де s_{h-1}, s_h – обмеження на N таке, що $s_{h-1} < N \le s_h$, $s_h = \sum_{i=0}^{h} C_n^i$.

Враховуючи (2), (4), (7) та за умови, що $P_2 = 1$ (див. (2)) буде справедливе

Твердження 2. Достовірність результату направленого перебору ключів одноразового блокноту дорівнює

$$P \approx \Phi\left(\frac{2h - n(1-2\delta)}{\sqrt{n(1-4\delta^2)}}\right) - \Phi\left(-\sqrt{\frac{n(1-2\delta)}{1+2\delta}}\right) + Lp^{h+1}q^{n-h-1}\left(1 - \frac{1}{4k\varepsilon^2}\right), \qquad (12)$$

де: n – довжина ключа одноразового блокноту; $0 \le h \le n$; $L = V - \sum_{l=0}^{h} C_n^l$; $\sum_{l=0}^{h} C_n^l \le V \le \sum_{l=0}^{h+1} C_n^l$; V – кількість опробувань ключа; ε – задане відхилення для p; $k(k < s)$ – кількість відомих елементів чистої гами, що вибирається з *s* елементів шифртексту різних шифртелеграм.

Слід зазначити, що в результаті направленого перебору ключів у більшості випадків буде отримано декілька можливих відкритих текстів і всі вони матимуть достовірність *P*. Питання вибору критерію відкритого тексту з величиною $P_2 = 1$ є окремою науковою задачею.

Висновки

Підсумовуючи сказане, звернемо увагу на те, що класичний метод оцінки криптографічної стійкості практичних реалізацій шифру одноразового блокноту э процедурою статистичного тестування генератора ключових даних з метою перевірки виконання вимог критерія теоретичної стійкості (1).

Запропонований же в статті метод дозволяє оцінювати параметри стійкості одноразових блокнотів при відсутності фізичного доступу до генераторів ключів.

Література: ***1.*** *Шеннон К. Работы по теории информации и кибернетике/ Пер. с англ. Под ред. Н. А. Железнова. – М.: ИЛ, 1963. – 35 с.* ***2.*** *Зубов А. Ю. Совершенные шифры. М.: "Гелиос АРВ" 2003. - 54 с.* ***3.*** *Ковальчук Л. В., Мельник С. В., Бездетный В. Т. Вероятностные характеристики схем генерации ключей с неравновероятным распределением. "Радиотехника".Харьков: 2005, т. 140 - 23с.*

УДК 681.3

ЕКСПЕРТНА КІЛЬКІСНА ОЦІНКА АНТИВІРУСНОЇ БЕЗПЕКИ КОМП'ЮТЕРНИХ СИСТЕМ

Вячеслав Шорошев
НДІ НАВС України

Анотація: **Надаються рекомендації щодо антивірусного захисту корпоративних комп'ютерних мереж Intranet, методів експертної кількісної оцінки антивірусної безпеки від потенційно загрозливих видів комп'ютерних вірусів та пропонується модель політики антивірусної безпеки комп'ютерних систем.**

Summary: **The recommendations concerning anti–virus protection of corporate computer networks Intranet are given, of methods of an expert quantitative estimation of anti–virus safety from potentially me nacing kinds of computer viruses and the model of politics of anti–virus safety of computer systems is offered.**

Ключові слова: **Антивірус, антивірусна безпека, політика антивірусної безпеки, ризик антивірусної безпеки.**

І Вступ

Проблема антивірусного захисту все більше стає не тільки актуальною, але й обов'язковою компонентою забезпечення безпеки комп'ютерних систем (КС).

З моменту появи першого комп'ютерного вірусу пройшло вже кілька десятків років, з тих пірважливість цієї проблеми не тільки не зменшилась, але навпаки, значно збільшилась. Комп'ютеризація призвела не тільки до інформатизації суспільства, але і до поширеності вірусної інфекції.

Хоча вірусні атаки в комп'ютерних системах будуть завжди, застосування деяких рекомендацій і

правил дозволить звести можливу вірусну загрозу до мінімуму.

По–перше, для захисту корпоративних комп'ютерних мереж Інтранет (ККМ) та усунення небезпеки вірусного зараження сервера варто обмежити права користувачів при роботі з файлами на дисках сервера.

По–друге, рекомендується використовувати комплект антивірусних пакетів різних виробників – наприклад, один з них СНД-продукт, другий – західних країн [7, 8, 9]. Причому продукти одного з виробників необхідно установити на сервері, другого – на робочих станціях мережі Інтранет.

По–третє, дистрибутивні копії програмних продуктів краще купувати у офіційних продавців. При цьому значно знижується імовірність вірусного зараження, хоча відомі випадки купівлі інфікованих дистрибутивів. Навіть завантаження файлів з Ваб-ресурсів відомих компаній нічого не гарантує. Наприклад, на сервері Microsoft досить довгий час знаходився документ, уражений макровірусом Wazzu [9].

З популяризацією ОС Linux почали мусуватися слухи про можливі епідемії вірусів у цьому середовищі. Проте, цього поки що не трапилося. Одна з причин — дистрибутиви Linux випускаються багатьма виробниками, і вони не завжди є цілком сумісними між собою. У підсумку вірус, написаний під використання бібліотек визначеного дистрибутива Linux, буде нешкідливим у подібних продуктах інших розроблювачів, де ця бібліотека відсутня.

Цей фактор плюс слабка поширеність цієї ОС посприяли тому, що для цієї ОС створено поки одиничні віруси. Схожа ситуація склалася і з мобільними телефонами. Відомі випадки розсилання шкідливих SMS, однак через те, що віруси спрацьовували тільки на певних терміналах (які використовують один тип мікропрограм), ця проблема не переросла в глобальну.

Дуже актуальним є питання – як встановити все-таки – коли комп'ютер інфікований? Якщо ваш ПК поводиться незвичайно (підозріло повільно працює, прикладення не запускаються, на жорсткому диску без вашого відома вилучається інформація), то можлива причина – зараження вірусом. Тому скористайтеся антивірусною програмою для виявлення і знешкодження вірусу, попередньо обновивши антивірусні бази.

До повної перевірки комп'ютера необхідно максимально обмежити до нього доступ. Відключити його від локальної мережі, не переписувати з нього інформацію на інші комп'ютери і не запускати прикладення (крім антивірусних пакетів).

Якщо антивіруси нічого не знайшли, але підозра про інфікованість комп'ютера залишилася, зверніться безпосередньо до виробника антивірусного продукту – можливо, вам "повезло" і ви знайшли новий вірус.

Який же засіб вибрати для захисту від вірусної атаки? Це і складне, і просте питання. Огляд і аналіз результатів тестування традиційних і нових антивірусів різних країн, проведені ентузіастами антивірусного захисту на сторінках популярних журналів, а також спроба дати кількісну оцінку ступеню антивірусного захисту/антивірусної безпеки можуть значно допомогти в організації захисту комп'ютерних систем (КС) від вірусних атак [7 – 9].

