

ДОДАТОК А
СЛАЙДИ ПРЕЗЕНТАЦІЇ

Харківський національний університет радіоелектроніки

Кафедра Інформаційно-мережної інженерії

Кваліфікаційна робота магістра на тему:

**Дослідження та порівняльний аналіз
антивірусних програм**

Студент:	Вервейко Владислав Володимирович
Група:	ІМІм – 19 - 2
Керівник:	доц. к.т.н. Чеботарьова Дарія Василівна

Харків - 2021

Мета роботи:

дослідження сучасних вірусних і антивірусних програм та порівняльний аналіз антивірусних програм.

Задачі:

- 1) дослідити сучасні комп'ютерні вірусів та антивірусні програми,
- 2) проаналізувати сучасні тенденції розвитку антивірусних програм в Україні та світі,
- 3) розглянути особливості ураження комп'ютерів вірусами та методи організації антивірусної безпеки,
- 4) виконати порівняльний аналіз сучасних антивірусних програм.

2

Аналіз розвитку антивірусних програм

Антивірусна програма - спеціалізована програма для виявлення комп'ютерних вірусів і небажаних (шкідливих) програм, відновлення заражених (модифікованих) цими програмами файлів та запобігання подальших заражень (модифікацій) файлів або операційної системи шкідливим кодом.

у 1984 р. Енді Хопкінсом були створені найперші антивірусні програми: СНК4ВОМВ і ВОСНК4ВОМВ.

3

Сучасні тенденції розвитку антивірусних програм

- Впровадження нових технологій (перенос послуги і даних в хмару, моделі штучного інтелекту і машинного навчання тощо).
- Впровадження нових нормативних вимог.
- Створення інноваційних способів вбудовування функцій безпеки в продукти для протидії загрозам.
- Антивірусні програми еволюціонують у бік розробки інструментів прогнозування вірусних атак.
- Використання для виявлення загроз аналізу аномальної поведінки, що властива шкідливому ПЗ.
- Застосування методів багатфакторної авторизації.

4

Хакерські атаки на Україну

Останні роки Україна переживає інформаційну війну, одним з доказів якої є величезна кількість кібератак.

За останні роки РФ здійснила понад 7 тисяч кібератак проти України. Їхня головна мета – дестабілізувати ситуацію в державі.

Такі кібератаки наносять непоправної шкоди різним галузям та сприяють величезним фінансовим збиткам.

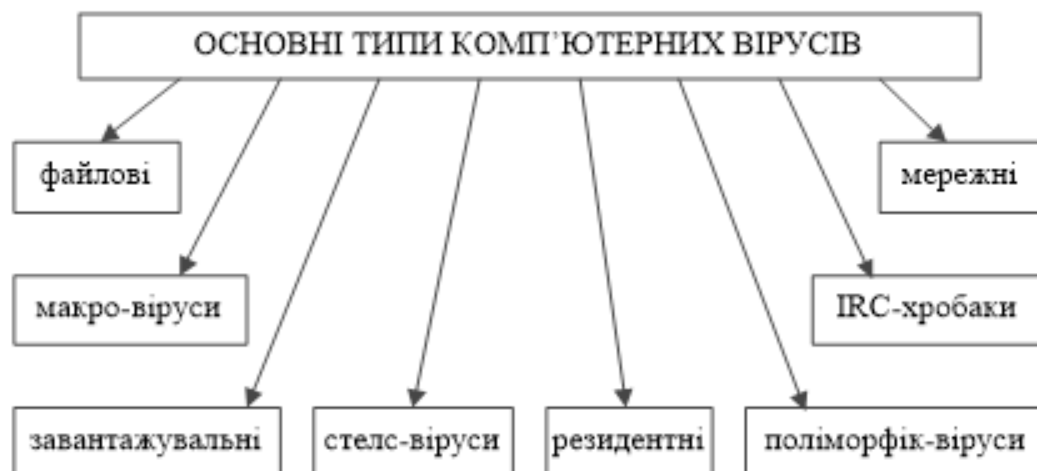


Класифікація вірусних програм



6

Типи вірусних програм



7

Джерела вірусів

- глобальні мережі (зокрема електронна пошта);
- електронні конференції, файл-сервери ftp і BBS;
- локальні мережі;
- піратське програмне забезпечення;
- персональні комп'ютери загального користування;
- випадкові користувачі комп'ютера;
- заражений зовнішні накопичувачі (зокрема флеш-пам'ять);
- програмні продукти, придбані нелегальним шляхом.

