Дальнейшее увеличение эффективности ПЗ может достигаться за счет:

- установления минимальной длины пароля (не менее 8 символов из букв, цифр, специальных знаков в двух регистрах);
- установления максимального срока действия пароля (до 1 месяца);
- обеспечения невозможности замены пароля по истечении его срока действия на один из используемых ранее;
- ограничения числа попыток неправильного ввода пароля;
- обеспечения замкнутости программной среды и др.

## V Выводы

Безопасность ПЗ в современных программных продуктах в значительной степени зависит от качества произвольно выбираемых пользователем (администратором) или генерируемых автоматически паролей.

Изложенные выше оценки и рекомендации позволяют повысить безопасность ПЗ для методов взлома, основанных на силовом переборе возможных равновероятных вариантов, на использовании известных вероятностей появления символов в осмысленных словосочетаниях, а также частотных словарей вероятных паролей.

При этом кардинальными методами усиления ПЗ являются введение ограничений на число неверно введенных значений пароля и обеспечение замкнутости программной среды, не позволяющей злоумышленнику запустить программы – парольные взломщики. Однако их практическая реализация в ряде случаев затруднена.

*Литература:* ***1.*** *Хофман Л. Дж. Современные методы защиты информации. М.: Советское радио, 1980.* ***2.*** *Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа. – СПб: Наука и техника, 2004.* ***3.*** *Анин Б. Ю. Защита компьютерной информации.– СПб: БХВ–Петербург, 2000.* ***4.*** *Емельянов С. Л., Гаращук В. В. Некоторые аспекты безопасности парольной защиты//Вісник ЧДТУ, №2/2006, С. 155–157.* ***5.*** *Безмалый В. Ф. Краткий обзор программ-взломщиков паролей//http:// www.zahist.kiev.ua. .****6.*** *Г. Красноступ, Д. Кудин. Шпионские программы и новейшие методы защиты от них // Науково-технічний збірник "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні", Вип..9, 2004, С. 67–75.* ***7.*** *В. Безмалый. Чем нас пытаются взломать // www.itacademy.com.ua .****8.*** *http://www.bezpeka.com–Официальный сайт "Центра информационной безопасности".****9.*** *Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях./Под ред. В. Ф. Шаньгина . – М.: Радио и связь, 1999.*

**УДК 681.3**

# АНТИВІРУСНІ ПРОГРАМИ СВІТОВИХ БРЕНДІВ: ПОРІВНЯЛЬНА ОЦІНКА МОЖЛИВОСТЕЙ, РЕКОМЕНДАЦІЇ З ЇХ ВИБОРУ, НОВИЙ МЕТОД ПРОГНОЗУВАННЯ АНТИВІРУСНОЇ БЕЗПЕКИ

***Вячеслав Шорошев***
*ДНДІ МВС України*

***Аннотация:*** **Надаються порівняльна оцінка світових лідерів антивірусних програм, рекомендації по їх вибору, а також метод прогнозування антивірусної безпеки в комп'ютерних системах і мережах.**
Summary: **The guidelines on their selection, and also method of forecasting (prediction) of anti-virus safety are given a comparative estimation of the world (global) leaders of the anti-virus programs.**
*Ключові слова:* **Антивірусні програми, детектуваня вірусів, виявлення вірусів, розпізнавання вірусів, антивірусна безпека, ризик антивірусної безпеки.**

## I Вступ

Рейтингові оцінки антивірусних програм світових брендів і зростання їх можливостей в останній час досить вагомі. Але одних рейтингових оцінок антивірусних програм вже недостатньо. Для адміністратора безпеки завжди важливо знати – по-перше, який комплект антивірусних програм найбільш пріоритетний для підвищення антивірусної безпеки оцінюваної комп'ютерної системи або локальної мережі, особливо

Інтранет. І по-друге, при використанні якого комплекта антивірусних програм буде найменший ризик антивірусної безпеки? Пропонуються практичні рекомендації щодо вибору таких комплектів антивірусів і новий метод прогнозування антивірусної безпеки. Чому "комплектів" антивірусів?

Справа в тому, що кожна антивірусна програма може виявляти й розпізнавати не всі, а тільки певні види вірусів, наприклад, мережні, поліморфні, віруси-хробаки, DoS-віруси, скрипт-вируси, email-віруси, мобільні віруси, нарешті, останні новинки у вигляді вірусів-шпигунів і проактивних вірусів і т. ін. Універсального антивірусного засобу просто не існує, його навіть практично створювати недоцільно, хоча теоретично й можливо. Доцільно застосовувати кілька антивірусів (комплект 2 – 3 антивірусів за критерієм "ефективність-вартість"), щоб їх можливостями сукупно й надійно перекрити весь можливий діапазон вірусних атак будь-якого виду з ризиком, не вище заданого.