II Основна частина

Пропонується наш погляд на найбільш поширені основи побудови системи антивірусної безпеки в корпоративних комп'ютерних мережах Інтранет. При цьому під Інтранет розуміється корпоративна локальна обчислювальна мережа, що має постійне або термінове підключення до Інтернет [11].

Отже, розглянемо низку принципових підходів та правил, яких необхідно дотримуватись при формуванні політики антивірусної безпеки корпоративної комп'ютерної мережі Інтранет.

По–перше, кінцевий користувач не може приймати участі в антивірусному захисті мережі. Адже він зможе відкрити дірку для проникнення вірусів в Інтранет, попросту відключивши антивірусне програмне забезпечення (АПЗ) на своєму комп'ютері/робочій станції/сервері тощо.

По–друге, керування системою антивірусного захисту має бути централізованим. Це знизить витрати на адміністрування взагалі і підвищить ефективність захисту.

По–третє, система захисту має бути багаторівневою і не охоплювати лише один сегмент корпоративної мережі Інтранет. Наприклад, встановлювати антивірус на шлюз і не давати співробітникам можливості використовувати на роботі зйомні носії інформації. Однак при пересиланні електронною поштою зашифрованого чи заархівованого файлу, закритого паролем, останній не перевіряється антивірусною програмою (у залежності від настроювань вона або пропускає файл, не перевіривши, або не пропускає його, що змушує користувача звертатися до адміністратора).

Тому для корпоративних мереж Інтранет, комерційних і державних структур пропонується використовувати трирівневу систему антивірусного захисту.

Рівень перший: *захист від вірусів HTTP–, FTP– і SMTP–шлюзів* (фільтрація всього поштового і Internet-трафика). Більшість вірусів буде відтинатися вже на цьому етапі.

Рівень другий: *захист файлових серверів і серверів корпоративної електронної пошти* (наприклад,

Microsoft Exchange Server, Lotus Notus). Крім факту наявності АПЗ на сервері, необхідно висунути ще одну вимогу – робота антивірусного монітора в резидентному режимі з контролем усіх файлів, що записують і редагують на сервері.

Рівень третій: *захист робочих станцій.* Тут бажаний також антивірусний монітор, але при низькій продуктивності комп'ютерів можна обійтися й антивірусним сканером, що буде запускатися один раз у день. На цьому рівні будуть виявлятися віруси в зашифрованій пошті, а також заархівjвані з паролем файли, що прийшли з Інтернет–Мережі.

Завжди необхідно також пам'ятати про *відновлення вірусних баз.* За підрахунками розроблювачів АПЗ, щотижня у світі з'являється до 300 нових вірусів. Якщо якась частина з них буде виявлятися евристичним аналізатором антивірусної програми, то інша безперешкодно проникне в систему. Більше того, частота відновлень є одним із критеріїв при виборі АПЗ (купівля ж неліцензійного АПЗ — рішення, що має сумнівну цінність при захисті корпоративної інформації).

Нарешті, *вибірково–адаптивна технічна підтримка АПЗ.* Універсального антивірусного захисту на сьогодні не існує і воно навіть неможливе (захист завжди конкретний під об'єкт, загрозу, АПЗ, ефективність, вартість). Вибір залежить від топології конкретної мережі, граничних витрат, необхідного рівня захисту тощо. Фахівці сторонньої організації можуть надати кваліфіковану допомогу при установці АПЗ, настроюванні роботи системи антивірусної безпеки і відновленні антивірусних баз. До того ж є і можливість організації пілотного проекту (у тому числі і сертифікація), навчання адміністратора. Перераховані вище задачі найчастіше може вирішувати лише структура, що спеціалізується в питаннях безпеки Інтранет.

Щодо захисту від вірусних і хакерських атак. Якщо порівняти збиток, заподіяний у даний час українським комерційним і державним структурам вірусами і хакерами, то останні в цьому "змаганні" явно програють. Причина не в ефективному захисті цих вітчизняних структур, а в тім, що Україна, з ряду причин, знаходиться поки ще на перших етапах реалізації сучасних інформаційних технологій захисту, хоча наші пакети НД ТЗІ Департаменту СТСЗІ СБ України не поступаються аналогічним західним.

Але нас практично не торкаються інформаційні війни, а Web-сервери і локальні мережі українських компаній і організацій — занадто дрібна дичина для Internet-злочинців і хуліганів: ні грошей, ні слави. Інша справа віруси. Для них не існує кордонів і рангів, домашній ПК "будь-якого пана Миколи" є не менш ласим шматочком, чим корпоративний сервер General Motors.

Якщо заглянути за наш західний кордон, то можна побачити, що бешкетують віруси і там, але частка невірусних атак істотно вище. Там більше, отже, і увага до такої ситуації і відповідної постановки задач безпеки від них. Закупівля ж різнорідного АПЗ для закриття кожної дірки в системі захисту неефективна і, врешті решт, невигідна. І що оптимальним на сьогоднішній день є поки що вибір комплексних рішень, які враховують складний зв'язок між об'єктами ККМ і здатні адаптуватися під конкретну її конфігурацію для забезпечення максимальної захищеності інформаційних ресурсів за критерієм "ефективність-вартість". Тому в більшості випадків тільки грамотно побудована, комплексна, інтегрована антивірусна система захисту здатна врахувати такі аспекти, як захист від загроз порушення конфіденційності, цілісності, доступності і спостереженості інформації ККМ від вірусних і хакерських атак.

Які ж технології використовуються для побудови таких комплексних систем захисту інформації Інтранет від загроз ззовні й із свого середовища? Розглянемо найбільш узагальнену класифікацію цих загроз для Інтранет.

З одного боку, загрози варто розподілити на *локальні і видалені.* Локальні загрози не залежать від підключення комп'ютера до мережі, у той час як видалені використовують для атак недоліки в проектуванні і реалізації мережних рішень. Методи захисту, що використовуються в першому і другому випадках, часто збігаються, але все-таки досить різні, щоб виправдати розподіл.

З іншого боку, загрози можна поділяти на *навмисні і випадкові.* До першої категорії відносяться ті загрози, реалізація яких зв'язана з певними злочинними діями, до другої ж – ті, котрі можуть здійснюватися спонтанно і можливі через низьку якість програмного чи апаратного забезпечення. Яскравий приклад — нестабільна робота на етапах реалізації брендів і софтів Біла Гейтса, наприклад MS Windows 95, саме з цієї операційної системі почалася інформатизація України.

Почнемо з *локальних* випадкових загроз. До таким відносяться збої в роботі апаратних засобів, проблеми апаратної і програмної сумісності, неефективне використання системних ресурсів. Останнє відноситься до загроз з тієї причини, що сповільнює роботу ККМ, збільшуючи час доступу до інформації і, таким чином, являє собою загрозу доступності. Більш того, продуктивна робота всієї системи захисту прямо залежить від ефективності використання інформаційних ресурсів.

