

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ РЕСПУБЛИКИ АДЫГЕЯ МАЙКОПСКИЙ МЕДИЦИНСКИЙ  
КОЛЛЕДЖ

ПРОЕКТНАЯ РАБОТА ПО  
ИНФОРМАТИКЕ НА ТЕМУ  
"КОМПЬЮТЕРНЫЕ ВИРУСЫ И  
СРЕДСТВА БОРЬБЫ С НИМИ".

Выполнила студентка группы Ф-14 Прошина Дарья.

Руководитель исследовательской работы Хагуп Юлия Заурбиевна.

# СОДЕРЖАНИЕ:

1. ВВЕДЕНИЕ.
2. ТЕРМИН И ПРОИСХОЖДЕНИЕ КОМПЬЮТЕРНОГО ВИРУСА.
3. ОСНОВНЫЕ ИСТОЧНИКИ КОМПЬЮТЕРНЫХ ВИРУСОВ.
4. ПЕРВЫЕ ПРИЗНАКИ ЗАРАЖЕНИЯ КОМПЬЮТЕРНЫМ ВИРУСОМ.
5. КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ.
6. КОМПЬЮТЕРНЫЕ ЧЕРВИ.
7. СРЕДСТВА БОРЬБЫ С КОМПЬЮТЕРНЫМИ ВИРУСАМИ.
8. КРАТКОЕ ОПИСАНИЕ САМЫХ ИЗВЕСТНЫХ АНТИВИРУСОВ.

# ВВЕДЕНИЕ.

1. **Цель:** ИЗУЧИТЬ ВСЕ ИЗВЕСТНЫЕ ВРЕДНОСНЫЕ КОМПЬЮТЕРНЫЕ ПРОГРАММЫ; УЗНАТЬ О СРЕДСТВАХ БОРЬБЫ С ВРЕДНОСНЫМИ ПРОГРАММАМИ, ИЗУЧИТЬ ДОСТОИНСТВА И НЕДОСТАТКИ АНТИВИРУСНЫХ ПРОГРАММ, О САМЫХ ЗНАЧАЩИХ ЛИЦАХ В ИСТОРИИ КОМПЬЮТЕРНОГО ПРОГРАММИРОВАНИЯ ВИРУСОВ ИЛИ АНТИВИРУСОВ.
2. **Задачи:**
  - СОБРАТЬ НЕОБХОДИМУЮ ДЛЯ РАБОТЫ ИНФОРМАЦИЮ.
  - ПРОВЕСТИ СОЦИАЛЬНЫЙ ОПРОС, ОБРАБОТАТЬ РЕЗУЛЬТАТ.
  - ГРАМОТНО ЗАЩИТИТЬ РАБОТУ, ОТВЕТИТЬ НА ВОЗНИКШИЕ ВОПРОСЫ.

# ТАК ЧТО ЖЕ ТАКОЕ КОМПЬЮТЕРНЫЙ ВИРУС?

Компьютерный вирус – вид вредоносного программного обеспечения, способный создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а так же распространять свои копии по разнообразным каналам связи, с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей или же приведение в негодность аппаратных комплексов компьютера.

# ИСТОРИЯ СОЗДАНИЯ КОМПЬЮТЕРНОГО ВИРУСА.

Существует много разных версий относительно даты рождения первого компьютерного вируса. Однако большинство специалистов сходятся на мысли, что компьютерные вирусы впервые появились в 1986 году, хотя исторически возникновение вирусов тесно связано с идеей создания самовоспроизводящихся программ. Одним из "пионеров" среди компьютерных вирусов считается вирус "Brain". Только в США этот вирус поразил свыше 18 тыс. компьютеров. В начале эпохи компьютерных вирусов разработка вирусоподобных программ носила чисто исследовательский характер, постепенно превращаясь на откровенно вражеское отношение к пользователям безответственных, и даже криминальных "элементов". В ряде стран уголовное законодательство предусматривает ответственность за компьютерные преступления в том числе за создание и распространение

