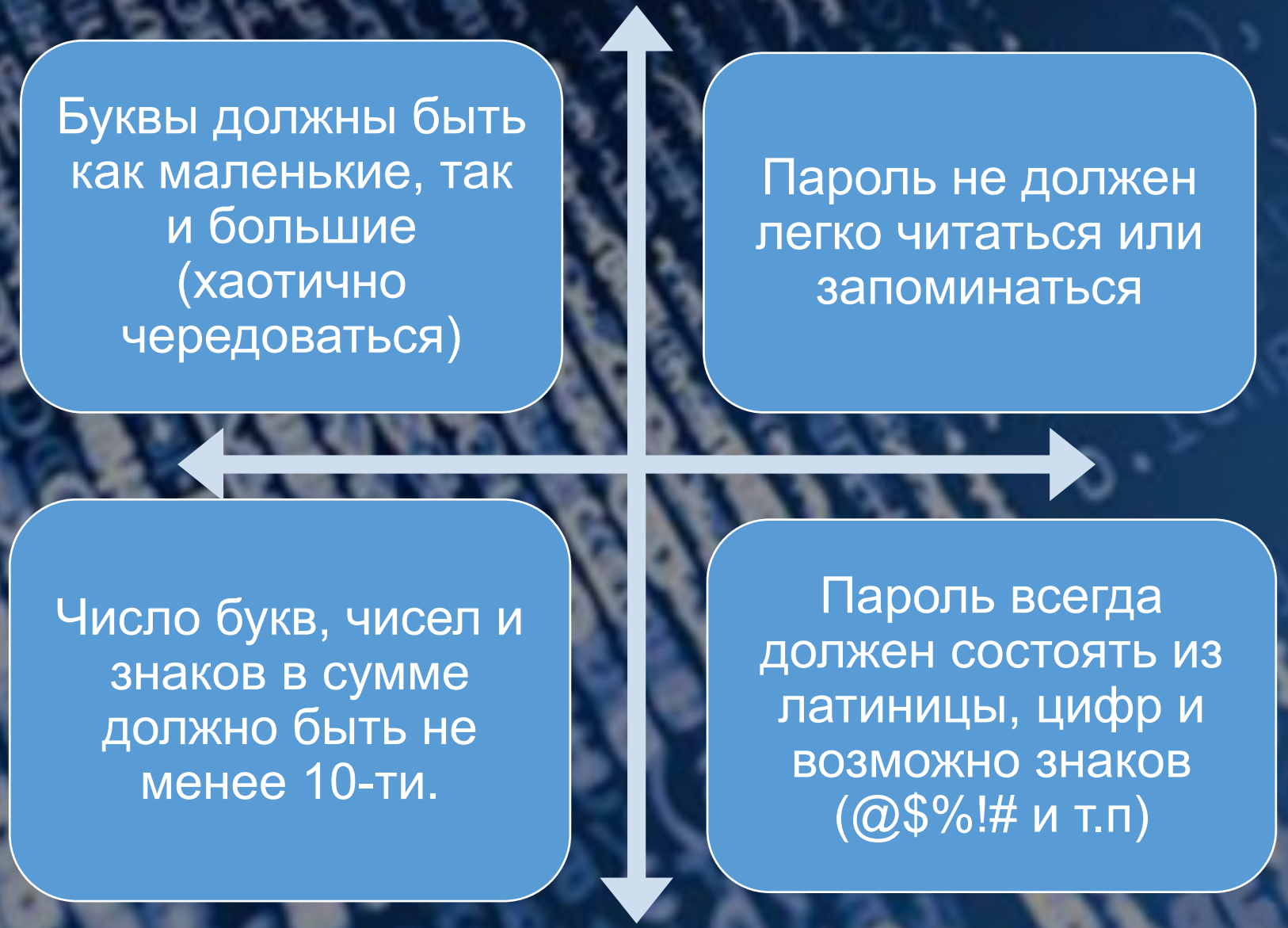
Как избежать несанкционированного доступа?

1.Запускайте программы с правами администратора, только в самых крайних случаях и только тогда, когда вы полностью доверяете программе. Такая программа может без опознавательных знаков загрузить на ваш компьютер вирус и интегрировать его таким образом, что даже самый лучший антивирус не сможет его опознать

2.Скачивайте и устанавливайте все самые свежие обновления для программ, особенно это касается обновлений антивируса и операционной системы.

Как избежать несанкционированного доступа?

3.Приучите себя к сложным паролям. Старайтесь иметь для каждой программы и учетной записи свой уникальный и тяжелый пароль.



Как избежать несанкционированного доступа?

4.Используйте файрвол (или как его ещё называют Брандмауэр) – это основная защита компьютера, которая должна быть включена при активном подключении к сети Интернет. Файрвол позволяет фильтровать подключения к вашему компьютеру, которые исходят из всемирной паутины.

5.При выборе антивируса, отдавайте предпочтение платным антивирусным программам.

6.Большую опасность представляет и ваша невнимательность, поэтому, когда программы Вас о чем-либо спрашивают, читайте эти всплывающие сообщения очень внимательно и принимайте взвешенное решение.

Как избежать несанкционированного доступа?

6.Большую опасность представляет и ваша невнимательность, поэтому, когда программы Вас о чем-либо спрашивают, читайте эти всплывающие сообщения очень внимательно и принимайте взвешенное решение.

А также:

Чтобы было меньше всплывающих окон, включайте защиту от рекламных баннеров в антивирусе;

Сразу же закрывайте сайты или программы, на которые «жалуется» антивирусная программа, браузер или файрвол.

Вывод:

Если следовать вышеизложенным правилам, то вы будете в безопасности и сможете избежать многих проблем.

Ряполова Елена
Самарская область,
г. Жигулёвск,
ГБОУ СОШ№10