*~7 минут*

**1**

**Вступление:**

Темой для моей ВКР я выбрала создание Программного комплекса для определения вредоносных файлов в системе (*ПКОВФ*). Эта тема на сегодняшний день крайне актуальна, так как вредоносные программы могут наносить и таки наносят огромный ущерб, начиная отдельным пользователем ПК и заканчивая экономикой и безопасностью целой страны.

Именно поэтому так важно бороться с вирусами актуальными и надежными средствами, гарантирующими защиту даже от новых и сложных вирусных программ.

**На слайдах:**

1. Вступительный слайд с названием ВКР
2. Статистика: ущерб от вирусов, возникновение новых вирусов каждый день\неделю, успешные срабатывания антивирусов

**2**

**Полиморфные вирусы и защита от них:**

Вирус – это …

На текущий момент почти все вирусы являются полиморфными, т.е. такими, которые …

Чтобы бороться с ними современное антивирусное ПО использует два метода: эвристическое сканирование и эмуляцию. Но у обоих методов есть существенные недостатки: у эмуляции – большие затраты времени и ресурсов, у эвристического анализа – вероятность ложных срабатываний и негарантированный результат порядка 60% (?) успеха.

Именно поэтому так важно разобраться с этой проблемой и найти какое-то более совершенное решение или улучшить то, что уже есть.

**На слайдах:**

1. Вирус – это… Полиморфизм – это… Примеры полиморфных вирусов
2. Эмуляция – это… Недостатки
3. Эвристический анализ – это… Недостатки

**3**

**Шифрование и энтропия:**

Так как полиморфизм заключается в шифровании кода вредоносного ПО каким-то сгенерированным ключом, но при этом алгоритмов шифрования существует разумно ограниченное количество, я предположила, что процент информации на бит данных, т.е. информационная энтропия зашифрованных вирусов должна полностью совпадать.

**На слайдах:**

1. Информационная энтропия – это…
2. Какие-то сравнения зашифрованного и незашифрованного кода??

**4**

**PE-файл, метод плавающего окна:**

Отталкиваясь от этого, я разработала программу, которая на данном этапе может анализировать исполняемые файлы на предмет заражения вирусным кодом. Работает она следующим образом:

Парсером PE-заголовка, взятым из свободного доступа, я получаю доступ к секциям ……….

Из существующих я выбираю для анализа только один – с самым большим весом. Его я подгружаю в т.н. анализатор, где …. методом плавающего окна.

**На слайдах:**

1. PE-файл – это… Структура PE-заголовка.
2. *Рисунок* Выделение кода(?) из секции, имитация чтения методом плавающего окна.

**5**

**Работа программы в целом:**

Считанные данные в режиме реального времени рассчитываются по формуле информационной энтропии. Грубо говоря, каждый фрагмент, считанный методом плавающего окна, определяет координаты на графике информационной энтропии.

И ключевым моментом является то, что у зашифрованных одним алгоритмом (?), но разными ключами вирусов эти графики полностью совпадают.

Вот схема работы программы

**На слайдах:**

1. График энтропии (со скрина программы)
2. Схема работы программы

**6**

**Графики энтропии. Успехи в работе ПКОВФ:**

Этот метод не требует использования вирусных сигнатур или оценки поведения запущенного исполняемого файла. Он экспериментально подтвержден с использованием написанного мною программного продукта *ПКОВФ*. На слайдах видно полное совпадение графиков в случае анализа вредоносного ПО и в то же время графики абсолютно разные, если сравнивать вирус с незараженным файлом. Так же вот графики двух незараженных файлов. Они так же сильно отличаются.

**На слайдах:**

1. Графики вируса и вируса
2. Вируса и здорового
3. Здорового и здорового

**7**

**Доработки и развитие ПКОВФ. Нейросеть:**

Это отличные показатели. И возможно, мое решение станет новым методом борьбы с современными вредоносными ПО и будет встроено в антивирусы.

Сейчас же оно все еще требует доработок. У меня составлен план по созданию полноценного продукта для сканирования системы на вирусы. Первым шагом к этому станет добавление в *ПКОВФ* нейронной сети (ИНС).

А нужна она для того, чтобы не пользователь анализировал эти графики, а она сама. Достаточно выбрать входные значения. По моим предположениям это будут следующие варианты, которые нужно экспериментально сравнивать:

…

…

…

Они воссоздадут график энтропии с нормальной погрешностью для используемой ИНС. А обученная на разных примерах – вирусах и незараженных файлах, она сможет отличать одни от других.

Это значительно ускорит и упростит работу с *ПКОВФ.* Я собираюсь использовать простейшую нейросеть типа(?)…

**На слайдах:**

1. Скрин *ПКОВФ*
2. Нейросеть – это… Обучение нейросети в схемах.

**8**

**Выводы**

Плюсы (ни одно антивирусное ПО не имеет на данный момент схожего алгоритма обнаружения ВПО, скорость работы, малые траты ресурсов ПК, а главное – всегда актуально: найдет новые и неизвестные вирусы) и минусы (сырое, постоянно обучать ИНС или автоматизировать этот процесс(?), …) ПКОВФ.

Пока что ПКОВФ не поддерживает значительную часть функционала, но при всем этом уже успешно выполняет свою главную функцию – правильное распознавание вирусов, а значит, я на верном пути. Я буду дорабатывать свой проект, так как мне интересна эта тема. И надеюсь, что вскоре он станет продуктом массового пользования и возможно своего рода прорывом в сфере компьютерной безопасности.

**На слайдах:**

1. Плюсы и минусы
2. Что-то заключительное про прорыв и компьютерную безопасности
3. Спасибо за внимание. Конец