ARTICLE

DOI 10.36074/grail-of-science.19.09.2025.042

МОДЕЛЬ ДОСЛІДЖЕННЯ АНТИВІРУСНИХ СИСТЕМ

Вдовиченко Ірина Никифорівна
канд. техн. наук, доцент
ст. викладач кафедри комп'ютерних систем та мереж
Криворізький національний університет, Україна

Маркова Оксана Миколаївна
канд. пед. наук, доцент,
доцент кафедри комп'ютерних систем та мереж
Криворізький національний університет, Україна

Анотація. *Представлене дослідження є продовженням наукової роботи з напряму забезпечення безпеки від витоку інформації на підприємстві. В роботі розглянуто перелік сучасних світових брендів, розробників та дослідників антивірусних програм, а також доведено актуальність захисту від комп'ютерних вірусів та використання антивірусних систем у цьому процесі. Запропоновано модель дослідження антивірусних систем для визначення оптимальної системи, з розглянутих. Представлені результати та розрахунки проведеного дослідження. За результатами дослідження зроблені висновки та пропозиції. Для реалізації моделі та проведення дослідження використано пакет SPSS, призначений для складного статистичного аналізу даних.*

Ключові слова: *антивірусні програми; модель; дослідження; аналіз; кластер; фактор.*

Постановка проблеми. У сучасному світі, де цифровізація охоплює всі сфери діяльності, питання забезпечення інформаційної безпеки стають критично важливими. Кількість кібератак та витоків даних постійно зростає, що створює серйозні виклики для компаній та організацій.

Організації всіх рівнів, від малих підприємств до великих корпорацій, залежать від своєї здатності безпечно зберігати та використовувати дані. Проте з розвитком технологій зростає і кількість загроз, спрямованих на отримання несанкціонованого доступу до цих даних. Згідно зі звітом IBM 2023 року, середня вартість витоку даних для компанії становить понад 4,35 мільйона доларів, що підтверджує актуальність цієї проблеми. Сьогодні кіберзлочинність є одним із найактуальніших викликів для бізнесу та суспільства загалом [2].

Одним з елементів кіберзлочинності є комп'ютерні віруси. Комп'ютерні віруси відносяться до шкідницьких програм, які призначені для реалізації загроз інформації, що зберігається в КС, або для прихованого нецільового використання ресурсів КС, або іншого впливу, що перешкоджає нормальному функціонуванню КС. Дуже небезпечними вважають віруси, що викликають

 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

порушення конфіденційності, знищення, необоротну модифікацію (у тому числі й шифрування) інформації, а також віруси, що блокують доступ до інформації, що приводять до відмови апаратних засобів та завдають збитки користувачам.

Тому питання боротьби з комп'ютерним вірусами є досить актуальною задачею.

Аналіз досліджень та публікацій. Дослідженнями в галузі антивірусних програм займалися такі спеціалісти, як Реймонд Томлінсон (створив першу автоматичну антивірусну програму "Reaper" у 1971 році), Анди Хопкінс (написав перші антивірусні утиліти CHK4BOMB і BOMBSQAD у 1984 році) та компанія ThunderByte (створила програму "Vaccine" у 1987 році). Також значний внесок зробив Боб Томас, який у 1973 році написав перший мережевий вірус Creeper, що послужив каталізатором для розробки антивірусних рішень, хоча його програма не була антивірусною, а скоріше першим самовідтворюваним мережевим кодом.

Сучасними світовими розробниками та дослідниками антивірусних програм є Procon Software, S&S International, Hoffman Datenshutz, Norman Data Defense Systems, Symantec, Noviz Data [6].

В Україні одним з найбільш відомих вітчизняних дослідників та розробників антивірусного програмного забезпечення є компанія «Лабораторія Zillya!» з антивірусом Zillya! Цей антивірус вперше був випущений у 2009 році. Окрім цього, українські інтернет-провайдери, такі як Укртелеком, співпрацюють з іноземними компаніями, наприклад, з Eset, для надання послуг антивірусного захисту користувачам та аналізу антивірусного програмного забезпечення. Цьому питанню приділяється увага і на законодавчому рівні. Одним з основних вітчизняних законів в галузі боротьби з комп'ютерними вірусами є Закон України «Про основні засади забезпечення кібербезпеки України». Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [4].