Наприклад, якщо персонал, відповідальний за антивірусний захист, із причин перевантаження мережних з'єднань чи нестабільної роботи сервера не одержить вчасно повідомлення про виявлення

симптомів вірусної епідемії, збиток істотно перевищить ті засоби, яких вистачило б для запобігання подібній ситуації.

Захистом від локальних спонтанних загроз є засоби діагностики і системні утиліти, такі як Checkit, Norton Utilities, McAfee Tools тощо. Вони надають широкий спектр послуг з діагностики і рішення проблем.

Однак усі вони мають істотний недолік – вони локальні. Як буде видно надалі, ключовим фактором ефективного застосування тієї чи іншої технології антивірусного захисту в Інтранет є централізація засобів керування.

Локальні навмисні загрози незаслужено забуті у світлі загальною метушнею і галасом, піднятих навколо мережних хробаків і хакерів, здатних через глобальну мережу одержати доступ до будь-якої конфіденційної (корпоративної) інформації. Найчастіше набагато простіше викрасти коштовну інформацію не за допомогою складних видалених маніпуляцій, а шляхом "фізичного" вторгнення і викрадення носіїв. Причому під вторгненням тут варто розуміти не тільки зовнішній несанкціонований доступ, але і доступ нелояльних співробітників, "випадкових" відвідувачів, залишених один на один з активною консоллю, персонал компаній і організацій, що надають послуги щодо обслуговування техніки, а також звичайних електриків, прибиральників і всіх тих, на кого поширюється термін – "техперсонал".

Мабуть єдиним на сьогодняшній день способом уберегти себе від подібного роду атак є засоби захисту (переважно апаратні) від несанкціонованого доступу, подібні Decros Protect, основою для яких служать криптографічні перетворення. Не вдаючись у докладний перелік усіх можливостей таких систем, відзначимо ключові ефекти від їхнього використання.

Без наявності апаратного ключа чи знання паролю користувач не може навіть завантажити комп'ютер. Фізичне викрадення носія інформації безглуздо, оскільки конфіденційні дані зберігаються в зашифрованому вигляді, а ключі, використовувані при шифруванні, знаходяться на персональних зовнішніх носіях (тоукенах). Спеціалізовані захищені протоколи дозволяють здійснювати видалене адміністрування робочих станцій, блокуючи роботу при підозрі на несанкціонований доступ. Більше того, використання вбудованих апаратних реалізацій криптоалгоритмів дозволяє зберегти незмінною швидкість роботи системи, на противагу очікуваному зниженню продуктивності.

Від загроз локальних перейдемо до загроз *видалених.*

Поширеність вірусів і хакерів зумовлений, *в першу чергу*, низькою імовірністю виявлення зловмисника. Компаніям, що постраждали від видалених атак, як правило бракувало навіть комусь виставити позов про відшкодування збитків. А ризик настільки великий, що страхові компанії ще не швидко прийдуть на цей ринок. Вихід із ситуації тільки в застосуванні сучасних технологій захисту, причому не розрізнено, а в комплексі.

У другу чергу, постраждалим невигідно принижувати свій імідж безпеки від постійно діючих і зростаючих вірусних атак.

Сьогодні можна визначити чотири основних підходи до захисту корпоративних комп'ютерних мереж Інтранет.

По-перше, це *фільтрація інформації,* що надходить як ззовні, так і з самої локальної мережі Інтранет. На цьому принципі побудовані так називані міжмережні екрани (брандмауери firewalls). Рішення подібного типу поділяються на програмні й апаратні. Останні дорожчі, але мають більшу продуктивність і тому використовуються переважно як корпоративні *міжмережні екрани* (рис. 1). Вони встановлюються між Internet і корпоративним шлюзом Інтранет, щоб утворити перший рубіж оборони. Це дозволяє відгородити локальну мережу від інформації, що надходить з неблагонадійних адрес Internet, а також запобігти витоку інформації з визначених адрес Інтранет.

Іншою важливою задачею апаратних firewalls є *нейтралізація атак* на відмовлення в обслуговуванні (Denial of Service). Одні з найпростіших з погляду реалізації, ці атаки є й одними із найнебезпечніших. На частку програмних firewalls приходиться, як правило, захист локальних станцій (див. ЧИП 9/2001, с. 96). У великих організаціях використання на всіх робочих станціях персональних firewalls не тільки марнотратно, але і практично даремно, тому що жадає від усіх співробітників певного рівня кваліфікації для підтримки належного рівня захисту. Однак використання єдиної консолі керування дозволяє ефективно вирішити цю проблему із залученням мінімуму додаткових засобів.

Іншим підходом до рішення проблеми видалених атак є усунення причин, що роблять їх здійсненними. Кожна видалена атака використовує одне чи кілька слабких місць у програмному забезпеченні (ПЗ) – *уразливостей.* Отже, для запобігання атакам потрібно усунути останні. Саме цю можливість реалізують *сканери безпеки* (рис. 2). Вони тестують використовуване ПЗ на предмет наявності уразливостей одним з наступних способів:

– визначають версію ПЗ і вказують відомі для цих версій дірки в безпеці, роблять аналіз коду в

пошуках характерних, для деяких уразливостей, ділянок;

– безпосередньо здійснюють видалені атаки і, враховуючи досягнений ефект, судять про наявність слабких місць проти можливих атак НСД.

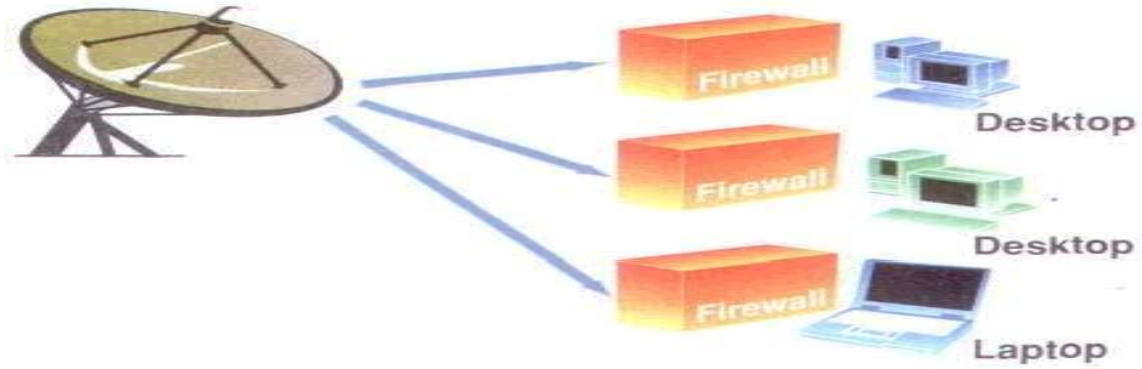

Рисунок 1 – Використання персональних firewalls для видалених станцій

Сканери безпеки надають також докладну інформацію про систему захисту, рекомендації з усунення недоліків і в деяких випадках автоматично ставлять патчи.