Всіх адміністраторів безпеки, користувачів і власників комп'ютерних систем завжди хвилює питання їх антивірусної безпеки. Адже кількість комп'ютерних вірусів зростає вже не щорічно, а щомісяця і ця тенденція загрозливо стабільна. Так, з 2001р. по 2005р. кількість комп'ютерних вірусів збільшилася з 40000 до 140000, а статистика вірусних атак за даними лабораторії Касперського загрозливо постійна. Так, за період з 2002 по 2005 роки зафіксовано від 5 до 20 вірусних епідемій щоквартально [1].

Крім того, серед усіх видів атак та загроз на комп’ютерні системи доля комп’ютерних вірусів за тією ж статистикою з 1999 р. по 2006 р. становила 65 – 90%!

Також переконливі дані щодо загальних обсягів втрат світової економіки від вірусних атак, які приведено в Computer Economics, 2005 Malware Report. Так, відмічаються два піки втрат до 17 млрд. долларів в 2004 и 2005 роках, а щорічні втрати світової економіки з 1999 р. тримаються на відмітці понад 10 млрд. доларів.

Таким чином, наведені дані ще раз підтверджують зростаючу актуальність антивірусної безпеки, а також необхідність її вдосконалювання як розробкою й використанням нових програм і пакетів антивірусного захисту, так і методів прогнозування ефективності їх захисту.

## II Основна частина

Політика антивірусної безпеки завжди була вирішальною компонентою в системах захисту інформації в комп’ютерних системах і мережах (далі КС). Вона передбачає забезпечення надійного та ефективного захисту проти будь-яких вірусних атак (потенційно загрозливих, реальних, перспективних). Так, поява в антивірусах евристичного режиму виявлення нових вірусів з невідомими їх сигнатурами та алгоритмами деструктивних дій надало автору можливість використати цей режим для імовірної кількісної оцінки стану антивірусної безпеки. Така спроба вперше була запропонована в 1999 р. в [2, 3]. З того часу автором регулярно надаються огляди брендів антивірусного захисту з довідковими таблицями їх тестів (табл. 1).

**Метод прогнозування** антивірусної безпеки КС за вимогами запропонованих AVS-правил (anti-virus safety) полягає у послідовності здійснення наступних етапів [4].

Таблиця 1 – Можливості світових брендів антивірусних програм

| Найменування антивірусної програми | Фірма-провайдер, її адреса | Процент розпізнаних вірусів (Pn) | Термін сканування (хвил.) |
|---|---|---|---|
| AVP | Procon Software, 07745 Jena | 99.3% (0.99) | 5.1 |
| AVScan | H+BEDV, 88069 Tettnag | 91.2% (0.91) | 4.9 |
| CPAV | Symantec, 40237 Duesseldorf | 72.6% (0.73) | 12.8 |
| Dr. Solomon’s AVTK | S&S International, 20537 Hamburg | 96.5% (0.96) | 4.3 |
| F-Prot Proffesional | Percom-Verlag, 22041 Hamburg | 89.1% (0.89) | 7.1 |
| Iris Antivirus | Hoffman Datenshutz, 40239 Dusseldorf | 89.6% (0.9) | 15.1 |
| McAffee Scan | McAffee Network Security&Menagement, 81677 Munchen | 91.3% (0.91) | 9 |
| Microsoft Antivirus | Microsoft, 85713 Unterschleissheim | 34% (0.34) | 6.2 |
| Norton Virus Control | Norman Data Defense Systems, 42697 Solingen | 97.1% (0.97) | 6.2 |
| Norton Antivirus | Symantec, 40237 Dusseldorf | 87.1% (0.87) | 2.3 |
| Sophos Sweep | Noviz Data, 23569 Luebeck | 97.6% (0.98) | 7.4 |
| Thunderbyte | Promus Conception, 45468 Muenchen | 88.5% (0.88) | 0.6 |

1. **Здійснюється прогнозування.** Прогнозування починається з формування основних положень політики антивірусної безпеки КС певного призначення і конфігурації залежно від множини факторів безпеки, запропонованих в моделі політики антивірусної безпеки КС (рис. 1). Це, насамперед, визначення загроз та видів комп'ютерних вірусів (реальних, потенційно загрозливих, перспективних), визначення об'єктів антивірусного захисту та комплектів антивірусів для кожного з них.

Реально загрозливими (реальними) вірусами визначаються ті, які є реальною загрозою для об'єкта КС. Ними можуть бути один/усі з потенційно загрозливих вірусів, старі віруси із архівних файлів, спеціальні та нові віруси тощо.

Спеціальними вірусами визначаються різні шкідливі програми – конструктори вірусів, генератори вірусних атак, вірусні утиліти тощо.

Перспективними визначаються New-віруси, Win32-віруси, DoS-віруси, Mobil-віруси, Spiware-віруси, віруси проактивних деструктивних дій тощо.

За визначенням Лабораторії Касперського [1] spyware-віруси – це підмножина троянських програм, рекламних модулів і потенційно загрозливих програм, це просто маркетинговий термін для виділення нового класу Security-програм, spyware-вірусів не існує взагалі. Проактивний захист спеціально створено для виявлення ще невідомого деструктивного програмного забезпечення. Він вважається як досить перспективний. Основні підходи проактивного захисту полягають у використанні наступних механізмів та послуг безпеки: евристичий аналізатор, безпека на основі політик, Intrusion Protection System (IPS), захист від переповнення буфера (Buffer Overrun protection), блокиратори поведінки, статистичні методи. З лютого 2007 р. в Україну почали надходити в продаж антивіруси Касперського версій 6.0 і вище з проактивним захистом [1]. Проактивний захист вже понад два роки реалізовано іспанським антивірусом Panda (за даними міжнародної виставки EnterEX 2007).