Мета роботи. В роботі пропонується модель дослідження антивірусних систем. На основі цієї моделі проведено дослідження та розрахунки і представлені результати. Для реалізації моделі пропонується використати статистичний пакет SPSS, призначений для складного статистичного аналізу даних. З урахуванням актуальності теми, автори знайомлять з моделлю, яка може бути корисною для дослідження антивірусних програм.

Виклад основного матеріалу. Для визначення оптимальної антивірусної програми розроблено наступну модель (рис.1).

Для проведення дослідження щодо визначення оптимальної антивірусної програми проаналізували 6 програм за такими характеристиками: програмна сумісність, сумісність з ОС, місце на HDD, можливість роботи в мережі, надійність, вартість, простота навчання, та інші (8 характеристик).

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

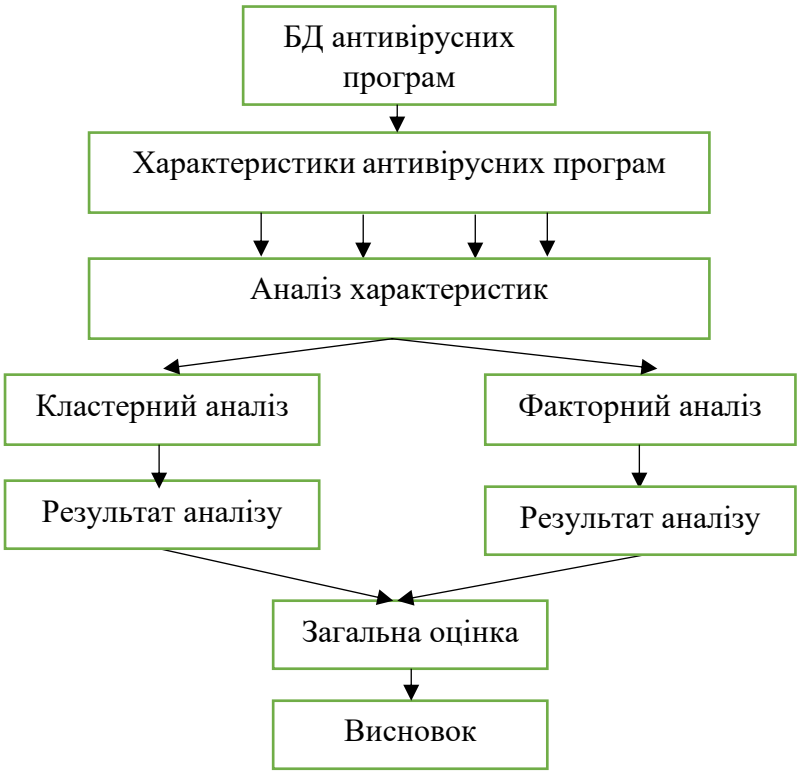
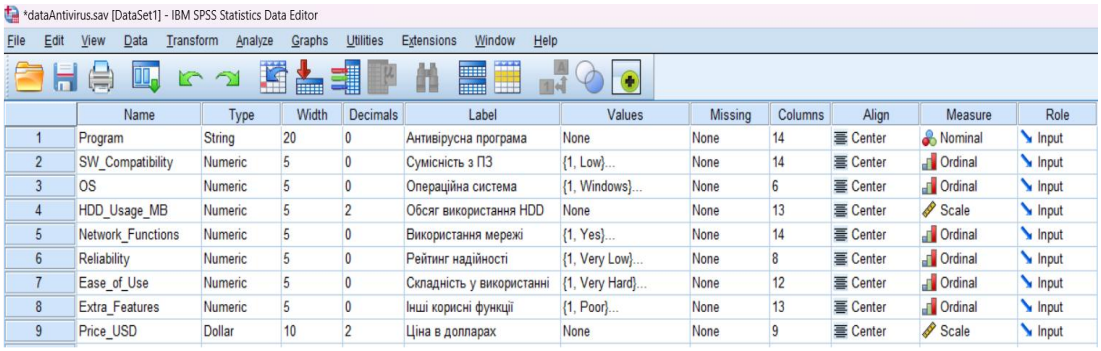


Рис. 1. Модель дослідження

Спроектуємо таблицю для дослідження зазначеної предметної галузі, використовуючи можливості програмного забезпечення SPSS (рис. 2).