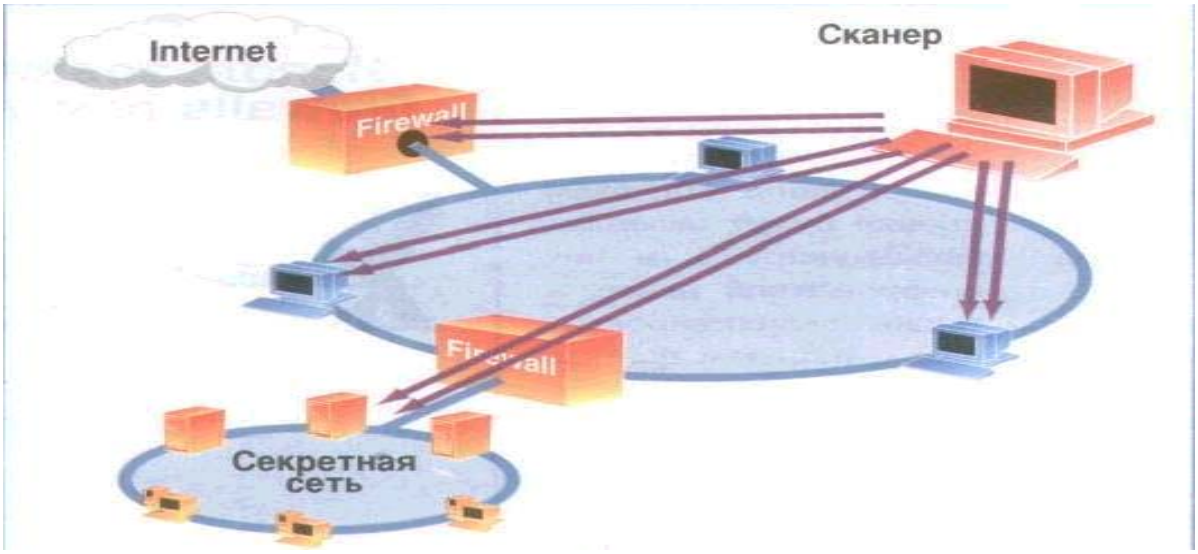

Рисунок 2 – Стандартна схема використання сканера безпеки

Третій підхід заснований на *визначенні атаки за її зовнішніми ознаками.* Працюючі в такий спосіб, монітори безпеки аналізують системні події і транзитні по мережі пакети з метою вчасно виявити підозрілі дії й інформувати про їх персонал Інтранет. Цей підхід пасивний, тобто не здатний протистояти нападу, але є єдиним способом знайти успішну атаку.

Нарешті, ще один метод дозволяє одночасно запобігти негативному ефекту від видаленої атаки і зафіксувати її в момент проведення. Спеціальне програмне забезпечення *емулює працюючу ККМ (оманна ККМ)* із серверами, робочими станціями і маршрутизаторами, створюючи у зловмисника ілюзію успішної атаки (рис. 3). Насправді він намагається атакувати неіснуючі системи, у той час як персонал, що забезпечує безпеку, може відстежити його власну мережну адресу.

На наш погляд, використання запропонованих вище підходів окремо, чи в комплексі робить зовнішню вірусну чи хакерську атаку дуже скрутною.

Таким чином, ми розглянули основи побудови антивірусного захисту на прикладі найбільш поширених корпоративних мереж Інтранет. Вони визначають певні підходи, правила та практичні рекомендації. Але завжди залишається невирішеною вічна проблема – яка ж стійкість побудованого антивірусного захисту, за якими критеріями її оцінити, бажано не якісними, а кількісними. Правила, підходи, заходи антивірусного захисту – це вже щось, але не все. На першому плані стояв захист комп'ютерних систем від атак несанкціонованого доступу.

Будь який захист інформації в КС оцінюється за певними критеріями. На перших кроках

комп'ютеризації міжнародній спільноті провідних країн світу (США, Канада, Англія, Франція, Німеччина, Нідерланди, СРСР, Російська Федерація, Україна) за солідними інвестиційними програмами вистачило понад сімнадцять років (1983–1999 роки), щоб розробити єдині міжнародні та національні критерії комп'ютерної безпеки для експертної оцінки *захищеності від загроз порушення конфіденційності, цілісності, доступності, спостереженості та гарантії безпеки інформації КС.*

Рисунок 3 – Використання фальшивої корпоративної комп'ютерної мережі

Так, від простої універсальної шкали 6–10 узагальнених критеріїв комп'ютерної безпеки (критерії TCSEC, ITSEC) до великої сукупності часткових критеріїв (понад 200 для CCITSE, ISO 15408), 110 часткових критеріїв (НД ТЗІ 2.5–004–99, Україна) – такий шлях розвитку критеріїв безпеки інформації КС від загроз НСД [1–5, 10]. Але й до цього часу відсутні аналогічні критерії експертної оцінки захищеності КС від комп'ютерних вірусів. І це, мабуть, не випадково. Потрібні подальші розробки, дослідження, інвестиції.

Перші спроби експертної кількісної оцінки ефективності антивірусного захисту ПЕОМ було зроблено в роботах [6, 8, 9]. Але до цього визначився і другий напрямок оцінки ефективності антивірусного захисту – оцінювати захист не КС, а можливості захисту самих антивірусів. Так, все більшого поширення серед розробників різних країн і фірм набуває практика тестування самих програм і пакетів антивірусного захисту за певними балами і рейтингами та за певною сукупністю часткових показників функціонування антивірусів. Це вірно, але цього не достатньо.

Поки що зовсім не регламентована і не оцінюється антивірусна безпека КС, наприклад [1, 2], як для захисту від загроз НСД (мінімальний рейтинг захисту від НСД С2/FC2, відносно стійкий B2/FB2 та стійкий B3/FB3 захист від НСД за критеріями TCSEC/ITSEC).

Надалі для формування політики надання послуг антивірусної безпеки КС та експертної оцінки ефективності надання цих послуг пропонуються наступні методичні і критеріальні підходи, правила антивірусної безпеки (anti–virus safety, AVS–правила) та рекомендації. Особливостей цього напрямку безпеки дуже багато.

Так, видів і класифікацій комп'ютерних вірусів існує багато. Але початок покладено в фундаментальних роботах Н. Безрукова, В. Касперськрго, коли була зроблена перша спроба універсальної класифікації комп'ютерних вірусів з визначенням їх сигнатур, дескрипторів, довжини тіла вірусу, сімейств, деструктивних дій і деструктивних ознак тощо. Але для формування політики антивірусної безпеки КС доцільно визначити просту, найбільш узагальнену і доступну для пересічних користувачів класифікацію вірусів. При такому підході доцільно почати з визначення та уточнення певних підходів антивірусного захисту та відповідних термінологічних понять.

По–перше, для формування політики безпеки КС визначаємо складову політику не антивірусного *захисту*, а антивірусної *безпеки*. Поняття "захист" від вірусів передбачає пасивні оборонні дії. Поняття "безпека" передбачає, навпаки, активні оборонні контрдії проти певних загроз. Тому при такій постановці задачі для формування складових і концептів політики безпеки КС найбільш доцільно визначати "політику надання послуг антивірусної безпеки".