2. **Визначаються об'єкти** антивірусного захисту КС, наприклад, ПЕОМ, робочі станції, сервери, кінцеві термінали, КС класу 1, 2, 3 тощо. Політика антивірусної безпеки кожного об'єкту КС повинна забезпечуватись на рівні не менш заданого за критерієм "ризик антивірусної безпеки-вартість" [4].

Вона реалізується, насамперед, вибором антивірусів за їх можливостями згідно з даними так званих "довідкових таблиць" фахівців-ентизуастів антивірусного захисту КС, фірменних тестових рейтингів і балів тощо, яких повинно бути якомога більше, а також прогнозуванням антивірусної безпеки методом запропонованих "AVS-правил", тобто використанням певного аналітичного методу і математичних співвідношень.

Метод AVS-правил є подальшим розвитком відомих моделей і правил захисту Biba (1977 р.), Gougen-Meseguer (1982 р.), Sutherland (1986 р.), Clark-Wilson (1989 р.), при цьому модель Кларка-Вильсона вважається однією з найкращих щодо підтримки цілісності інформаційних систем. Запропонований метод AVS-правил забезпечує апріорі прогнозування антивірусної безпеки КС за даними значень показника Pn в табл. 2 – 6, які постійно і регулярно доповнюються та оновлюються AVS-фахівцями.

3. **Визначається аналітичний метод** (математичні співвідношення) кількісної оцінки ризику антивірусної безпеки для кожного з видів вірусів згідно з моделлю політики антивірусної безпеки (рис. 1).

4. **Здійснюється прогнозування** антивірусної безпеки КС та її кількісне експертне оцінювання методом AVS-правил за наступними математичними співвідношеннями для основних видів вірусів згідно з моделлю політики антивірусної безпеки (рис. 1). Модель політики антивірусної безпеки повинна, на нашу думку, постійно доповнюватись та удосконалюватись.

Так, для робочої станції/ПЕОМ ризик антивірусної безпеки від атак Win-вірусів Rwin оцінюється за співвідношенням:

$$Rwin = \prod_{n=1}^{N} (1 - Pn), \qquad (1)$$

де Pn – імовірність виявлення і знешкодження відомих і невідомих вірусів n-ю антивірусною програмою за результатами її тестових випробувань згідно з даними табл. 2;

N – кількість антивірусів в робочому комплекті, яким забезпечується антивірусний захист робочої станції/ПЕОМ.

Наприклад, для захисту ПЕОМ від Win-вірусів (табл. 2) використовуються два антивіруси (N=2) – UNA 1.61.0.97 (Pn = 0.72) і DrWeb for Windows 4.29b (Pn = 0.81). Тоді Rwin = (1- 0.72)(1 – 0.81) = 0.0532. Таким чином, ризик антивірусної безпеки ПЕОМ складає 5.32 %, тобто, до 5 % атак Win-вірусів будуть успішними і деструктивно впливати на роботу ПЕОМ.