Визначаємо змінні: Program – назва антивірусної програми (текстова змінна, ідентифікатор).

SW_Compatibility – сумісність з іншими програмами (1 = Low, ..., 5 = High).



*dataAntivirus.sav [DataSet1] - IBM SPSS Statistics Data Editor

File Edit View Data Transform Analyze Graphs Utilities Extensions Window Help

	Name	Type	Width	Decimals	Label	Values	Missing	Columns	Align	Measure	Role
1	Program	String	20	0	Антивірусна програма	None	None	14	Center	Nominal	Input
2	SW_Compatibility	Numeric	5	0	Сумісність з ПЗ	{1, Low}...	None	14	Center	Ordinal	Input
3	OS	Numeric	5	0	Операційна система	{1, Windows}...	None	6	Center	Ordinal	Input
4	HDD_Usage_MB	Numeric	5	2	Обсяг використання HDD	None	None	13	Center	Scale	Input
5	Network_Functions	Numeric	5	0	Використання мережі	{1, Yes}...	None	14	Center	Ordinal	Input
6	Reliability	Numeric	5	0	Рейтинг надійності	{1, Very Low}...	None	8	Center	Ordinal	Input
7	Ease_of_Use	Numeric	5	0	Складність у використанні	{1, Very Hard}...	None	12	Center	Ordinal	Input
8	Extra_Features	Numeric	5	0	Інші корисні функції	{1, Poor}...	None	13	Center	Ordinal	Input
9	Price_USD	Dollar	10	2	Ціна в долларах	None	None	9	Center	Scale	Input

Рис. 2. Проектування таблиці

Оцінює, наскільки добре антивірус працює разом з іншим ПЗ.

OS – операційна система, яку підтримує антивірус (1 = Windows, 2 = Linux, 3 = MacOS). Основна ОС або найбільш пріоритетна, для якої доступна програма.

HDD_Usage_MB – обсяг використання диска в мегабайтах. Скільки місця займає антивірус на жорсткому диску.

Network_Functions – використання мережевих функцій (0 = ні, 1 = так). Чи має антивірус функції, що використовують інтернет або мережу.

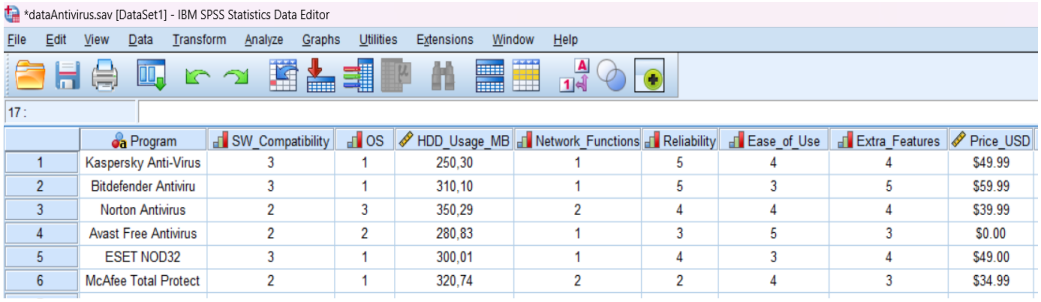
Reliability – рейтинг надійності (1 = Very Low, ..., 5 = Very High). Оцінка стабільності та довіри до антивіруса.

Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

Ease_of_Use – зручність у використанні (1 = Very Hard, ..., 5 = Very Easy). Наскільки просто користуватися програмою.

Extra_Features – кількість додаткових функцій (1 = Poor, ..., 5 = Excellent). Функції, що виходять за межі базового захисту (батьківський контроль, VPN тощо).

Price_USD – вартість програми в доларах США (Ціна ліцензії або підписки). Заповнена таблиця представлена на рис. 3.