# ОСНОВНЫЕ ИСТОЧНИКИ КОМПЬЮТЕРНЫХ ВИРУСОВ.

# ОСНОВНЫЕ ИСТОЧНИКИ ВИРУСОВ:

- ДИСКЕТА, НА КОТОРОЙ НАХОДЯТСЯ ЗАРАЖЕННЫЕ ВИРУСОМ ФАЙЛЫ;
- КОМПЬЮТЕРНАЯ СЕТЬ, В ТОМ ЧИСЛЕ СИСТЕМА ЭЛЕКТРОННОЙ ПОЧТЫ И INTERNET;
- ЖЕСТКИЙ ДИСК, НА КОТОРЫЙ ПОПАЛ ВИРУС В РЕЗУЛЬТАТЕ РАБОТЫ С ЗАРАЖЕННЫМИ ПРОГРАММАМИ;
- ВИРУС, ОСТАВШИЙСЯ В ОПЕРАТИВНОЙ ПАМЯТИ ПОСЛЕ ПРЕДШЕСТВУЮЩЕГО ПОЛЬЗОВАТЕЛЯ.

# ПЕРВЫЕ ПРИЗНАКИ ЗАРАЖЕНИЯ КОМПЬЮТЕРНЫМ ВИРУСОМ:

- УМЕНЬШЕНИЕ ОБЪЕМА СВОБОДНОЙ ОПЕРАТИВНОЙ ПАМЯТИ;
- ЗАМЕДЛЕНИЕ ЗАГРУЗКИ И РАБОТЫ КОМПЬЮТЕРА;
- НЕПОНЯТНЫЕ (БЕЗ ПРИЧИН) ИЗМЕНЕНИЯ В ФАЙЛАХ, А ТАКЖЕ ИЗМЕНЕНИЯ РАЗМЕРОВ И ДАТЫ ПОСЛЕДНЕЙ МОДИФИКАЦИИ ФАЙЛОВ;
- ОШИБКИ ПРИ ЗАГРУЗКЕ ОПЕРАЦИОННОЙ СИСТЕМЫ;
- НЕВОЗМОЖНОСТЬ СОХРАНЯТЬ ФАЙЛЫ В НУЖНЫХ КАТАЛОГАХ;
- НЕПОНЯТНЫЕ СИСТЕМНЫЕ СООБЩЕНИЯ, МУЗЫКАЛЬНЫЕ И ВИЗУАЛЬНЫЕ ЭФФЕКТЫ И Т.Д.

# КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ.

# ПО МЕТОДУ СУЩЕСТВОВАНИЯ В КОМПЬЮТЕРНОЙ СРЕДЕ ВИРУСЫ ДЕЛЯТСЯ НА ТАКИЕ ВИДЫ:

## РЕЗИДЕНТНЫЕ

РЕЗИДЕНТНЫЙ ВИРУС, БУДУЧИ ВЫЗВАН ЗАПУСКОМ ЗАРАЖЕННОЙ ПРОГРАММЫ, ОСТАЕТСЯ В ПАМЯТИ ДАЖЕ ПОСЛЕ ЕЕ ЗАВЕРШЕНИЯ. ОН МОЖЕТ СОЗДАВАТЬ ДОПОЛНИТЕЛЬНЫЕ ПРОЦЕССЫ В ПАМЯТИ КОМПЬЮТЕРА, РАСХОДУЯ РЕСУРСЫ. МОЖЕТ ЗАРАЖАТЬ ДРУГИЕ ЗАПУЩЕННЫЕ ПРОГРАММЫ, ИСКАЖАЯ ИХ ФУНКЦИОНАЛЬНОСТЬ. МОЖЕТ “НАБЛЮДАТЬ” ЗА ДЕЙСТВИЯМИ ПОЛЬЗОВАТЕЛЯ, СОХРАНЯЯ ИНФОРМАЦИЮ О ЕГО ДЕЙСТВИЯХ, ВВЕДЕННЫХ ПАРОЛЯХ, ПОСЕЩЕННЫХ САЙТАХ И Т. П.

## НЕРЕЗИДЕНТНЫЕ

НЕРЕЗИДЕНТНЫЙ ВИРУС ЯВЛЯЕТСЯ НЕОТЪЕМЛЕМОЙ ЧАСТЬЮ ЗАРАЖЕННОЙ ПРОГРАММЫ И МОЖЕТ ФУНКЦИОНИРОВАТЬ ТОЛЬКО ВО ВРЕМЯ ЕЕ РАБОТЫ.