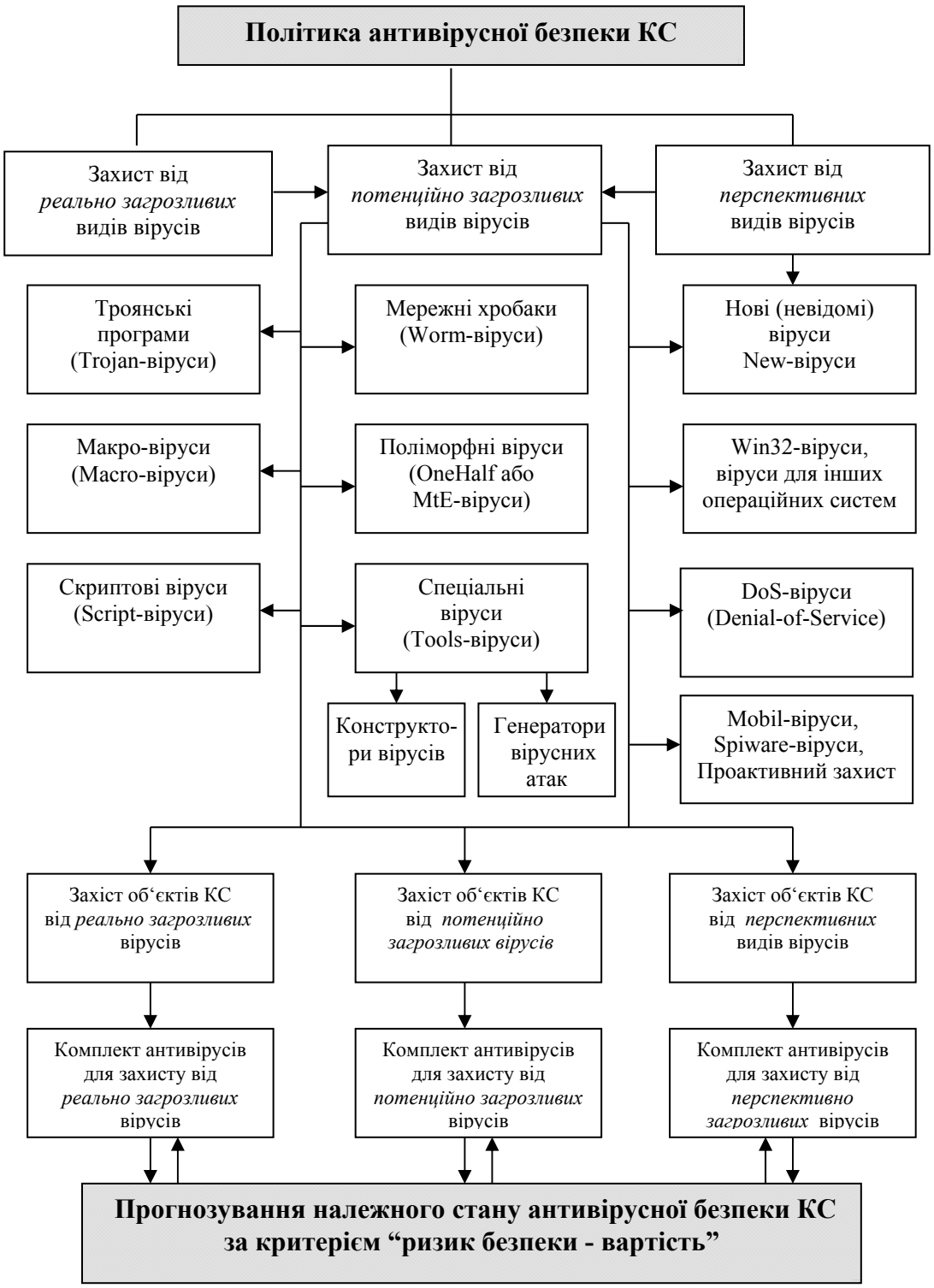


**Рисунок 1 – Модель політики антивірусної безпеки КС**

Аналогічно співвідношенню (1) оцінюється ризик антивірусної безпеки від атак Linux-вірусів Rlin, мережних хробаків Rwrm, троянських програм Rtro, макро-вірусів Rmac, скриптових вірусів Rskr, спеціальних вірусів Rtls, поліморфних вірусів Rmte, DoS-вірусів Rdos, нових невідомих вірусів Rnew, мобільних вірусів Rmob.

Таким чином, згідно з (1) прогнозується ризик антивірусної безпеки кожного об‘єкту КС вибором антивірусів та їх кількості в антивірусному комплекті згідно з даними табл. 2, а також за новими довідковими даними табл. 3 – 6 [1]. Такі довідкові таблиці мають регулярно доповнюватись та уточнюватись.

Вартість антивірусу оцінюється окремо при її наявності у довідкових таблицях за результатами тестових випробувань (наприклад, табл.2), а також за іншими даними (аналітичні та статистичні огляди провідних журналів і видань, прайси тощо).

Таблиця 2 – Можливості антивірусних програм світових брендів

| Найменування антивірусної програми | Розробник (країна) | Постачальник | Вартість (доларів) | Сканування електронної пошти (да/ні) | Час сканування вірусів (хвилин) | Відсоток розпізнаних вірусів (Pn) |
|---|---|---|---|---|---|---|
| KAV Personal Pro 4.0.5.37 | Лабораторія Касперсь-кого | компанія “ЦЕБІТ” | 69 | да (мережний антивірус) | 11.4 | 99 % (0.99) |
| McAfee VirusScan 7.02.6000 | Network Associates Technology | компанія “ЦЕБІТ” | 64 | да (мережний антивірус) | 7.08 | 95 % (0.95) |
| RAV AntiVirus Desktop 8 | GeCAD Software (Румунія) | Через Веб-сайт виробника | 29 | да (мережний антивірус) | 6.85 | 94 % (0.94) |
| PandaAntivirus Platinum 7.04.00 | Panda Software | Через Веб-сайт виробника | 75 | да (мережний антивірус) | 4.5 | 90 % (0.9) |
| PCcillin 2003 | Trend Micro (Китай) | компанія “ЦЕБІТ” | 55 | да (мережний антивірус) | 11.75 | 87 % (0.87) |
| NAV Antivirus 2003 Version 9.00.40 | Symantec | компанія “ЦЕБІТ” | 45 | да (мережний антивірус) | 10.01 | 82 % (0.82) |
| DrWeb for Windows Version 4.29b | ЗАО “ДіалогНаук а” | компанія “ЦЕБІТ” | 66 | да (мережний антивірус) | 7.04 | 81 % (0.81) |
| UNA 1.61.0.97 | Український націон. центр | Український націон. центр | 25 | да (мережний антивірус) | 4.2 | 72 % (0.72) |
| AVG 6.0 AntiVirus System | GriSoft Inc. (Чехія) | Через Веб-сайт виробника | 40 | да (мережний антивірус) | 12.2 | 52 % (0.52) |