По–друге, політика антивірусної безпеки передбачає забезпечення надійного та ефективного захисту КС проти будь–яких потенційних, реальних і перспективних вірусних атак. Поява у антивірусах евристичного режиму виявлення нових, невідомих вірусів з новими, невідомими їх сигнатурами та алгоритмами деструктивних дій надає можливість використати цей режим для імовірної кількісної оцінки їх ефективності. Така спроба вперше була зроблена в роботах [6, 8].

Так, у цих роботах для організації антивірусного захисту ПЕОМ за станом на той час визначалось за доцільне дотримуватись таких рекомендацій:

1. Кожний антивірус здатний виявляти і знешкоджувати не всі віруси, а тільки обмежену кількість із них; при цьому різні антивірусні програми можуть сканувати, виявляти та знешкоджувати різні віруси, хоча і з деяким перекриттям, але за різними сигнатурами, дескрипторами й алгоритмами атак вірусів, а також за різними результатами виявлення та знешкодження цих вірусів. Саме тому для захисту ПЕОМ пропонувалось використовувати тільки NM-комплект антивірусних програм.

2. NM-комплект повинен бути багаторівневим, тобто забезпечувати N рівнів захисту не тільки проти відомої загальної кількості M вірусів (тоді їх за станом на кінець 1998 р. існувало понад 23000), а також проти невідомих нових вірусів (за можливостями тодішніх найкращих антивірусних програм це становило від 3–5% до 10–15% від їхньої загальної кількості).

3. До появи вітчизняних антивірусів у складі такого базового чотирьохрівневого антивірусного комплекту, як свідчить багаторічний досвід їх успішного застосування ще з часів колишнього СРСР, доцільно використовувати кращі поліфаги Aidstest Д. Лозинського, Dr.Web I. Данилова, Adinf + Adinf Cure Module Д. Мостового, В. Ладигіна, Д. Зуєва фірми АО ДіалогНаука і мережений поліфаг Antiviral Toolkit Pro Е. Касперського фірми КАМІ Російської Федерації. На той час вони охоплювали усю сукупність відомих вірусів країн СНД і за цим показником мали значну перевагу перед антивірусами провідних західних країн, які у своїх базах містили, в основному, маски (сигнатури) власних вірусів і тому не охоплювали усю сукупність вірусів СНД, в тому числі і в Україні.

4. Базовий комплект доцільно доповнювати антивірусними програмами провідних західних країн для підвищення імовірності знешкодження, насамперед, мережних і макро-вірусів та для скорочення терміну екстреного антивірусного контролю ПЕОМ.

5. Стійкість захисту ПЕОМ *Рвір* антивірусного комплекту із N антивірусів оцінювалась за формулою:

$$P_{вір} = 1 - \prod_{n=1}^{N} (1 - Pn),$$

де Pn – імовірність виявлення і знешкодження відомих і нових вірусів n–ю антивірусною програмою по результатам її тестових випробувань фірмою–розробником по визначеній сукупності вірусів (якомога найбільшої).

Для експертної оцінки приймались наступні значення показника Pn: Aidstest – 0.91, Adinf + Adinf Cure Module – 0.97, Dr.Web – 0.8, 0.85, 0.9 відповідно в мінімальному, середньому та максимальному режимах евристичного аналізу вірусів, Antiviral Toolkit Pro – 0.8, імпортних західних антивірусів – згідно з табл. 1.

Таблиця 1. Можливості імпортних 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

Примітка: Pn: Aidstest – 0.91, Adinf + Adinf Cure Module – 0.97, Dr.Web – 0.8, 0.85, 0.9 відповідно в мінімальному, середньому та максимальному режимах евристичного аналізу вірусів, Antiviral Toolkit Pro – 0.8

Як бачимо, такий підхід надавав можливість оцінити стійкість захисту ПЕОМ комплектом із N антивірусів. Але на тепер цього занадто мало.

При формуванні політики безпеки для експертної оцінки стану антивірусної безпеки КС певної конфігурації, призначеності та певного класу і підкласу пропонуються модель політики антивірусної безпеки (рис. 4), а також наступні методичні, критеріальні та алгоритмічні підходи і правила антивірусної

безпеки.