КОМПЬЮТЕРНЫЕ ЧЕРВИ.

# КОМПЬЮТЕРНЫЕ ЧЕРВИ.

СЕТЕВЫЕ ЧЕРВИ (ДРУГОЕ НАЗВАНИЕ – КОМПЬЮТЕРНЫЕ ЧЕРВИ) – ЭТО ПРОГРАММЫ, КОТОРЫЕ СОЗДАНЫ С ВНУТРЕННИМ МЕХАНИЗМОМ РАСПРОСТРАНЕНИЯ ПО ЛОКАЛЬНЫМ И ГЛОБАЛЬНЫМ КОМПЬЮТЕРНЫМ СЕТЯМ С НЕКОТОРЫМИ ЦЕЛЯМИ.

Данными целями являются:

1. ПРОНИКНОВЕНИЕ НА УДАЛЕННЫЕ КОМПЬЮТЕРЫ С ЧАСТИЧНЫМ ИЛИ ПОЛНЫМ ПЕРЕХВАТОМ УПРАВЛЕНИЯ ИМИ (СКРЫТЫМ ОТ ПОЛЬЗОВАТЕЛЯ – ХОЗЯИНА ЭТОГО КОМПЬЮТЕРА РАЗУМЕЕТСЯ);
2. ЗАПУСК СВОЕЙ КОПИИ НА КОМПЬЮТЕРЕ;
3. ДАЛЬНЕЙШЕЕ РАСПРОСТРАНЕНИЕ ПО ВСЕМ ДОСТУПНЫМ СЕТЯМ, КАК ЛОКАЛЬНЫМ, ТАК И ГЛОБАЛЬНЫМ.

## ЧЕРВЬ МОРРИСА

Он был самым страшным из известных на тот момент компьютерных вирусов (1988год!). Этот сетевой червь был одной из первых известных программ, эксплуатирующих переполнение буфера. Ему удалось сделать невозможное - вывести из строя всю глобальную сеть. Правда стоит отметить, что сеть тогда еще не была такой уж и глобальной. Сбой хоть и длился совсем не долгое время, но убытки от него были оценены в 96 миллионов долларов. Его создателем



# СРЕДСТВА БОРЬБЫ С КОМПЬЮТЕРНЫМИ ВИРУСАМИ.

# ДЛЯ ЗАЩИТЫ ОТ ВИРУСОВ МОЖНО ИСПОЛЬЗОВАТЬ:

ОБЩИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, КОТОРЫЕ ПОЛЕЗНЫ ТАКЖЕ КАК СТРАХОВКА ОТ ФИЗИЧЕСКОЙ ПОРЧИ ДИСКОВ, НЕПРАВИЛЬНО РАБОТАЮЩИХ ПРОГРАММ ИЛИ ОШИБОЧНЫХ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ;

ПРОФИЛАКТИЧЕСКИЕ МЕРЫ, ПОЗВОЛЯЮЩИЕ УМЕНЬШИТЬ ВЕРОЯТНОСТЬ ЗАРАЖЕНИЯ ВИРУСОМ;

СПЕЦИАЛИЗИРОВАННЫЕ ПРОГРАММЫ ДЛЯ ЗАЩИТЫ ОТ ВИРУСОВ.

ОБЩИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ПОЛЕЗНЫ НЕ ТОЛЬКО ДЛЯ ЗАЩИТЫ ОТ ВИРУСОВ. ИМЕЮТСЯ ДВЕ ОСНОВНЫЕ РАЗНОВИДНОСТИ ЭТИХ СРЕДСТВ:

КОПИРОВАНИЕ ИНФОРМАЦИИ — СОЗДАНИЕ КОПИЙ ФАЙЛОВ И СИСТЕМНЫХ ОБЛАСТЕЙ ДИСКОВ;

РАЗГРАНИЧЕНИЕ ДОСТУПА ПРЕДОТВРАЩАЕТ НЕСАНКЦИОНИРОВАННОЕ ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИИ, В ЧАСТНОСТИ, ЗАЩИТУ ОТ ИЗМЕНЕНИЙ ПРОГРАММ И ДАННЫХ ВИРУСАМИ,