	Program	SW_Compatibility	OS	HDD_Usage_MB	Network_Functions	Reliability	Ease_of_Use	Extra_Features	Price_USD
1	Kaspersky Anti-Virus	3	1	250,30	1	5	4	4	$49.99
2	Bitdefender Antiviru	3	1	310,10	1	5	3	5	$59.99
3	Norton Antivirus	2	3	350,29	2	4	4	4	$39.99
4	Avast Free Antivirus	2	2	280,83	1	3	5	3	$0.00
5	ESET NOD32	3	1	300,01	1	4	3	4	$49.00
6	McAfee Total Protect	2	1	320,74	2	2	4	3	$34.99

Рис. 3. Заповнена таблиця

Для кластерного аналізу здійснено ієрархічну класифікацію у пункті меню *Analyze* оберемо *Classify – Hierarchical Cluster* (рис. 3.).

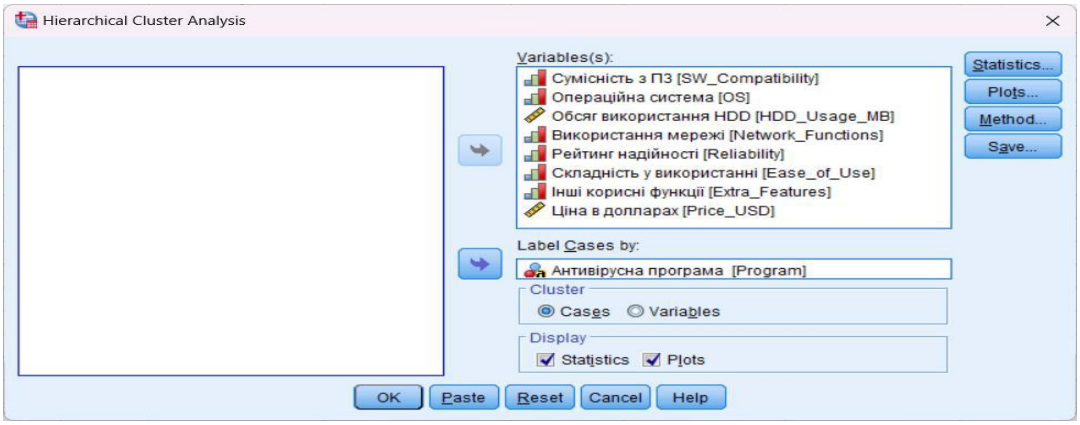


Рис. 3. Діалогове вікно з розподіленими даними

Після виконання необхідних обробок у вікні виводу буде представлено результати проведеного кластерного аналізу. Після звичайного статистичного зведення підсумків за спостереженнями буде представлена таблиця, яка відображає порядок агломерації та дендрограма (рис. 4).

Agglomeration Schedule

Stage	Cluster Combined		Coefficients	Stage Cluster First Appears		Next Stage
	Cluster 1	Cluster 2		Cluster 1	Cluster 2	
1	2	5	1,690	0	0	2
2	1	2	1,954	0	1	4
3	3	6	3,348	0	0	4
4	1	3	2,915	2	3	5
5	1	4	2,703	4	0	0

Рис. 4. Таблиця Agglomeration Schedule

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

На першому кроці були об'єднані програми Bitdefender Antivirus (2) та ESET NOD32 (5) на відстані 1,690. Це означає, що ці дві програми мають найвищу подібність за показниками надійності, сумісності та додаткових функцій.

На другому кроці об'єдналися Kaspersky Anti-Virus (1) та Bitdefender Antivirus (2) з відстанню 1,954 — середній рівень надійності та ціни, подібний профіль простоти використання. На третьому кроці злилися Norton Antivirus (3) та McAfee Total Protection (6) на відстані 3,348, об'єднавши безкоштовний/доступний сегмент із середньою надійністю.

Далі відбувається поступове об'єднання трьох кластерів: Кластери (1+2) та (3+6) зливаються на кроці 4 із відстанню 2,915. Вони потім з'єднуються з кластером (4+5) на кроці 5 із відстанню 2,703.