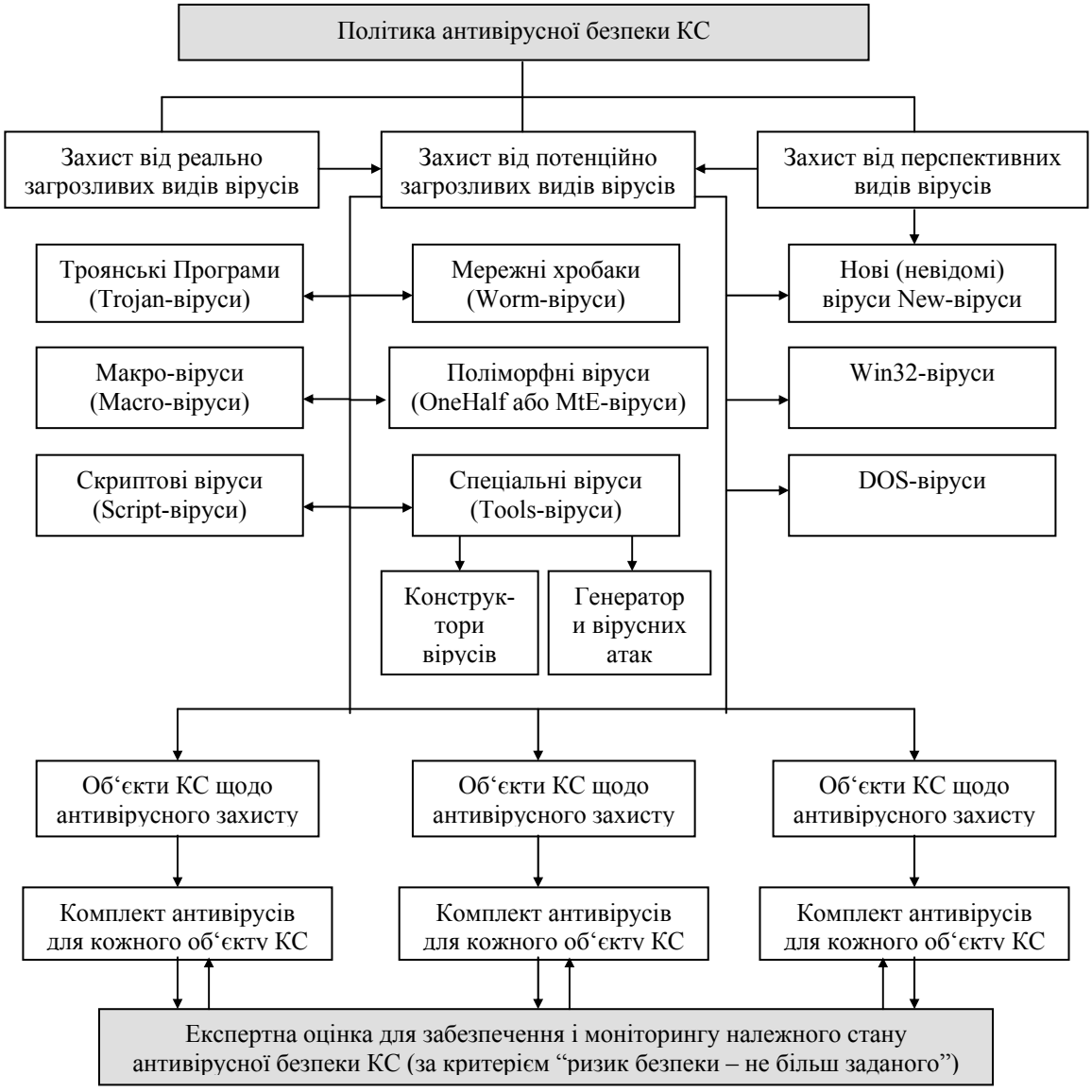

Рисунок 4 – Модель політики антивірусної безпеки КС

1. Для забезпечення антивірусної безпеки КС визначаються певні об'єкти КС, що потребують автономного/окремого антивірусного захисту, наприклад, ПЕОМ, робочі станції, сервери, кінцеві термінали тощо.

2. Для кожного об'єкта КС визначаються потенційно загрозливі, реально загрозливі, спеціальні та перспективні комп'ютерні віруси, від яких треба забезпечити його захист.

Потенційно загрозливими вірусами визначаються: DOS-віруси, Win32-віруси, мережні хробаки (Worm-віруси); троянські програми (Troyan-віруси); макро-віруси (Macro-віруси); скриптові віруси (Script-віруси); поліморфні віруси (OneHalf-віруси); спеціальні віруси (Tools-віруси, MtE); нові/перспективні віруси (New-віруси).

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

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

Новими вірусами визначаються невідомі або ті, які поки що відсутні у вірусних базах усіх/певних антивірусів;

3. Кожному **об'єкту** КС за спеціальним алгоритмом-правилом надається експертна оцінка **реального ризику** антивірусної безпеки для кожного із визначених реальних вірусів;

4. Для певної **конфігурації КС** по спеціальному алгоритму–правилу надається експертна оцінка **реального ризику** антивірусної безпеки для кожного із визначених реальних вірусів;

5.Для кожного **об'єкту** КС за спеціальним алгоритмом–правилом надається експертна оцінка **потенційного ризику** антивірусної безпеки для кожного із визначених потенційних вірусів;

6. Для певної **конфігурації** КС по спеціальному алгоритму–правилу надається експертна оцінка **потенційного ризику** антивірусної безпеки для кожного із визначених потенційних вірусів;

7. Для кожного **об'єкту** КС по спеціальному алгоритму–правилу надається експертна оцінка **належного ризику** антивірусної безпеки належним **комплектом** антивірусів;

8. Для певної **конфігурації** КС по спеціальному алгоритму–правилу надається експертна оцінка **належного ризику** антивірусної безпеки належним **комплектом** антивірусів;

9. Реальний, потенційний та належний ризик антивірусної безпеки КС визначається, оцінюється і досягається за багато етапів експертної оцінки рішенням Адміністратора безпеки КС, Розробника політики антивірусної безпеки чи Власника КС.

Згідно поданого вище (п. п. 1–9) кількісна оцінка ризику антивірусної безпеки КС здійснюється за певними критеріальними і системними підходами та по наступним математичним співвідношенням. При цьому за основу приймаються такі послідовності декомпозиції компонент антивірусної безпеки: об'єкт антивірусного захисту КС – комплект антивірусів для кожного об'єкту – антивірусна безпека КС.

Таблиця 2 – Можливості антивірусних програм

Найменування антивірусної програми	Розробник (країна)	Постачальник	Вартість (доларів, біля)	Сканування електронної пошти (да/ні)	Час сканування вірусів (хвилин)	Відсоток розпізнаних вірусів (Pn)
KAV Personal Pro 4.0.5.37	Лабораторія Касперського	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 "ДіалогНаука"	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)

Антивірусна безпека кожного об'єкту КС повинна визначатись і забезпечуватись на рівні не менш належного. Вона досягається використанням тільки комплекту антивірусів певного їх складу і кількості та за їх показниками, наприклад, згідно табл. 2 і додатково табл. 1 тощо.

Реальний насамперед, а потім і потенційний ризик антивірусної безпеки КС визначається залежно від найбільш узагальненої класифікації потенційно загрозливих видів комп'ютерних вірусів: DOS–, Win–,

Worm–, Troyan–, Macro–, Script–, Tools–, OneHalf–, New–вірусів (рис.4).

Цей ризик антивірусної безпеки оцінюється по наступним математичним співвідношенням окремо для кожного об'єкту КС.

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

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

де Pn – імовірність виявлення і знешкодження відомих і нових вірусів n–ю антивірусною програмою по результатам її тестових випробувань згідно табл. 2 та додатково табл. 1; N – кількість антивірусів в робочому комплекті, який забезпечує антивірусний захист робочої станції/ПЕОМ.

Наприклад, для захисту ПЕОМ використаються 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 5.3 %, тобто до 5 % атак Win–вірусів будуть успішними і впливати на роботу ПЕОМ.

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

$$Rwin = \prod_{n=1}^{N}(1 - Pn) \quad (2)$$

$$Rwrm = \prod_{n=1}^{N}(1 - Pn) \quad (3)$$

$$Rtro = \prod_{n=1}^{N}(1 - Pn) \quad (4)$$

$$Rmac = \prod_{n=1}^{N}(1 - Pn) \quad (5)$$

$$Rskr = \prod_{n=1}^{N}(1 - Pn) \quad (6)$$

$$Rtls = \prod_{n=1}^{N}(1 - Pn) \quad (7)$$

$$Rmte = \prod_{n=1}^{N}(1 - Pn) \quad (8)$$

$$Rnew = \prod_{n=1}^{N}(1 - Pn) \quad (9)$$

$$Rdos = \prod_{n=1}^{N}(1 - Pn) \quad (10)$$

Належний ризик антивірусної безпеки кожного об'єкту КС забезпечується вибором антивірусів та їх кількості в антивірусному робочому комплекті згідно даних табл. 2 та табл. 1. Одне зауваження – ці таблиці постійно треба доповнювати за результатами тестування нових антивірусів їх розробниками та статистики вірусних атак службами антивірусної безпеки комп'ютерних систем державних установ, відомств, організацій та комерційних структур.

Нарешті, ризик антивірусної безпеки усієї КС певної конфігурації забезпечується вибором антивірусів

та їх кількості в антивірусному робочому комплекті для усіх об'єктів цієї КС по співвідношенням:

$$Ркс = 1 - \prod_{i=1}^{No} (1 - Pio), \quad (11)$$

$$Pio = \prod_{n=1}^{Nio} (1 - Pn), \quad (12)$$

$$Rкс = 1 - Ркс, \quad (13)$$

де No – кількість захищуваних об'єктів КС; і – порядковий номер об'єкту КС; Nio – кількість антивірусів для захисту і–го об'єкта КС; Ркс – 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 (7.1); Rкс – ризик антивірусної безпеки КС.