8

Ознаки зараження комп'ютера вірусами



9

Методи і технології захисту від шкідливих програм

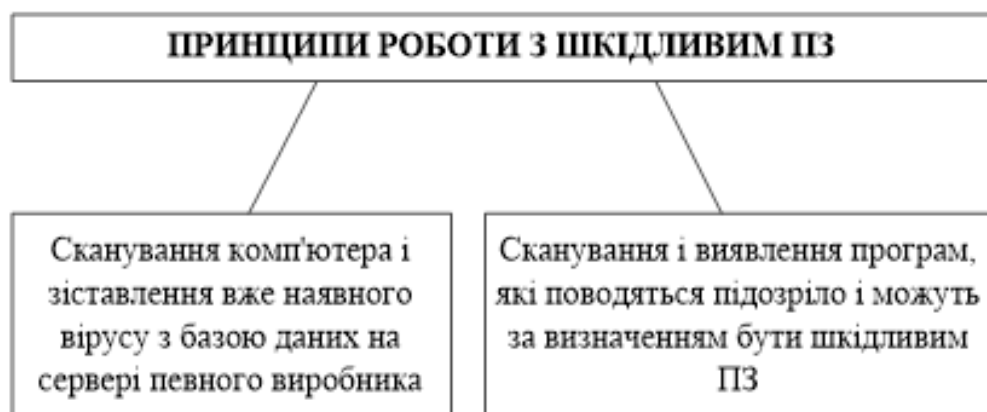
ПРАВИЛА БЕЗПЕЧНОГО ВИКОРИСТАННЯ ПК	
Обов'язкове використання антивірусного захисту	Більшість сучасних антивірусних програм захищають від найрізноманітніших комп'ютерних загроз - від вірусів, хробаків, троянських програм і рекламних систем. Інтегровані рішення з безпеки також ставлять фільтр проти спаму, мережних атак, відвідування небажаних і небезпечних інтернет-ресурсів
Не слід довіряти всій інформації, що надходить на ПК	Ніколи не слід відкривати файли і посилання, що приходять з невідомого джерела. Навіть якщо повідомлення отримано з джерела відомого (від знайомого або колеги по роботі), але присланий файл або посилання приходить несподівано, - краще перепитати про справжність повідомлення, оскільки зворотня адреса в електронній пошті легко підробляється
Слід звертати велику увагу на інформацію від антивірусних компаній	Слід звертати велику увагу на інформацію від антивірусних компаній і від експертів з комп'ютерної безпеки. Зазвичай вони своєчасно повідомляють про нові види інтернет-шахрайств, нові вірусні погрози та епідемії

Вимоги до антивірусних програм

ВИМОГИ ДО АНТИВІРУСНИХ ПРОГРАМ	
1. Стабільність і надійність роботи	Цей параметр є визначальним - навіть найкращий антивірус виявиться абсолютно марним, якщо він не зможе нормально функціонувати на комп'ютері, якщо в результаті якого-небудь збою в роботі програми процес перевірки комп'ютера не пройде до кінця. Тоді завжди є ймовірність того, що якісь заражені файли залишилися непоміченими
2. Розміри вірусної бази програми	З урахуванням постійної появи нових вірусів база даних повинна регулярно оновлюватися. Крім того необхідна можливість програми визначати різноманітні типи вірусів, і вміння працювати з файлами різних типів (архіви, документи). Важливим також є наявність резидентного монітора, який здійснює перевірку всіх нових файлів автоматично, у міру їх запису на диск
3. Швидкість роботи програми	Швидкість та наявність додаткових можливостей типу алгоритмів визначення навіть невідомих програми вірусів (евристичне сканування). Крім того необхідна можливість відновлювати заражені файли, не стираючи їх з жорсткого диска, а тільки видаливши з них віруси. Важливим є також відсоток помилкових спрацьовувань програми
4. Багато-платформність	Наявність версій програми під різні ОС. Якщо антивірус використовується тільки на одному комп'ютері, то цей параметр не має великого значення. Але антивірус для великої організації просто зобов'язаний підтримувати всі поширені операційні системи. Крім того, при роботі в мережі важливою є наявність серверних функцій, призначених для адміністративної роботи та можливість роботи з різними видами серверів