Для визначення оптимальної кількості кластерів вирішальне значення має показник коефіцієнт. Під цим коефіцієнтом мається на увазі відстань між двома кластерами, визначена на підставі обраної міри відстані. У нашому випадку це відстань Мінковського, визначена з використанням стандартизованих значень. Оптимальним вважається число кластерів, рівне різниці кількості спостережень (маємо 6) і кількості кроків, після якого коефіцієнт збільшується стрибкоподібно (маємо 2). Тобто оптимальне число кластерів дорівнює 6 – 2 = 4. Після визначення оптимальної кількості кластерів організуємо для кожного спостереження видачу інформації про належність до кластера (рис. 5).

Cluster Membership

Case	4 Clusters
1:Kaspersky Anti-Virus	1
2:Bitdefender Antiviru	1
3:Norton Antivirus	2
4:Avast Free Antivirus	3
5:ESET NOD32	1
6:McAfee Total Protect	4

Рис. 5. Таблиця з виведенням належності до кластерів

Кластер 1 характеризується максимальною надійністю (Mean Reliability ≈ 5), високим рівнем додаткових функцій (≈ 4.5) та преміальною вартістю (≈ 55 USD).

Кластер 2 та 3 має збалансовані показники надійності (≈ 4), середню ціну (≈ 44 USD) і середню простоту використання (≈ 3.5).

Кластер 4 відрізняється низькою/нульовою вартістю (0–35 USD), середньою надійністю (≈ 3) та найвищою простотою використання (≈ 4).

Виконавши далі звіт за змінними та кластерами та розрахунок середніх одержали такі висновки: Кластер 1 (High-End Security): висока сумісність і надійність, багато функцій; преміальний сегмен. Кластер 2 та 3 (Balanced Solutions): оптимальний баланс ціни і надійності, середній набір функцій.

 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

Кластер 4 (Budget/Free): мінімальні витрати і висока простота використання, але знижена надійність і менше додаткових можливостей.

При організації факторного аналізу використані наступні методології:

1.Метод екстракції: Principal Component Analysis (PCA).

2.Метод обертання: Varimax з нормалізацією Кайзера.

3.Критерій виділення факторів: Власні значення >1.

Аналіз результатів показав, що усі змінні мають високі значення екстракції (від 0.893 до 0.986), що свідчить про їхню чітку приналежність до виділених факторів (рис. 6).

Communalities

	Initial	Extraction
Сумісність з ПЗ	1,000	,986
Операційна система	1,000	,980
Обсяг використання HDD	1,000	,941
Використання мережі	1,000	,893
Рейтинг надійності	1,000	,977
Складність у використанні	1,000	,946
Інші корисні функції	1,000	,964
Ціна в долларах	1,000	,938

Extraction Method: Principal Component Analysis.

Рис. 6. Таблиця комунальності

Таблиця "Total Variance Explained" (рис. 7) показує, скільки відсотків дисперсії пояснює кожен фактор. Три компоненти пояснюють 95.318% дисперсії даних: Компонента 1: 56.415%. Компонента 2: 25.95%. Компонента 3: 12.953%.

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4,513	56,415	56,415	4,513	56,415	56,415	3,737	46,714	46,714
2	2,076	25,950	82,365	2,076	25,950	82,365	2,392	29,896	76,609
3	1,036	12,953	95,318	1,036	12,953	95,318	1,497	18,709	95,318
4	,296	3,698	99,016						
5	,079	,984	100,000						
6	7,651E-16	9,563E-15	100,000						
7	2,157E-16	2,697E-15	100,000						
8	-2,669E-17	-3,336E-16	100,000						

Extraction Method: Principal Component Analysis.

Рис. 7. Повна пояснена дисперсія

Фактор 1 найбільш пов'язаний з Extra_Features (0.976), Reliability (0.850), Price_USD (0.876), SW_Compatibility (0.724). Цей фактор відображає вартість та функціональність. Високі значення вказують на продукти з розширеними функціями, надійністю та вищою ціною.

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License

Фактор 2 найбільш пов'язаний з HDD_Usage_MB (0.934), Network_Functions (0.908). Фактор відображає використання ресурсів та мережеві можливості. Високі значення свідчать про продукти, що інтенсивно використовують пам'ять та мережу.