Надамо короткі методичні рекомендації щодо експертної кількісної оцінки з метою забезпечення належного стану антивірусної безпеки КС з використанням запропонованих алгоритмічних правил та за даними економічного збитку від вірусних епідемій за шість років (з 1995 по 2001 роки) за даними журналу Конфідент, компанії Computer Economist і результатів досліджень [5,6]. Як випливає з представлених нижче результатів досліджень цієї проблеми, збиток від вірусних атак росте щорічно при чотирьох шляхах вірусного зараження – електронна пошта (до 38%), завантаження файлів з Інтернет (до 38%), замет з носіями (до 20%), неліцензійне програмне забезпечення (до 4%). Зростає і низка потенційно загрозливих видів комп'ютерних вірусів, які усе більш удосконалюються і стають усе більш небезпечними (табл. 3, 4).

Таблиця 3 – Вірусні епідемії, що мали найбільш важкі наслідки по розмірах заподіяного збитку (за даними Computer Economist)

Вірус	Рік	**Збиток, млрд. дол.**	Індекс збитку
Nimda	2001	0,59	0,67
Code Red(s)	2001	2,62	2,99
SirCam	2001	1,05	1,20
Love Bug	2000	8,75	10,00
Melissa	1999	1,10	1,26
Explorer	1999	1,02	1,17

Таблиця 4 – Збиток, понесений світовою економікою від вірусних атак с 1995 по 2001 роки (за даними журналу Конфідент і Computer Economist)

Шляхи зараження вірусами **мереж Інтранет** *	**Статистика по рокам**						
	1995	**1996**	**19967**	**1998**	**1999**	**2000**	**2001**
Електронна пошта (до 38%)						**17.1**	**11.8 (на 22.09.01)**
Завантаження файлів з Інтернет (до 38%)				**6.1**	**12.1**		
Замет з носіями (до 20%)		**1.8**	**3.3**				
При установці неліцензійного програмного забезпечення (до 4%)	**0.5**						

На думку фахівців Computer Economist, що розділяють й інші дослідники даної проблеми, самим активним став вірус I Love You, що, з'явившись у травні 2000 року, зміг проникнути на 40 млн. комп'ютерів і призвів до втрат, що обчислюються сумою 8,7 млрд. дол. Тепер всі інші віруси навіть індексуються відносно I Love You: індекс збитку показує відносний економічний вплив різних вірусів стосовно поки неперевершеної активності чи "ненажерливості" I Love You в епідеміях (табл. 3).

Як видно з таблиці 3, особливо загрозливими визначились віруси Code Red(s) і SirCam, але до результатів I Love You їм усе–таки далеко. Однак навіть ці астрономічні цифри, на думку фахівців, дуже далекі від реальних.

По–перше, не всі компанії подають чи оцінюють свої втрати.

По–друге, при обчисленнях збитку, як правило, не приймаються в розрахунок багато складових і, у першу чергу, упущена вигода.

На жаль, в Україні це питання на серйозному і систематизованому рівні поки не піднімалося і скільки–

небудь реальної статистики по розглянутій проблемі не відомо.

Алгоритмічне правило AVS–1. Локальна обчислювальна мережа установи (КС класу 2) складається з п'яти ПЕОМ/робочих станцій та одного серверу. Оцінити ризик антивірусної безпеки такої КС при наданні відповідних послуг робочих комплектів антивірусів для кожного із визначених об'єктів антивірусного захисту КС за умови – належний 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 використається мережний антивірус KAV Personal Pro версії 4.0.5.37 (Pn = 0.99, табл. 2);

– для антивірусного захисту серверу використаються мережні антивіруси KAV Personal Pro версії 4.0.5.37 (Pn = 0.99) та McAfee VirusScan 7.02.6000 (Pn = 0.95).

2. Згідно формул (11–13) та (3), а також даних табл. 4 отримуємо (за умови N1o = N2o = N3o = N4o = N5o = 1, N6o = 2):

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

Алгоритмічне правило AVS–2. Об'єктом захисту від макро–вірусів визначається одна ПЕОМ/робоча станція КС. Оцінити 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 використається антивірус KAV Personal Pro версії 4.0.5.37 (Pn = 0.99, табл. 2);

– варіант 2 – для антивірусного захисту ПЕОМ/робочої станція КС використається вітчизняний антивірус UNA 1.61.0.97 (Pn = 0.72, табл. 2);

2. Згідно формул (11–13) та (3), а також даних табл. 2 отримуємо (за умови N1o = 1):

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

Таким чином, використання вітчизняної антивірусної програми UNA 1.61.0.97 не забезпечує належний ризик антивірусної безпеки не більш 0.05%, необхідно використовувати тільки антивірусні програми KAV Personal Pro версії 4.0.5.37 (Pn = 0.99, табл. 2), при якому Rпеом = 0.01(варіант 1) або McAfee VirusScan 7.02.6000 (Pn = 0.95, табл. 2), при якому Rпеом = 0.05.

Алгоритмічне правило AVS–3. Об'єктом захисту від мережних хробаків (наприклад, від мережного електронного вірусу–шпигуна Sircam), визначається одна відповідальна робоча станція Інтранет. Оцінити ризик антивірусної безпеки Rpc такого об'єкту Інтранет за умови – належний ризик від атак мережного електронного вірусу–шпигуна Sircam не більш 0.01 %.

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

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

– варіант 2 – для антивірусного захисту робочої станції Інтранет використається мережний вітчизняний антивірус UNA 1.61.0.97 (Pn = 0.72, табл. 2);

2. Згідно формул (11–13) та (3), а також даних табл. 2 отримуємо (за умови N1o = 1):

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

Таким чином, використання вітчизняної антивірусної програми UNA 1.61.0.97 не забезпечує належний

ризик антивірусної безпеки не більш 0.01%, необхідно використовувати тільки антивірусні програми, які мають показник Pn =/> 0.99 по табл. 2, наприклад, це тільки мережний антивірус KAV Personal Pro версії 4.0.5.37 (Pn = 0.99, табл. 2).

Алгоритмічне правило AVS–4. Згідно статистиці вірусних атак на мережі Інтранет визначено, що найбільш небезпечними є два шляхи їх зараження комп'ютерними вірусами (вірусних атак) – електронна пошта і завантаження файлів з Інтернет (до 80 %). Локальна обчислювальна мережа організації має постійне з'єднання з Інтернет, 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 їх антивірусної безпеки від вірусних атак по каналам електронної пошти повинен бути – для робочих станцій не більш 0.01 %, для серверу не більш 0.0001%. Це здійснюється в два етапи.

