

# Ochrona przed programami złoslíwymi systemu operacyjnego i poczty elektronicznej

>

## **Cel i zakres pracy.....5**

### **Rozdział 1.**

#### **Pojęcie wirusa i robaka komputerowego.....6**

##### 1.1.Co to jest i jak działa wirus komputerowy.....6

###### 1.1.1. Struktura zzonego pliku i algorytm powielania się wirusa.....7

###### 1.1.2. Powstanie pierwszego wirusa i jego działanie.....9

##### 1.2. Robak komputerowy – opis i działanie.....10

###### 1.2.1. Powstanie pierwszego robaka.....11

###### 1.2.2. Zasada działania robaka.....12

### **Rozdział 2.**

#### **Klasyfikacja wirusów oraz opis ich funkcjonowania.....14**

##### 2.1. Wirusy nierezydentne.....14

###### 2.1.1. Sposób powielania się wirusa nierezydentnego.....14

##### 2.2. Wirusy rezydentne.....17

###### 2.2.1. Algorytm działania wirusa rezydentnego.....17

##### 2.3. Szybkie infekторы.....20

##### 2.4. Wolne infekторы.....20

##### 2.5. Wirusy plikowe (tzw. zwykle ,file viruses).....20

##### 2.6. Wirusy towarzyszące.....22

##### 2.7. Makrowirusy.....23

##### 2.8. Wirusy pasożytnicze.....24

2.9. Wirusy polimorficzne.....	25
2.10. Retrowirusy.....	26
2.11. Fagi.....	26
2.12. Wirusy typu WIRUSY TYPU "stealh".....	26
2.13. Wirusy sektora startowego dysku ( wirusy boot sektora, boot sector viruses ).....	27
2.14. Wirusy FAT (wirusy tablicy alokacji plików ).....	27

## **Rozdział 3.**

### **Inne programy złośliwe.....**

3.1. Tylne wejścia i furtki.....	28
3.2. Bomby logiczne.....	29
3.3. Bakterie i króliki.....	30
3.4. Konie trojańskie.....	30
3.4.1. Przykłady koni trojańskich.....	32
3.4.1.1. Prosiak 0.70.....	32
3.4.1.2. Cafeini 1.1.....	36
3.4.1.3. Netbus 1.7.....	37
3.4.1.4. Netbus 2.0.....	39
3.4.1.5. Trojan.PSW.GOPtrojan.....	40
3.4.1.6. Donald Dick.....	41
3.4.1.7. Wincrash.....	42
3.4.1.8. Back Orifice.....	43
3.4.1.9. Acid shiver.....	44
3.4.2. Wykrywanie koni trojańskich.....	47
3.4.3. Konie trojańskie służące do ochrony przed koniami trojańskimi.....	48
3.4.3.1. Netbuster.....	48
3.4.3.2. Gaban Bus.....	49
3.5. Przykłady robaków internetowych rozprzestrzeniających się przez sieć wykorzystując pocztę elektroniczną.....	50
3.5.1. I-Worm.Myparty.....	51
3.5.2. I-Worm.Kiray.....	52
3.5.3. Klez.e.....	52
3.5.4. JS.Coolsite.....	54

3.5.5. I-Worm.Gigger.....	55
3.5.6. I-Worm.GOPworm.....	56
3.5.7. Fundll.....	56
3.5.8. Gokar.....	57
3.5.9. Maldał.....	58

## **Rozdział 4.**

### **Zagrożenia wirusem komputerowym i sposoby działania wirusów z różnym obiektem zakaźnym.....**

60

4.1. Pliki wykonywalne COM.....	60
4.2. Pliki exe dla systemu DOS (stare exe).....	62
4.3. Pliki nowe exe dla Windows (NE).....	65
4.4. Pliki systemowe sys.....	67
4.5. Pliki wsadowe bat.....	69
4.6. Pliki doc.....	70
4.7. Pliki xls.....	70
4.8. Pliki asm.....	71
4.9. Sektory systemowe.....	71
4.10. Główny rekord ładujący (ang. master eotrecord - mer).....	72
4.11. Rekord ładujący (ang. boot -sector).....	72
4.12. Jednostki alokacji plików (jap).....	73
4.13. Wirusy kombinowane.....	74