# ВСЕ АНТИВИРУСНЫЕ ПРОГРАММЫ МОЖНО РАЗДЕЛИТЬ НА НЕСКОЛЬКО КАТЕГОРИЙ:

- 1) ПРОГРАММЫ-ДЕТЕКТОРЫ.
- 2) ПРОГРАММЫ-ЛЕКАРИ.
- 3) ПРОГРАММЫ-РЕВИЗОРЫ.
- 4) ЛЕКАРИ-РЕВИЗОРЫ.
- 5) ПРОГРАММЫ-ФИЛЬТРЫ.
- 6) ПРОГРАММЫ-ВАКЦИНЫ.

# САМЫЕ ПОПУЛЯРНЫЕ АНТИВИРУСНЫЕ ПРОГРАММЫ.

В СЕТИ INTERNET МНОГО КРАТКИХ "ШУТОЧНЫХ" ОПИСАНИЙ САМЫХ  
ПОПУЛЯРНЫХ И ИСПОЛЬЗУЕМЫХ АНТИВИРУСНЫХ ПРОГРАММ.

РАССМОТРИМ 4 САМЫХ РАСПРОСТРАНЕННЫХ АНТИВИРУСА СРЕДИ  
ПОЛЬЗОВАТЕЛЕЙ.

## KASPERSKY

ПЕХОТНЫЙ БАТАЛЬОН. ЛАГЕРЬ ВОКРУГ КОМПА, РОЕТ ОКОПЫ И СТАВИТ МИНЫ, МИНИРУЕТ ВСЕ, ОБМАТЫВАЕТ КОЛЮЧЕЙ ПРОВОЛОКОЙ, ОБОЗНАЧАЕТ СЕКТОРА ОБСТРЕЛА ОРУДИЙ И ПУЛЕМЕТОВ. ОБОРОНУ МОЖНО ПРОРВАТЬ ЛИШЬ ПРИ ПЯТИКРАТНОМ ЧИСЛЕННОМ ПРЕВОСХОДСТВЕ И ТОЛЬКО ПОСЛЕ МНОГОЧАСОВЫХ БОМБАРДИРОВОК.

**Преимущества:** Враг сможет пройти лишь превратив компьютер в пустыню.

**Недостатки:** Солдаты хотят кушать, а минные поля и окопы тормозят перемещение гражданских, так что ресурсов системы не остается.

**KASPERSKY**



**ANTI•VIRUS**

## DR. WEB

БАТАЛЬОН КАРАТЕЛЕЙ. ОКРУЖАЕТ КОМПЬЮТЕР ОЦЕПЛЕНИЕМ, СТАВИТ ВОЕННОЕ ПОЛОЖЕНИЕ, КРУГЛОСУТОЧНОЕ ПАТРУЛИРОВАНИЕ, КОМЕНДАНТСКИЙ ЧАС, А ЗА ПРОВИННОСТЬ - РАССТРЕЛ НА МЕСТЕ.

КАРАТЕЛИ ХВАТАЮТСЯ ЗА ОРУЖИЕ ПО ЛЮБОМУ ПОВОДУ, И ДАЖЕ ЕСЛИ ЕГО НЕТ, ПРОСТО ЖЕСТОКО ИЗБИВАЮТ ПРИКЛАДАМИ ВСЕХ, КТО ПОКАЖЕТСЯ ИМ ПОДОЗРИТЕЛЬНЫМ, ДАЖЕ ЕСЛИ ЭТО САМ ХОЗЯИН. ЕСЛИ ХОДИТЬ С ПОДНЯТЫМИ РУКАМИ, МЕДЛЕННЫМ ШАГОМ И ПОВЕСИТЬ НА ГРУДЬ ПРОПУСК, ЕСТЬ ШАНС, ЧТО БИТЬ БУДУТ НЕ СИЛЬНО И НЕ ОЧЕНЬ ДОЛГО.

