Феномен компьютерных вирусов как вершина эволюции разрушающих программных воздействий

Модель программы, инфицированной некоторым типичным по своему

поведению компьютерным вирусом V1

```
program V1_инфицированная_программа

    . . .

    ; Начало последовательности заведомо исполняемых команд
    . . .

    V1          ; Внедренный вызов программной компоненты V1
    . . .

    ; Конец последовательности заведомо исполняемых команд

    . . .


    ; Начало тела вируса V1

    procedure V1
        Инфицировать
        if Наступило_условие_выполнения_действия_V1 then
            Выполнить_действие_V1
        endif
        Устранить_последствия_внедрения_вызова_V1
    endprocedure

    procedure Инфицировать
        repeat
            Жертва:=Очередной_программный_файл
        while Файл_содержит_признак_внедрения_V1(Жертва)
        Разместить_тело_V1_в_файле(Жертва)
        Внедрить_вызов_V1_в_файл(Жертва)
        Установить_признак_внедрения_V1_для_файла(Жертва)
    endprocedure
```

```
    function Наступило_условие_выполнения_действия_V1 : boolean
    procedure Выполнить_действие_V1
    procedure Устранить_последствия_внедрения_вызова_V1
    function Очередной_программный_файл : file
    function Файл_содержит_признак_внедрения_V1(Файл : file) : boolean
    procedure Разместить_тело_V1_в_файле(Файл : file)
    procedure Внедрить_вызов_V1_в_файл(Файл : file)
    procedure Установить_признак_внедрения_V1_для_файла(Файл : file)

    ; Конец тела вируса V1


endprogram
```

Наличие классификационных признаков

V1_инфицированная_программа

if Наступило_условие_выполнения_действия_V1 **then**
    Выполнить_действие_V1
endif

V1

Устранить_последствия_внедрения_вызова_V1

Очередной_программный_файл

ТЕОРИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Проблема формального определения компьютерного вируса

AUTOEXEC.BAT

```
sys a:
copy *.* a:\
sys b:
copy *.* b:\
sys c:
copy *.* c:\
...
```

$$C: R' \underset{Def}{\to} R'',\ R' \subset P,\ R'' \subset P, \qquad (2.1)$$

$$\chi_R(r) \underset{Def}{=} \left\{ \begin{array}{l|l} 1 & r \in R \\ 0 & r \notin R \end{array} \right\}$$

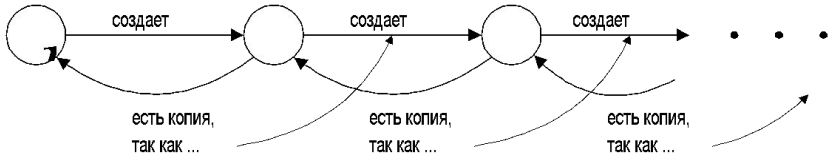
$$\chi_R(r) = \left\{ \begin{array}{l|l} 1 & \chi_R(C(r)) = 1 \\ 0 & \chi_R(C(r)) = 0 \ \vee \ r \notin R' \end{array} \right\},\ r \in P\,. \qquad (2.2)$$

$$r_1 \in R'$$

$$\exists k \left(k \in \square\!\!\square,\ 1 < k < +\infty \right) \left[C^k(r_1) \notin R' \right], \qquad (2.3)$$

$$k < +\infty \qquad C^k(\square) = \underbrace{C(C(\ldots(C(\square))\ldots))}_{k \text{ раз}}$$

$(2.2), (2.3) \Rightarrow \quad \chi_R(r_1) = 0$, то есть $r_1 \notin R$



$\{r_i\}_{i=0,1,\ldots}$, где $r_0 \in R'$ и $r_i = C(r_{i-1}) \in R',\ i = 1, 2, \ldots$.

$$\exists r_j \left(j \in \{0\} \cup \mathbb{N},\ j < +\infty \right) \exists l \left(l \in \mathbb{N},\ l < +\infty \right) \left[C^l(r_j) = r_j \right]. \qquad (2.4)$$

$$\chi_R(r) = \left\{ \begin{array}{l|l} 1 & C^{k-1}(r) \in R' \\ 0 & C^{k-1}(r) \notin R' \end{array} \right\},\ k \in \mathbb{N},\ k \geq 2,\ r \in P. \qquad (2.5)$$

Окончательное определение КВ

Определение 2.1. *Компьютерный вирус* – это программная компонента, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера и прочие выполняемые объекты как в рамках одного компьютера, так и в пределах вычислительных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения (в пределах, как минимум, нескольких поколений). Компьютерный вирус относится к вредоносным программным компонентам.

Памятка о формате файлов для сдачи лабораторных работ

- Синтаксис именования
- Семантика содержания

Формальная грамматика именования

<Имя архивного файла> ::= *<Идентификатор лабораторной работы>*.**zip**

<Имя файла пояснительной записки> ::= *<Идентификатор лабораторной работы>*.**rtf**

<Идентификатор лабораторной работы> ::= *<Группа>*.*<Работа>*.*<ФИО>*.*<Версия>*
<Группа> ::= *<Поток><Номер>*
<Работа> ::= **LR***<Номер>*
<ФИО> ::= *<Фамилия><И><О><Полный тезка>*
<Версия> ::= **v***<Номер>*
<Поток> ::= **PS** | **VM** | **IVT**
<Номер> ::= *<Цифра><Цифра>*
<Фамилия> ::= *<Прописная буква><Последовательность строчных букв>*
<И> ::= *<Прописная буква>*
<О> ::= *<Прописная буква>*
<Полный тезка> ::= ∅ | *<Цифра>*

<Последовательность строчных букв> ::= ∅ | *<Последовательность строчных букв><Строчная буква>*
<Прописная буква> ::= **A** | **B** | ... | **Z**
<Строчная буква> ::= **a** | **b** | ... | **z**
<Цифра> ::= **0** | **1** | ... | **9**

Здесь: ∅ – «пустой» символ