11

Принципи роботи з шкідливим ПЗ, що використовують антивірусні програми

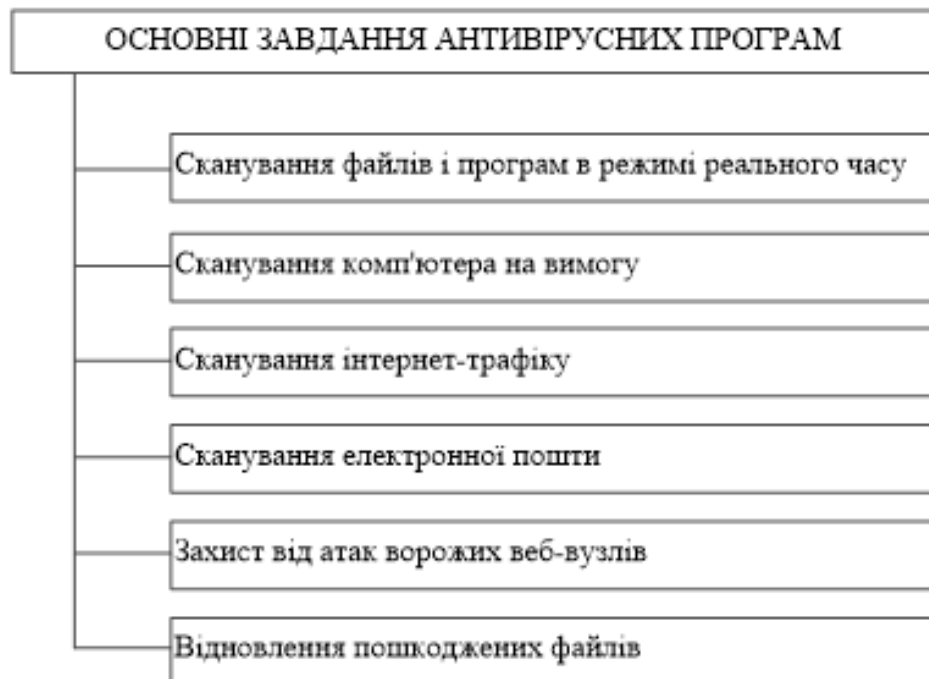


12

Класифікація антивірусних модулів



Завдання антивірусних програм



14

Порівняльний аналіз антивірусних програм

№	Антивірус	Захист	Ефективність	Зручність використання
1	BullGuard Internet Security	4	6	4
2	Kaspersky Internet Security	6	4	5
3	NortonLifeLock	4	5	6
4	AhnLab V3 Internet Security	6	5	5
5	Avast Free AntiVirus	3	4	4
6	AVG Internet Security	5	6	5
7	Avira Antivirus Pro	4	4	5
8	Microsoft Windows Defender	5	5	5

Критерій оцінювання:

- 0 – не функціонує, 1 – функціонує, але не знаходить віруси
- 2 – функціонує, але знаходить прості віруси,
- 3 – функціонує, але не оновлюються бази даних
- 4 – функціонує, але не протидіє складним вірусам
- 5 – функціонує, але бувають збої в роботі
- 6 – повністю функціонує у фоновому режимі

15

Розрахунок ймовірності захисту

Розрахунок ймовірностей захисту кожною антивірусною програмою виконано за допомогою формули:

$$V = \frac{\sqrt[n]{\prod_{j=1}^n w_{ij}}}{\sum_{k=1}^n \sqrt[n]{\prod_{j=1}^n w_{kj}}},$$

де $\prod_{j=1}^n w_{ij}$ – добуток всіх елементів рядка;

$\sum_{k=1}^n \sqrt[n]{\prod_{j=1}^n w_{kj}}$ – загальна сума всіх добутоків кожного рядка матриці ймовірностей;

V_i – ймовірність захисту.