**Преимущества:** ВРАГ НЕ ПРОЙДЕТ.

**Недостатки:** ГОСТИ И ХОЗЯЕВА ТОЖЕ.



## MSAFEE

Танковая бригада. Рычат моторы, чумазые танкисты хватают пробегающих мимо дам, а за лесом идет пальба. Выглядит внушительно и весомо, в бою работает быстро, и эффективно. Враг внутрь проникнуть не может.

**Преимущества:** Надежность.

**Недостатки:** Танковая смазка нынче очень дорога, не говоря уже о снарядах и горючем. Иногда забывают за врагов, если вокруг сильно много дам.



**McAfee**<sup>®</sup>  
Proven Security™

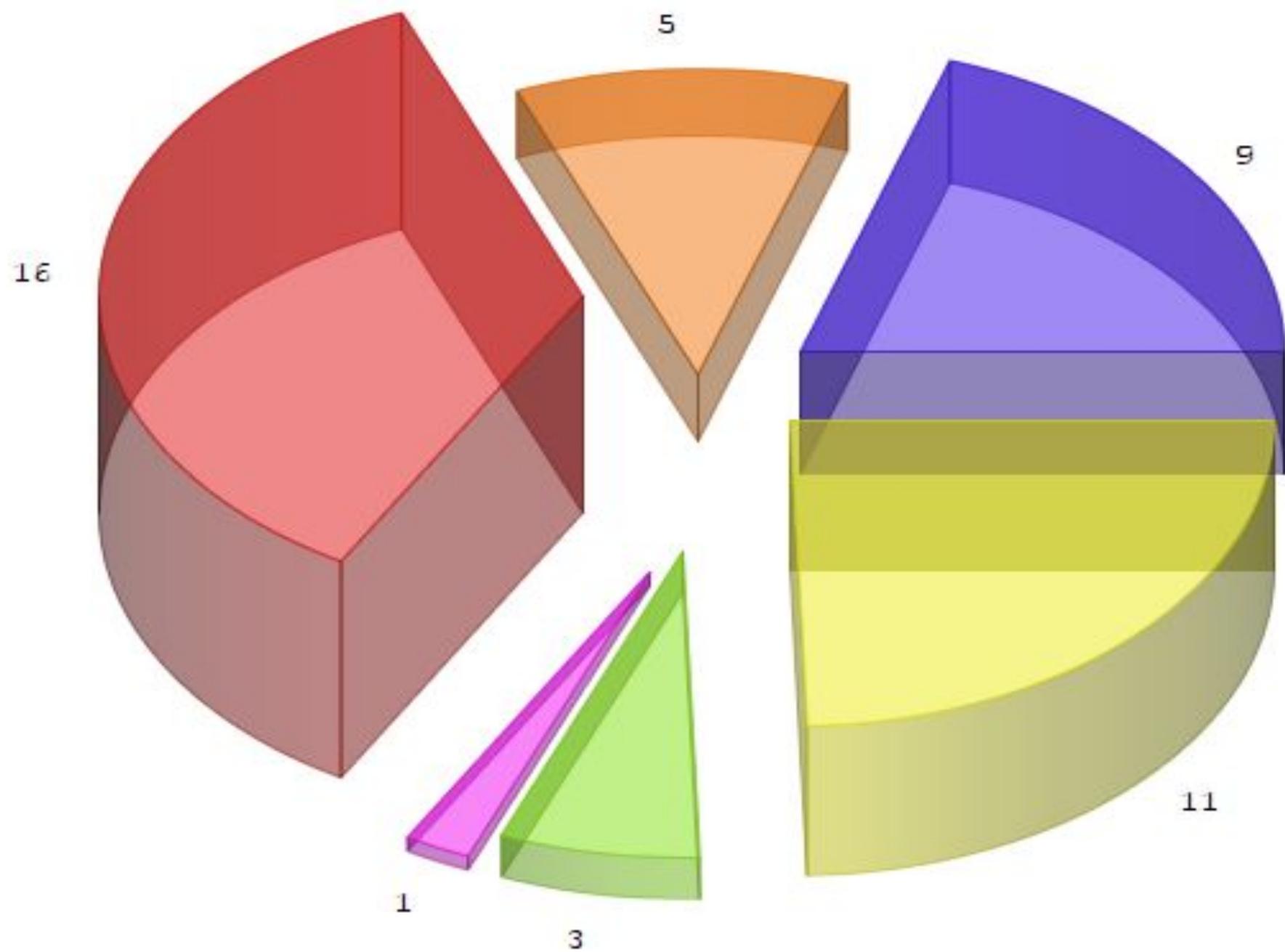
# NORTON

ОККУПАЦИОННАЯ АРМИЯ. ОФИЦЕРЫ  
БЕСПЛАТНО ПЬЮТ ШНАПС В  
РОСКОШНЫХ РЕСТОРАНАХ И КАФЕШКАХ,  
СОЛДАТЫ БЕГАЮТ ПО ДВОРАМ,  
РЕКВИЗИРУЮТ СЪЕСТНОЕ,  
ЗАНИМАЮТСЯ МЕЛКИМ МАРОДЕРСТВОМ.  
ДРУГОЙ-ТО ВРАГ В СТРАНУ, КОНЕЧНО,  
УЖЕ НЕ ПРОЛЕЗЕТ, ЭТО ДА. Но и  
ЖИЗНЬ В УСЛОВИЯХ ОККУПАЦИИ,  
ЗНАЕТЕ ЛИ, ТОЖЕ НЕ САХАР.

**ПРЕИМУЩЕСТВА:** ГРАНИЦА НА ЗАМКЕ.  
НАМЕРТВО.