5. **Ризик антивірусної безпеки усієї КС** певної конфігурації Rкс забезпечується вибором певних антивірусів та їх кількості в антивірусному комплекті для кожного із об‘єктів КС за співвідношеннями:

$$Pкс = 1 - \prod_{i=1}^{No} (1 - Pio), \tag{2}$$

$$Pio = \prod_{n=1}^{Nio} (1 - Pn), \tag{3}$$

$$Rкс = 1 - Pкс, \tag{4}$$

де No – кількість захищуваних об‘єктів КС;

i – порядковий номер оцінюваного об‘єкту антивірусного захисту КС;

Nio – кількість антивірусів для захисту і-го об‘єкта КС;

Pкс – імовірність виявлення та знешкодження вірусів для усієї КС;

Pio – імовірність виявлення та знешкодження вірусів для і –го об‘єкту КС;

Pn – відомий показник згідно формули (1);
Rкс – ризик антивірусної безпеки КС.

6. **Надаються практичні рекомендації** щодо порядку (прикладів) експертної кількісної оцінки ступеню забезпечення заданого стану антивірусної безпеки КС з використанням певної множини AVS-правил та їх аналітичних і математичних співвідношень залежно від видів вірусів, об'єктів захисту від них та конфігурації оцінюваної КС. Множина AVS-правил постійно доповнюється адміністратором безпеки та службою захисту КС. Надалі надаються правила **AVS-1…5** з практичними прикладами розрахунків щодо нового методу апріорі-прогнозування можливого стану антивірусної безпеки КС.

**Зауваження:** за AVS-правилами прогнозується тільки апріорі "можливий" стан антивірусної безпеки КС з ризиком не більш заданого.

**Правило AVS-1. Л**окальна обчислювальна мережа установи (КС класу 2, тобто локальна обчислювальна мережа) складається з п'яти ПЕОМ/робочих станцій та одного серверу. Оцінити можливий ризик антивірусної безпеки такої КС при наданні відповідних послуг комплектів антивірусів для кожного із об'єктів захисту КС за умови – заданий ризик від атак мережних хробаків не більш 0.01 %.

1. Спочатку оцінюємо ризик антивірусної безпеки визначених об'єктів конфігурації КС, тобто для кожної із п'яти ПЕОМ/робочих станцій (РС) та серверу локальної мережі за таких умов:

- для антивірусного захисту кожної із п'яти РС використовується мережний антивірус KAV Personal Pro версії 4.0.5.37 (Pn = 0.99, табл. 2);
- для антивірусного захисту серверу використовуються мережні антивіруси KAV Personal Pro версії 4.0.5.37 (Pn = 0.99) та McAfee VirusScan 7.02.6000 (Pn = 0.95).

2. Згідно з формулами (1) та (3), а також даними табл. 2 отримуємо (за умови N1o = N2o = N3o = N4o = N5o = 1, N6o = 2):

$$P1o\ (\text{РС №1, worm-вірус}) = 1 - (1 - 0.99) = 0.99,$$
$$P2o\ (\text{РС №1, worm-вірус}) = 1 - (1 - 0.99) = 0.99,$$
$$P3o\ (\text{РС №1, worm-вірус}) = 1 - (1 - 0.99) = 0.99,$$
$$P4o\ (\text{РС №1, worm-вірус}) = 1 - (1 - 0.99) = 0.99,$$
$$P5o\ (\text{РС №1, worm-вірус}) = 1 - (1 - 0.99) = 0.99,$$
$$P6o\ (\text{сервер, worm-вірус}) = 1 - (1 - 0.99)(1 - 0.95) = 0.9995,$$
$$Pкс = 1 - (1 - P1o)(1 - P2o)(1 - P3o)(1\text{-}P4o)(1 - P5o)(1 - P6o) =$$
$$= 1 - (1 - 0.99)(1 - 0.99)(1 - 0.99)(1 - 0.99)(1 - 0.99)(1 - 0.94) = 0.999999999994,$$
$$Rкс = 1 - Pкс = 1 - 0.999999999994 = 0.000000000006 << 0.01\ \%.$$

**Правило AVS-2.** Об'єктом захисту від макро-вірусів визначається одна ПЕОМ/робоча станція КС. Оцінити можливий ризик антивірусної безпеки такого об'єкту КС при наданні відповідних послуг робочих комплектів антивірусів за умови – належний ризик від атак макро-вірусів - не більш 0.05 %.