1. Перший етап – це **аналіз можливостей антивірусів** для виявлення та знешкодження вірусів електронної пошти згідно даних табл. 2, а також табл.1. Так, з ними здатні боротися усі мережані антивіруси. Для цього треба оцінювати, насамперед, в табл. 2 значення показника Pn. Чим він має більше значення, 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 **найбільш потужних**, тобто з найбільш широким арсеналом захисту від загрозливих для Вашої мережі Інтранет видів вірусів.

2. Другий етап – **вибір складу комплектів** антивірусів. Вибирати доцільно тільки ті комплекти, які здані виявляти і знешкоджувати віруси електронної пошти з ризиком безпеки не більш заданого та найменш дорогі, тобто **за критерієм "ризик антивірусної безпеки – вартість".** Експертну оцінку можна здійснювати по формулі (3) для мережаних хробаків.

Так, можна визначити декілька варіантів AVS–4.1 – AVS –4.4 щодо складу комплектів антивірусів для заданої захищеності робочих станцій та серверу Інтранет.

1. Варіант AVS–4.1. Комплект з одного антивірусу KAV Personal Pro версії 4.0.5.37 (Pn = 0.99, табл. 2). Ризик антивірусної безпеки по формулі (3) дорівнюється:

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

2. Варіант AVS–4.2. Комплект з антивірусу KAV Personal Pro версії 4.0.5.37 (Pn = 0.99) та антивірусу McAfee VirusScan 7.02.6000 (Pn = 0.95). Ризик антивірусної безпеки по формулі (3) дорівнюється (N=2):

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

3. Варіант AVS–4.3. Комплект з антивірусу KAV Personal Pro версії 4.0.5.37 (Pn = 0.99), антивірусу McAfee VirusScan 7.02.6000 (Pn = 0.95) та антивірусу DrWeb for Windows Version 4.29b (Pn = 0.81). Ризик антивірусної безпеки по формулі (3) дорівнюється (N=3):

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

4. **Варіант 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 = 0.72):
Ризик антивірусної безпеки по формулі (3) дорівнюється (N=3):

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

Таким чином, для серверу можна пропонувати тільки комплект антивірусів AVS–4.3, а для робочих станцій підходять комплекти антивірусів AVS–4.1 – AVS–4.4. Але за критерієм "ризик антивірусної безпеки – вартість" для робочих станцій заданим вимогам задовольняє тільки комплект AVS–4.1.

Наведені приклади свідчать, що такі AVS–алгоритми чи AVS–правила можна і необхідно постійно нарощувати за досвідом боротьби з вірусами та експлуатації Інтранет. У цій статті вони наведені лише для демонстрації працездатності запропонованого методу експертної кількісної оцінки антивірусної безпеки КС певних конфігурацій за математичними співвідношеннями (1– 13).

Висновки

1. Найбільшого поширення серед розробників різних країн і фірм щодо антивірусного захисту має

практика тестування самих програм і пакетів антивірусного захисту за певними балами і рейтингами та за певною сукупністю часткових показників функціонування тільки антивірусів. Це вірно, але цього не достатньо. Необхідно ще обов'язково оцінювати стан антивірусної безпеки самої комп'ютерної системи при використанні цих антивірусів. Безсумнівно, що це має велике практичне значення.

2. Для формування політики безпеки комп'ютерних систем доцільно визначати складову політику не антивірусного захисту, а антивірусної безпеки. Поняття "захист" від вірусів передбачає пасивні оборонні дії. Поняття "безпека" передбачає, навпаки, активні оборонні контрдії проти певних загроз. Тому при такій постановці задачі для формування складових політики безпеки комп'ютерних систем найбільш доцільно визначати "політику надання послуг антивірусної безпеки".

3. Запропоновані основи побудови системи антивірусної безпеки в корпоративних комп'ютерних мережах Інтранет, методи та приклади експертної кількісної оцінки стану антивірусної безпеки комп'ютерних систем різних конфігурацій можуть бути корисними для їх адміністраторів безпеки, користувачів, власників при організації антивірусного захисту, а також для аспірантів, магістрів, студентів вищих навчальних закладів і науково–дослідних установ при проведенні досліджень по цій тематиці.

*Література: **1**. Шорошев В. В., Домарев В. В. Журнал "Бизнес и безопасность" № 1, 2 1998 г. Рекомендации по обеспечению безопасности конфиденциальной информации согласно "Критериев оценки надежных компьютерных систем TCSEC" (Trusted Computer Systems Evaluation Criteria)", США, "Оранжевая книга". **2**. Шорошев В. В., Домарев В. В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно европейским "Критериям оценки безопасности информационных технологий ITSEC" (Information Technology Security Evaluation Criteria). Журнал "Бизнес и безопасность" № 3, 1998 г. **3**. Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 5 1998 г. Международные стандарты безопасности компьютерных систем: эволюция развития, проблемы, рекомендации. **4**. Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 6 1998 г. Рекомендации по основам информационной безопасности согласно Канадских критериев CTCPEC (Canadian Trusted Computer Product Evaluation Criteria), 1993 г. **5**. Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 1 1999г. Рекомендации по основам информационной безопасности согласно Единых критериев CCITSE (Common Criteria for Information Technology Security Evaluation), 1996 – 1997 г. г. **6**. Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 2 1999 г. Класифікація комп'ютерних вірусів і основи захисту від них. **7**. Шорошев В. В., Ильницкий А. Е. Журнал "Бизнес и безопасность" № 3, 4, 5 1999 г. Основи захисту інформації ПЕОМ від загроз НСД. **8**. Шорошев В. В., Ильницкий А. Е., Маматкулов В. Т., Кривошеєв Е. А. Журнал "Бизнес и безопасность" № 6. 1999 г. Антивирусная защита вашей ПЭВМ. **9**. Ільніцький А. Ю., Шорошев В. В., Близнюк І. Л. Основи захисту інформації від несанкціонованого доступу. Звіт НДР, К. 2000. **10**. Зегжда Д. П.. Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с. **11**. Симонович С. Windows 98: учебный курс – СПб: Питер Ком, 1998. – 512 с.: ил.*

УДК 681.3.06

БЛОКОВИЙ СИМЕТРИЧНИЙ ШИФР НА ОСНОВІ МОДУЛЬНОЇ АРИФМЕТИКИ

Віталій Сокирук, Володимир Лужецький
Вінницький національний технічний університет

Анотація: **Пропонується блоковий симетричний шифр на основі модульної арифметики. Блоки даних та секретні ключі розглядаються як цілі числа, над якими виконуються арифметичні операції множення, ділення, додавання та віднімання за модулем 2^n.**
Summary: **Block cipher based on modular arithmetic is offered. Data blocks and secret keys examine as big integer numbers on which the multiplication, division, addition and subtraction modulo 2^n is executed.**
Ключові слова: **Захист інформації, криптографія, блокові симетричні шифри.**

І Вступ

Блокові симетричні шифри (БСШ) широко застосовуються для захисту інформації в сучасному інформаційному суспільстві. Вони є невід'ємним атрибутом багатьох систем захисту інформації і вирішують широкий спектр сучасних криптографічних задач. БСШ володіють високою швидкістю і забезпечують високий рівень криптостійкості, що робить їх використання безальтернативним для задач