**НЕДОСТАТКИ:** ВРАГ УЖЕ ВНУТРИ.





- KASPERSKY
- AVAST
- Другое
- Не использую
- NORTON
- ESET NOD32 Sp

# Вывод:

ПРОВЕДЯ ИССЛЕДОВАНИЕ НА ТЕМУ «КОМПЬЮТЕРНЫЕ ВИРУСЫ И СРЕДСТВА БОРЬБЫ С НИМИ», Я ПРИШЛА К ВЫВОДУ ЧТО КОМПЬЮТЕРНЫЕ ВИРУСЫ ОЧЕНЬ ОПАСНЫ И ПОЭТОМУ НУЖНО РЕГУЛЯРНО ПРОВОДИТЬ ПРОФИЛАКТИКУ ПРОТИВ НИХ; А ТАКЖЕ СЛЕДИТЬ ЗА ТЕМ, НА КАКИХ САЙТАХ В СЕТИ ИНТЕРНЕТ ВЫ БЫВАЕТЕ, ТАК КАК ОЧЕНЬ МНОГИЕ ИЗ НИХ ЧРЕЗВЫЧАЙНО ОПАСНЫ, КАК ДЛЯ САМОГО КОМПЬЮТЕРА, ТАК И ДЛЯ ВАШЕЙ ЛИЧНОЙ ИНФОРМАЦИИ, НАХОДЯЩЕЙСЯ НА УСТРОЙСТВЕ (НАПРИМЕР ПАРОЛИ, НОМЕРА СЧЕТОВ, ЛИЧНЫЕ ПЕРЕПИСКИ И ТАК ДАЛЕЕ); ПОЭТОМУ НА УСТРОЙСТВЕ ОБЯЗАТЕЛЬНО ДОЛЖНА БЫТЬ ЗАЩИТА (В ВИДЕ АНТИВИРУСНЫХ ПРОГРАММ, А ЛУЧШЕ НЕСКОЛЬКИХ). А ЕСЛИ ВАМ ВСЕ-ТАКИ УДАЛОСЬ «ПОЙМАТЬ» ВИРУС, ТО НЕОБХОДИМО НЕЗАМЕДЛИТЕЛЬНО УДАЛЯТЬ ВСЕ ДАННЫЕ С ПОМОЩЬЮ ОСОБЫХ ЭТАПОВ; А ЕЩЕ ЛУЧШЕ СРАЗУ ПЕРЕДАТЬ ЭТО ДЕЛО В РУКИ ПРОФЕССИОНАЛОВ.

*-КОМПЬЮТЕРНЫЙ ВИРУС, ЭТО ВРАГ  
ИЛИ ДРУГ?  
-ЭТО КОРМИЛЕЦ!*

ЕВГЕНИЙ КАСПЕРСКИЙ