1. Спочатку оцінюємо імовірність виявлення та знешкодження макро-вірусів за таких умов:

- варіант 1 – для антивірусного захисту ПЕОМ/робочої станція КС використовується антивірус KAV Personal Pro версії 4.0.5.37 (Pn = 0.99, табл. 2);
- варіант 2 – для антивірусного захисту ПЕОМ/робочої станція КС використовується вітчизняний антивірус UNA 1.61.0.97 (Pn = 0.72, табл. 2);

2. Згідно з формулами (1) та (3), а також за даними табл. 6 отримуємо (за умови N1o = 1):

$$Pпеом = 1 - (1\text{-}\ 0.99) = 0.99,$$
$$Rпеом = 1 - Pпеом = 1 - 0.99 = 0.01 (\text{варіант 1}),$$
$$Pпеом = 1 - (1 - 0.72) = 0.72,$$
$$Rпеом = 1 - Pпеом = 1 - 0.72 = 0.28\ (\text{варіант 2}).$$

Таким чином, використання вітчизняної антивірусної програми UNA 1.61.0.97 не забезпечує належний ризик антивірусної безпеки (не більше 0.05%). Необхідно використовувати тільки антивірусні програми KAV Personal Pro версії 4.0.5.37 (Pn = 0.99, табл. 2) або McAfee VirusScan 7.02.6000 (Pn = 0.95, табл. 2).

**Правило AVS-3.** Об'єктом захисту від мережних хробаків (наприклад, від мережного електронного вірусу-шпигуна Sircam) є одна робоча станція локальної мережі Інтранет. Оцінити ризик антивірусної безпеки Rpc такого об'єкту Інтранет за умови – допустимий ризик від атак мережного електронного вірусу-шпигуна Sircam - не більше 0.01 %.

1. Спочатку оцінюємо імовірність виявлення та знешкодження атак електронного вірусу-шпигуна Sircam за умов:

- варіант 1: для антивірусного захисту робочої станції Інтранет використовується мережний антивірус KAV Personal Pro версії 4.0.5.37 (Pn = 0.99, табл. 2);
- варіант 2: для антивірусного захисту робочої станції Інтранет використовується мережний

вітчизняний антивірус UNA 1 .f 1.0.97 (Pn = 0.72, табл. 2).

2. Згідно з формулами (1) та (3), а також за даними табл. 6 отримуємо (за умови, що N1o = 1):

Ppc =1 – (1- 0.99)=0.99,

Rpc =1 – Ppc =1 – 0.99 =0.01 (варіант 1),

Ppc =1 – (1 – 0.72)=0.72,

Rpc = 1 – Ppc = 1 – 0.72 = 0.28 (варіант 2).

Таким чином, використання вітчизняної антивірусної програми UNA 1.61.0.97 не забезпечує належний ризик антивірусної безпеки (не більше 0.01%), необхідно використовувати тільки антивіруси, які мають показник Pn =/> 0.99, наприклад, це тільки мережний антивірус KAV Personal Pro версії 4.0.5.37 (Pn = 0.99, табл. 2).

**Правило AVS-4.** Згідно з статистикою вірусних атак на мережі Інтранет визначено, що найбільш небезпечними є два шляхи їх зараження комп'ютерними вірусами (два можливі канали вірусних атак) – електронна пошта і завантаження файлів з Інтернет (до 80%) [4]. Локальна обчислювальна мережа організації має постійне з'єднання з Інтернетом, у своєму складі вона має один сервер і 10 робочих станцій. Надати пропозиції щодо складу антивірусного комплекту для кожної робочої станції і серверу за умови, що ризик їхнього антивірусної безпеки від вірусних атак по каналам електронної пошти повинен бути: для робочих станцій - не більше 0.01 %, для серверу – не більше 0.0001%. Пошук рішення здійснюється в два етапи.

1. Перший етап – це аналіз можливостей антивірусів для виявлення та знешкодженні вірусів електронної пошти (табл. 1 – 6). З ними здатні боротися усі мережні антивіруси. Для цього треба оцінювати, насамперед, значення показника Pn, наведеного в табл. 1 – 6. Чим більше значення він має, тим краще. Одночасно треба звертати увагу на вартість антивірусу. Пропонувати можна тільки комплект антивірусів, який для надійності роботи повинен включати в себе більше одного антивірусу та з найбільш потужним, тобто з найбільш широким арсеналом захисту від загрозливих для даної мережі Інтранет видів вірусів.

2. Другий етап – вибір складу комплектів антивірусів. Вибирати доцільно тільки ті комплекти, які здатні виявляти і знешкоджувати віруси електронної пошти з ризиком безпеки, не більше заданого та найменш дорогі, тобто за критерієм "ризик антивірусної безпеки – вартість". Експертну оцінку можна здійснювати за формулою (1) для мережних хробаків.