Вибір найбільш переважного варіанту антивірусної програми

Для вибору єдиного найбільш ефективного варіанту з отриманих двох варіантів використовуємо додатковий умовний критерій переваги, що базується на мінімізації скалярної цільової функції у вигляді:

$$F(w_1, w_2, \dots, w_m) = \sum_{j=1}^m c_j w_j,$$

де c_j - коефіцієнти відносної важливості показників якості, причому $\sum_{j=1}^m c_j = 1$, w_j - оцінки якісних характеристик.

17

Вибір найбільш переважного варіанту антивірусної програми

Таблиця – Коефіцієнти важливості

№	Якісна характеристика	Коефіцієнт важливості (c_j)
1	Захист	0,5
2	Ефективність	0,3
3	Зручність використання	0,2

Розрахунок значень скалярної цільової функції:

$$F_4 = 0,5 \cdot 6 + 0,3 \cdot 5 + 0,2 \cdot 5 = 5,5;$$

$$F_6 = 0,5 \cdot 5 + 0,3 \cdot 6 + 0,2 \cdot 5 = 5,3$$

Порівнюючи між собою отримані значення скалярних цільових функцій отримуємо максимальне значення у F_4 . В результаті даного порівняння маємо: найбільш переважний варіант антивірусної програми – AhnLab V3 Internet Security.

18

Висновки

- Розглянуто тенденції розвитку антивірусних програм, Законодавство України з питань вірусних/антивірусних програм та проаналізовано вірусні атаки на Україну останніх років.
- Розглянуто характеристики комп'ютерних вірусів та проаналізовані питання організації антивірусної безпеки.
- Виконано порівняльний аналіз сучасних антивірусних програм. В результаті експериментальних досліджень (тестувань) було порівняно роботу цих програм та оцінено кожен з них за такими якісними характеристиками: захист від вірусів, ефективність та зручність використання. Результат аналізу: найбільш переважний варіант антивірусної програми – AhnLab V3 Internet Security.
- Результати роботи апробовано на 25-му Міжнародному молодіжному Форумі "Радіоелектроніка і молодь у XXI столітті" та опубліковано тези доповіді за темою роботи.

ДЯКУЮ ЗА УВАГУ!

ДОДАТОК Б
ПУБЛІКАЦІЯ ЗА ТЕМАТИКОЮ РОБОТИ

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЛЕКТРОНІКИ

МАТЕРІАЛИ 25-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

«РАДІОЕЛЕКТРОНІКА І МОЛОДЬ У ХХІ СТОЛІТТІ»

20 – 22 квітня 2021 р.

Том 4

КОНФЕРЕНЦІЯ

**«ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОКОМУНІКАЦІЙ
ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ ТЕХНОЛОГІЙ»**

Харків 2021

АНАЛІЗ ВИДІВ ЗАХИСТУ ОСОБИСТИХ ДАНИХ ВИКОРИСТОВУЮЧИ АНТИВІРУСНІ ПРОГРАМИ

Вервейко В.В.

Науковий керівник – доц., к.т.н. Чеботарьова Д.В.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інформаційно-мережна інженерія,
тел. (057) 702-13-06)

e-mail: vladyslav.verveiko@nure.ua, +380952174439

The rapid development of information technology is gradually transforming the world. Open and free cyberspace expands the freedom and opportunities of people, enriches society. But there is a downside, which is the theft of personal data, extortion or valuable information.

Having anti-virus programs on your personal computer can, if not prevent, severely prevent a fraudster from accessing information that is personal.