Фактор 3 найбільш пов'язаний з OS (0.908), Ease_of_Use (0.496). Фактор характеризує адаптацію до операційної системи та зручність використання. Найбільш перспективні продукти ті, що мають високі значення за Фактором 1 (функціональність, надійність) та Фактором 3 (зручність, адаптація до ОС).

Висновки та пропозиції. Кластерний аналіз дозволив розподілити програми на чотири групи за схожими характеристиками, виявивши сегменти: преміальні рішення, збалансовані продукти та бюджетні/безкоштовні варіанти. Факторний аналіз виявив три ключові фактори, що впливають на сприйняття продуктів: функціональність і вартість, використання ресурсів, а також адаптацію до ОС та зручність.

Результати підтверджують, що для вибору оптимальної антивірусної програми слід орієнтуватися на її надійність, набір функцій та ефективність роботи в конкретному середовищі. Отримані дані можуть бути корисними для подальшого дослідження ринку антивірусних програм (і не тільки) та вдосконалення продуктів.

За результатами аналізу, можна рекомендувати для покращення конкурентоспроможності програм, що варто зосередитися на оптимізації використання ресурсів (Фактор 2).

Дослідження, проведене за розробленою моделлю дає змогу виявити оптимальний варіант антивірусної програми (із переліку), стосовно вказаних характеристик.

Список використаних джерел:

[1] Богуш В.М., Богуш В.В., Бровко В.Д., Настрадін В.П. (2021) Основи кіберпростору, кібербезпеки та кіберзахисту. Ліра-К.
[2] Вдовиченко І.Н. (2025, 23–24 квітня). Сучасні тенденції використання штучного інтелекту в кібербезпеці. International scientific and technical conference Information Technologies in Metallurgy and Machine building – ITMM 2025. м. Дніпро. Україна. УДУНТ. DOI: 10.34185/1991-7848.itmm.2025.01.001.
[3] Вервейко В. В. (2021, 20 – 21 квітня). Аналіз видів захисту особистих даних використовуючи антивірусні програми. Матеріали 25-го Міжнародного молодіжного Форуму "Радіоелектроніка і молодь у XXI столітті" Конференція "Перспективи розвитку інфокомунікацій та інформаційно-вимірювальні технологіїм". м. Харків. Україна. ХНУРЕ.
[4] Верховна Рада України. (2017). Про основні засади забезпечення кібербезпеки України. № 45, ст.403. https://zakon.rada.gov.ua/laws/show/2163-19#Text.
[5] Хто і навіщо пише віруси. URL: http://zillya.ua/ru/kto-i-zachem-pishetvirusy (Дата звернення 12.09.2025).
[6] Шорошев В. (2007). Антивірусні програми світових брендів: порівняльна оцінка можливостей, рекомендації з їх вибору, новий метод прогнозування антивірусної безпеки. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. вип. 1 (14). 136–144. https://ela.kpi.ua/server/api/core/bitstreams/d428c62e-5199-404a-9808-e4dac787d884/content

 Авторські права захищені | Creative Commons Attribution-ShareAlike 4.0 International License

ANTIVIRUS SYSTEMS RESEARCH MODEL

Irina Vdovychenko
Candidate of Technical Sciences, Associate Professor
Senior Lecturer, Department of Computer Systems and Networks
Kryvyi Rih National University, Ukraine
Oksana Markova
Candidate of Pedagogical Sciences, Associate Professor,
Associate Professor, Department of Computer Systems and Networks
Kryvyi Rih National University, Ukraine

Summary. *The presented study is a continuation of scientific work in the direction of ensuring security against information leakage at the enterprise. The work considers a list of modern world brands, developers and researchers of antivirus programs, and also proves the relevance of protection against computer viruses and the use of antivirus systems in this process. A model for studying antivirus systems is proposed to determine the optimal one from those considered. The results and calculations of the conducted study are presented. Based on the results of the study, conclusions and proposals are made. To implement the model and conduct the study, the SPSS package, designed for complex statistical data analysis, was used.*
Keywords: *antivirus programs; model; research; analysis; cluster; factor.*

All rights reserved | Creative Commons Attribution-ShareAlike 4.0 International License