## **Rozdział 5.**

### **Sposoby przenikania wirusa do komputera.....**

75

5.1. Sposoby przenikania wirusów.....	75
5.2. Jak może nastąpić infekcja.....	75
5.3. Środki przenoszenia wirusów.....	77
5.3.1. Dyski elastyczne.....	77
5.3.2. Wymienne dyski sztywne.....	77
5.3.3. Kasety z taśmy magnetycznej.....	78
5.3.4. Nosniki innego rodzaju.....	78
5.3.5. Sieci.....	78

5.4. Drogi przenikania wirusów.....	78
5.4.1. Oprogramowanie pirackie.....	79
5.4.2. Biuletyny elektroniczne.....	79
5.4.3. Programy shareware.....	80
5.4.4. Programy publiczne (public domain).....	80
5.4.5. Rozproszone komputery osobiste.....	80
5.4.6. Dyskietki i CD-ROMy dołączane do czasopism komputerowych.....	81
5.4.7. Pracownicy firm serwisowych.....	81
5.5. Typowe ryzyko zainfekowania.....	81

## **Rozdział 6.**

### **Ochrona przed infekcją.....83**

6.1. Przygotowanie na ewentualny atak wirusa.....	85
6.2. Zapobieganie infekcjom wirusowym.....	86
6.3. Wykrycie wirusa.....	88
6.4. Powstrzymanie wirusa.....	89
6.5. Przywracanie sytuacji sprzed ataku wirusa.....	89
6.6. Tendencje rozwoju wirusów.....	90

## **Rozdział 7.**

### **Ochrona przed poszczególnymi rodzajami wirusów.....91**

7.1. Ochrona przed wszelkiego rodzaju wirusami i rodzaje programów wspomagających ochronę.....	91
7.2. Ochrona przed robakami.....	91
7.3. Ochrona przed koniami trojańskimi.....	92
7.4. Ochrona przed furtkami postawionymi w systemie.....	92
7.5. Ochrona przed bombami logicznymi.....	92

## **Rozdział 8**

### **Metody zabezpieczeń i walki z zakażeniem wirusowym.....93**

8.1. Kontrolowanie dostępu do sieci.....	93
8.1.1. Identyfikacja kanałów dostępu.....	94

8.1.2. Scentralizowane sieciowe serwery plików.....	94
8.1.3. Rozproszenie zaufania.....	95
8.1.4. Przesyłanie w sieciach z połączeniami ogólnie dostępnymi.....	96
8.2. Metody kontroli dostępu.....	96
8.3. Scentralizowane sieciowe serwery plików.....	97
8.4. Rozproszenie zaufania.....	97
8.5. Usługi poczty elektroinicznej.....	98

## **Rozdział 9**

### **Podstawowe rodzaje narzędzi przeciwwirusowych.....100**

9.1. Programy podsuwane wirusom do zaatakowania w pierwszej kolejności.....	100
9.2. Programy śledzące odwołania do systemu operacyjnego.....	100
9.3. Programy obliczające i sprawdzające sumy kontrolne plików.....	101
9.4. Programy detekcyjne.....	101
9.5. Programy uodporniające przed zakażeniem.....	101
9.6. Programy leczące, usuwające wirusy z plików oraz dysków.....	102

## **Rozdział 10.**

### **Działania programów antywirusowych i ich przykłady.....103**

10.1. Działanie programów antywirusowych.....	103
10.1.1. Skanery wirusowe.....	103
10.1.2. Skanery heurystyczne.....	105
10.1.3. Blokady zachowania.....	105
10.1.4. Testery integralności.....	105
10.2. Programy antywirusowe.....	106
10.2.1. AntiVirenKit 10.....	106
10.2.2. KAV Personal.....	107
10.2.3. Mks dla Windows.....	108
10.2.4. Symantec Norton Antivirus 2002.....	108

**Zakończenie.....110**

**Literatura.....111**