

004.491.42

В роботі розроблено модель та архітектуру розподіленої багаторівневої систем виявлення шкідливого програмного забезпечення в локальних комп'ютерних мережах, побудовану на основі принципів децентралізації та самоорганізації. Розподілена багаторівнева система відноситься до реагуючих систем і постійно здійснюватиме моніторинг запущених процесів та виконуваних програм в комп'ютерних системах мережі. Розроблена системи здійснюватиме перевірку наявного програмного забезпечення та запущених процесів в комп'ютерних системах локальної мережі на можливість віднесення до шкідливого програмного забезпечення.

Ключові слова: модель, архітектура, структура Крипке, шкідливе програмне забезпечення, поведінка, розподілена система, принцип самоорганізації, локальна комп'ютерна мережа.

O.S. SAVENKO  
Khmelnitskyi National University

### MODEL AND ARCHITECTURE OF THE DISTRIBUTED MULTILEVEL SYSTEM OF DETECTION MALWARE IN THE LOCAL COMPUTER NETWORKS

In the work the model and architecture of distributed multilevel detection systems of malicious software in local computer networks, based on the principles of decentralization and self-organization, has been developed. The basis of the constructed model of distributed multi-level systems is its structural parts, which are represented by program modules, which can be in different states. The transition between the classes of program modules is based on a defined set of transitions. Interaction and communication between software modules is based on their presence in certain states during operation. Distributed multi-level systems is a responsive system that will monitor selected events. Each program module contains a resident mechanism, the motive mechanisms for the transition between states, the transitions between which are given subsets of transitions, the data for which will be formed using artificial intelligence technologies. The developed system will verify the existing software and running processes in the computer systems of the local network to the ability to refer to malicious software. The principles and models of systems development are important for the theory and practice of creating effective systems for detecting malicious software in local computer networks built on the basis of decentralization and self-organization principles. The designed architecture of the distributed multilevel system allows it to be filled with various functions of detecting malicious software in local computer networks. The developed model of the architecture of the software modules of distributed multilevel systems is based on the principles of autonomy and multilevel. It allows you to increase the number of levels of the system without changing its architecture. The basis of the architecture of distributed multi-level systems are software modules with the same architecture, but each of them can independently take decisions based on various data collected from different computer systems of the network.

Keywords: model, architecture, structure Kripke, malware, behaviour, distributed system, self-organization principle, local computer network.



$$A = \{A_1, \dots, A_n\} \quad (1)$$



4.



5.

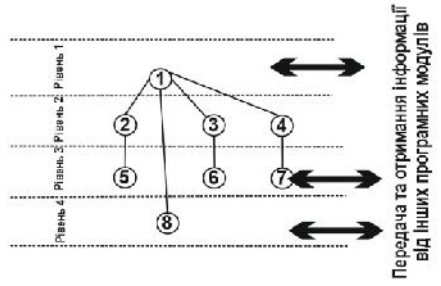
Рівень 1	Децентралізація
Рівень 2	Прийняття рішень
Рівень 3	***
***	***
Рівень n	***

.б.

( )



4. – 4 ; ,  
 1, 3 4 ,  
 1, 2, 3  
 4 2. 2 1 3,  
 3,



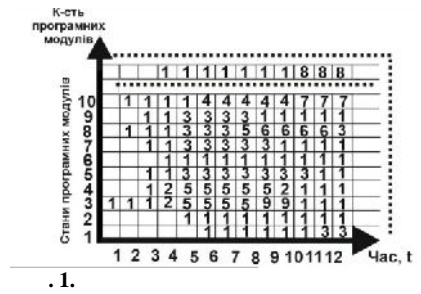
9.

- 1)
- 2)
- 3)
- 4)
- 5)

6) ;

7) ( );

8) ;



10.

10

$$M = S, S_0, R, F \quad (3)$$

$S$  – ,  $S_0$  – ( ,  
 $R$  – ,  $T_A$  –  
 $F$  – ,  $S$  ,  
 $A_i, i=1,2,\dots,n$ ,

$$S = \sum_{i=1}^n S_i ,$$

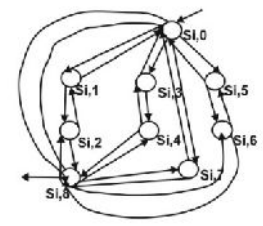
$$S_0 = \sum_{i=1}^n S_{0i} ,$$

$$R \subseteq S \times S ,$$

$$F \subseteq S$$

$$M_{A_i} = S_i, S_{0i}, R_i, F_{A_i} , \quad (4)$$

$i=1,2,\dots,n$ ,  $R_i$  –  
 $i$  – ,  $F_{A_i}$  –  
 $T_{A_i}$  ,  $2^{T_{A_i}}$ .