Так, за правилами AVS-4.1 – AVS-4.4 можна визначити декілька варіантів складу комплектів антивірусів для заданої захищеності робочих станцій та серверу мережі Інтранет:

**Правило AVS-4. 1.** Комплект з одного антивірусу KAV Personal Pro версії 4.0.5.37. (Pn = 0.99, табл. 2). Ризик антивірусної безпеки за формулою (1) дорівнює (N=1):

$$Rwrm = \prod_{n=1}^{N} (1 - Pn) = 1 - 0.99 = 0.01.$$

2. **Правило AVS-4. 2.** Комплект з антивірусу KAV Personal Pro 4.0.5.37 (Pn = 0.99) та антивірусу McAfee VirusScan 7.02.6000 (Pn = 0.95). Ризик антивірусної безпеки за формулою (1) дорівнює (N=2):

$$Rwrm = \prod_{n=1}^{N} (1 - Pn) = (1 - 0.99)(1 - 0.95) = 0.0005.$$

3. **Правило AVS-4. 3.** Комплект з антивірусу KAV Personal Pro версії 4.0.5.37 (Pn = 0.99), антивірусу McAfee Vi usScan 7.02.6W) (Pn = 0.95) та антивірусу DrWeb for Windows Version 4.29b (Pn = 0.81). Ризик антивірусної безпеки за формулою (1) дорівнює (N=3):

$$Rwrm = \prod_{n=1}^{N} (1 - Pn) = (1 - 0.99)(1 - 0.95)(1 - 0.81) = 0.000095.$$

4. **Правило AVS-4. 4.** Комплект з антивірусу KAV Personal Pro версії 4.0.5.37 (Pn = 0.99), антивірусу McAfee VirusScan 7.02.6000 (Pn = 0.95) та з вітчизняного антивірусу UNA 1.61.0.97(Pn = 072).

Ризик антивірусної безпеки за формулою (1) дорівнює (N=3):

$$Rwrm = \prod_{n=1}^{N} (1 - Pn) = (1 - 0.99)(1 - 0.95)(1 - 0.72) = 0.00014.$$

Таким чином, для сервера Intranet можна пропонувати комплект антивірусів за правилом AVS-4.3, а для робочих станцій підходять комплекти антивірусів за правилами AVS-4.1- AVS-4.4. Але за критерієм "ризик антивірусної безпеки не більш заданого" для робочих станцій заданим вимогам задовольняє тільки комплект антивірусів, вибраний за правилом AVS-4.1.

Наведені вище приклади практичних розрахунків (правила AVS-1…AVS-4) показали працездатність

запропонованого методу прогнозування антивірусної безпеки. Але довідкові таблиці результатів тестування антивірусів необхідно регулярно доповнювати новими версіями та новими антивірусними програмами. Нижче за даними [1] надаються чотири спеціально підготовлені довідкові таблиці за останніми на 2006 р. результатами тестувань антивірусів світових брендів.

В цих таблицях наведено відсоток так званого детекту, тобто виявлення і розпізнавання комп'ютерних вірусів, з різної їх тестової множини (тестових іспитів 551.795 вірусів в табл. 5, аналогічно тестових іспитів 174.184 вірусів в табл. 6, а також основний розрахунковий, за співвідношеннями (1) – (4), табличний показник Pn понад 40 найбільш популярних антивірусних програм світових брендів. Запропонований метод прогнозування антивірусної безпеки комп'ютерних систем і мереж надає можливість їх адміністраторам безпеки, користувачам та власникам своїм рішенням формувати низку AVS-правил.

Таблиця 3 – Можливості антивірусних програм світових брендів

| №/№ | Найменування антивірусної програми | Відсоток розпізнаних вірусів (Pn) |
|---|---|---|
| 1 | Avasti 4.6.691 Pro | 91.06%% (0.91) |
| 2 | AVG Pro 7.0.338 | 87.44 % (0.87) |
| 3 | Bit-Defender AV 8.0.200 | 97.34 % (0.97) |
| 4 | Dr.Web AV for Win 95-XP 4.32b | 92.47 % (0.92) |
| 5 | Esed Nod32 2.51.8 | 98.31 % (0.98) |
| 6 | F-Prot AV for Win 3.16c | 95.83 % (0.96) |
| 7 | H+B EDV AV Pro 6.31.00.03 | 93.63 % (0.94) |
| 8 | Kaspersky AV Personal Pro 5.0.372 | 99.88 % (0.998) |
| 9 | McAffee Virus Scan 10.0.21 | 98.19 % (0.98) |
| 10 | Semantec Norton AV 11.0,11.4 | 99.41 % (0.99) |
| 11 | Sophos AV 5.0 | 89.12 % (0.89) |
| 12 | Trend Micro Internet Sequrity 12.1.1034 | 91.25 % (0.91) |

Таблиця 4 – Можливості антивірусних програм світових брендів

| №/№ | Найменування антивірусної програми | Відсоток розпізнаних вірусів (Pn) |
|---|---|---|
| 1 | Avira AntiVir PE Premium | 99.03 % (0.99) |
| 2 | G DATA Security AntiVirusKit (AVK)* | 99.04 % (0.99) |
| 3 | Allwill Software Avasty Professional | 94.03 % (0.94) |
| 4 | GriSoft AVG Professional | 91.02 % (0.91) |
| 5 | Softwin BitDefender Professional+ | 96.02 % (0.96) |
| 6 | Dr.Web | 92 % (0.92) |
| 7 | Frisk Software F-Prot Anti-Virus | 92.01% (0.92) |
| 8 | F-Secure Anti-Virus* | 99.02 % (0.99) |
| 9 | Kaspersky Anti-Virus | 99.02 % (0.99) |
| 10 | MacAfee VirusScan | 95.02 % (0.95) |
| 11 | ESET NOD32 Anti-Virus | 98.08 % (0.98) |
| 12 | Norman ASA NormanVirusControl | 94.08 % (0.94) |
| 13 | Symantec Norton Anti-Virus | 98.04 % (0.95) |
| 14 | AEC TrustPort AV WS* | 98.08 % (0.98) |

Таблиця 5 – Можливості антивірусних програм світових брендів

| №/№ | Найменування антивірусної програми | Відсоток розпізнаних вірусів (Pn) |
|---|---|---|
| 1 | Avir 7.01.01.02 Premium | 95 % (0.95) |
| 2 | Avast 4. 7.871 Professional | 87 % (0.87) |
| 3 | AVG 7,1. 405 Professional | 82 % (0.82) |
| 4 | GriSoft AVG Professional | 91.02 % (0.91) |
| 5 | Bit-Defender 9 Professional | 95 % (0.95) |

| | | |
|---|---|---|
| 6 | Dr.Web 4.33.2 | 85 % (0.85) |
| 7 | E-Trust 7.2.0.0 | 50 % (0.5) |
| 8 | F-Port 3.16f | 84 % (0.84) |
| 9 | F-Secure 2006 6.1290 | 95 % (0.95) |
| 10 | Kaspersky 6.0.0.303 | 98. % (0.98) |
| 11 | MacAfee10.0.27 | 92 % (0.92) |
| 12 | Nod32 2.51.30 | 94 % (0.94) |
| 13 | Norman 5.90.23 | 84 % (0.84) |
| 14 | Norton 2006 Professional | 82 % (0.82) |
| 15 | Panda 2007 2.00.01 | 80 % (0.8) |
| 16 | Sophos Sweep 6.0.2 | 67 % (0.67) |
| 17 | Ukrainan National Antivirus 1.83 | 75 % (0.75) |

Таблиця 6 – Можливості антивірусних програм світових брендів

| №/№ | Найменування антивірусної програми | Відсоток розпізнаних вірусів (Pn) |
|---|---|---|
| 1 | Avasti 4.6.691 Pro | 91.06% (0.91) |
| 2 | AVG Pro 7.0.338 | 87.44% (0.87) |
| 3 | Bit-Defender AV 8.0.200 | 97.34% (0.97) |
| 4 | Dr.Web AV for Win 95-XP 4.32b | 92.47% (0.92) |
| 5 | Esed Nod32 2.51.8 | 98.31% (0.98) |
| 6 | F-Prot AV for Win 3.16c | 95.83% (0.96) |
| 7 | H+B EDV AV Pro 6.31.00.03 | 93.63% (0.94) |
| 8 | Kaspersky AV Personal Pro 5.0.372 | 99.88% (0.998) |
| 9 | McAffee Virus Scan 10.0.21 | 98.19% (0.98) |
| 10 | Semantec Norton AV 11.0,11.4 | 99.41% (0.99) |
| 11 | Sophos AV 5.0 | 89.12% (0.89) |
| 12 | Trend Micro Internet Sequrity 12.1.1034 | 91.25% (0.91) |

## III Висновки

1. Запропонований метод прогнозування антивірусної безпеки комп'ютерних систем і мереж певної конфігурації і призначення може бути корисним для адміністраторів безпеки, користувачів та власників, адже кількісна експертна оцінка можливого ризику антивірусної безпеки завжди не зайва і навіть необхідна як один із важливих і пріоритетних факторів безпеки.

2. Наведена множина довідкових таблиць 1 – 6 та варіантів практичних розрахунків ризику антивірусної безпеки за правилами AVS-1…AVS-4 свідчить, що їх треба регулярно доповнювати новими версіями антивірусів, використовувати кращий досвід боротьби з вірусними атаками в комп'ютерних системах і мережах в Україні.

*Література: **1.** Шорошев В. В., Слободанюк А. А., Тихонов В. Г. Антивирусная безопасность: состояние, проблемы, перспективы, рекомендации. Бизнес и безопасность № 1, 2007. **2.** Шорошев В. В. та інші. Класифікація комп'ютерних вірусів і основи захисту від них. Журнал "Бизнес и безопасность" № 2, 1999 г. **3.** Шорошев В. В. та інші. Антивирусная защита вашей ПЭВМ. Журнал "Бизнес и безопасность" № 6, 1999 г. **4.** Шорошев В. В. Основи формування політики безпеки комп'ютерних систем. Наукове видання. Бизнес и безопасность, К., 2006. – с.141, іл. **5.** А. Ю. Ільніцький, В. В. Шорошев, І. Л. Близнюк. Монографія "Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах органів внутрішніх справ України" (шифр "Торсіон-1"). Свідоцтво Державного департаменту інтелектуальної власності Міносвіти і науки України про реєстрацію авторського права на твір № 14446 від 20. 11. 2005 у вигляді програмного продукту "Торсіон-1". – К.: Видавництво НАВСУ, 2003р. – 316 с.*