11.  $A_i$

$S_{ij}S_{ip}$ ,  $i -$ ,  $j - p -$ ,  
 $S_{ij}S_{ip}S_{ij}S_{ih}S_{iy}S_{iu}S_{ie}S_{ik}.....$   
 ( . 11).  
 . 1  $S_i$   
 1

			$S_i$
$i$	$S_{i,0}$	0000	$i$ 6- ( )
	$S_{i,1}$	0001	
	$S_{i,2}$	0010	
	$S_{i,3}$	0011	
	$S_{i,4}$	0100	
	$S_{i,5}$	0101	
	$S_{i,6}$	0110	
	$S_{i,7}$	0111	
	$S_{i,8}$	1000	

$i=5$   
 000101  
 $S_5 = \{0000000101, 0001000101, 00100001010, 0011000101, 0100000101, 0101000101, 0110000101, 0111000101, 1000000101\}$ .

$V = \sum_{i=1}^n V_i$ ,  $V_i -$   
 $V' = \sum_{i=1}^n V'_i$ ,  $V'_i -$

$R_i - i -$   
 $R_i = \{$   

0000i	0001i,	0001i	0000i,	0001i	0100i,	0100i	0001i,
0100i	1000i,	1000i	0100i,	0000i	1000i,	1000i	0000i,
0000i	0010i,	0010i	0000i,	0010i	0101i,	0101i	0010i,
0101i	1000i,	1000i	0101i,	0000i	0011i,	0011i	0000i,
0011i	0110i,	0110i	0011i,	1000i	0110i,	0110i	1000i,
0000i	0111i,	0111i	0000i,	1000i	0111i,	0111i	1000i

 $\}$

$F_{A_i} S_i T_{A_i}$   
 ( . 2).

$P_{i,0}$	0000i	$S_{i,0}$
$P_{i,1}$	0000i, 0001i	$S_{i,1}$
...	...	...
$P_{i,47}$	0111i, 1000i	$S_{i,47}$

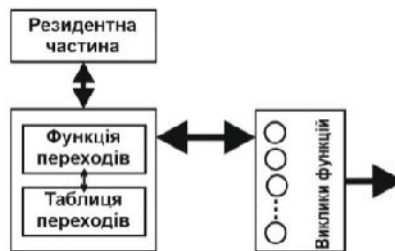
$P_{ij} . 8$

3.

	A <sub>i</sub>										V <sub>i</sub>	V <sub>i</sub> '	
		S <sub>i,0</sub>	S <sub>i,1</sub>	S <sub>i,2</sub>	S <sub>i,3</sub>	S <sub>i,4</sub>	S <sub>i,5</sub>	S <sub>i,6</sub>	S <sub>i,7</sub>	S <sub>i,8</sub>			
S <sub>i,0</sub>	p <sub>i,0</sub>	1	0	0	0	0	0	0	0	0	0	V <sub>i,0,0</sub>	V <sub>i,0,0</sub> '
	p <sub>i,1</sub>	1	1	0	0	0	0	0	0	0	0	V <sub>i,0,1</sub>	V <sub>i,0,1</sub> '
	p <sub>i,2</sub>	0	0	0	0	0	0	0	0	0	0	-	-
	p <sub>i,3</sub>	1	0	0	1	0	0	0	0	0	0	V <sub>i,0,3</sub>	V <sub>i,0,3</sub> '
	p <sub>i,4</sub>	0	0	0	0	0	0	0	0	0	0	-	-
	p <sub>i,5</sub>	1	0	0	0	0	1	0	0	0	0	V <sub>i,0,5</sub>	V <sub>i,0,5</sub> '
	p <sub>i,6</sub>	0	0	0	0	0	0	0	0	0	0	-	-
	p <sub>i,7</sub>	1	0	0	0	0	0	0	1	0	0	V <sub>i,0,7</sub>	V <sub>i,0,7</sub> '
p <sub>i,8</sub>	1	0	0	0	0	0	0	0	1	0	V <sub>i,0,8</sub>	V <sub>i,0,8</sub> '	
...	...	...	...	...	...	...	...	...	...	...	...	...	...
S <sub>i,8</sub>	p <sub>i,0</sub>	1	0	0	0	0	0	0	0	0	0	V <sub>i,0</sub>	V <sub>i,0</sub> '
	p <sub>i,1</sub>	0	0	0	0	0	0	0	0	0	0	-	-
	p <sub>i,2</sub>	1	0	1	0	0	0	0	0	0	0	V <sub>i,8,2</sub>	V <sub>i,8,2</sub> '
	p <sub>i,3</sub>	0	0	0	0	0	0	0	0	0	0	-	-
	p <sub>i,4</sub>	1	0	0	0	1	0	0	0	0	0	V <sub>i,8,4</sub>	V <sub>i,8,4</sub> '
	p <sub>i,5</sub>	0	0	0	0	0	0	0	0	0	0	-	-
	p <sub>i,6</sub>	1	0	0	0	0	0	1	0	0	0	V <sub>i,8,6</sub>	V <sub>i,8,6</sub> '
	p <sub>i,7</sub>	1	0	0	0	0	0	0	1	0	0	V <sub>i,8,7</sub>	V <sub>i,8,7</sub> '
p <sub>i,8</sub>	1	0	0	0	0	0	0	0	1	1	V <sub>i,8,8</sub>	V <sub>i,8,8</sub> '	

F<sub>A</sub>

. 12.



. 12.

1)