Стрімкий розвиток інформаційних технологій поступово трансформує світ. Відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство. Але є і зворотня сторона, яка являє собою крадіжку особистих даних, виманювання коштів чи цінної інформації.

Маючи на своєму персональному комп'ютері антивірусні програми можна якщо не запобігти, то доволі сильно завадити шахраю дістатися до інформації яка є особистою.

Метою роботи є аналіз видів захисту своїх персональних даних, аби вони не потрапили до рук шахраїв та не були продані на тінювих ресурсах. Тільки у 2020 році у даркнеті було опубліковано більш ніж 386 мільйонів записів користувачів.

Для вирішення задач захисту особистої інформації існують такі антивірусні програми як : BullGuard Internet Security, Kaspersky Internet Security, NortonLifeLock, AhnLab V3 Internet Security, Avast Free AntiVirus, AVG Internet Security, Avira Antivirus Pro, Microsoft Windows Defender.

Для знаходження кращих антивірусів ми будемо перевіряти їх на вміння знаходити вірусні програми та захищати користувача, ефективність – темп роботи та оновлення баз даних і відсутність сбоїв у роботі системи, а також зручність у використанні. В ході виконання роботи було взято 8 антивірусних програм та взявши параметри зазначені вище присвоїв кожному бали. Результат представлений у таблиці.

Таблиця 1 - Порівняльна характеристика антивірусних програм.

Антивірус	Захист	Ефективність	Зручність використання
BullGuard Internet Security	5.9	6	6
Kaspersky Internet Security	6	6	6
NortonLifeLock	5.6	5.8	6
AhnLab V3 Internet Security	6	6	5.5
Avast Free AntiVirus	5.9	6	6
AVG Internet Security	6	6	5.7
Avira Antivirus Pro	6	5.6	6
Microsoft Windows Defender	5.8	5.9	5.9

Підрахунок балів виконано за допомогою формули :

$$V_i = \frac{\sqrt[n]{\prod_{j=1}^N W_{ij}}}{\sum_{i=1}^N \sqrt[n]{\prod_{j=1}^N W_{ij}}} \quad (1)$$

де $\prod_{j=1}^N W_{ij}$ – добуток всіх елементів строк;

$\sum_{i=1}^N \sqrt[n]{\prod_{j=1}^N W_{ij}}$ – загальна сума всіх добутоків кожної строки матриці.

В результаті було знайдено кращу антивірусну програму яка впевнено впоралась із поставленими задачами і може захистити наш комп'ютер від вірусних програм. Kaspersky Internet Security надає найкращий захист і здатний запобігти втрату ваших даних або зараженню комп'ютера.

Відносно цього результату ми можемо прийти до висновку що усі антивіруси спрямовані на протидію шахраям та їх програм, і яким би ви антивірусом не користувались він буде виконувати свою функцію та захищати ваші дані.

Література:

1. К.Є. Кліментьев «Комп'ютерні віруси і антивіруси» ДМК Прес,2013р.
2. С.В. Гошко «Технології боротьби з комп'ютерними вірусами» СОЛОН Прес,2010р.
3. С. Мазаник «Безпека Комп'ютерів» ЕКСМО, 2014р.

АЛФАВІТНИЙ ПЕРЕЛІК

А

Andrii Zhuravka, 14, 16, 18
Ayodele Tega Ajadi, 46

Д

David Ogamune, 16
Denis Zhuravka, 14, 16, 18

Е

Ethel Chila, 18

І

Ikeza Obasi A. D., 44

Ј

Joel Kashaija, 66

О

Okwudili Gene Onukaogu, 14

Р

Pershyn I. V., 22

С

Samad Habib Suhel, 8

Т

Tresor M.A., 42

А

Аль-Вандави Саиф Ахмед Искандар
Исмаель, 104
Ащепков В.О., 119

Б

Безрученко О.Ю., 104
Бельков Е.А., 116
Беленцов А.С., 38
Білик В. О., 26
Білокурова А.О., 40
Богомазов С.А., 129
Бондаренко С.В., 159
Босенко Д.В., 169

Бураківська А. О., 100

В

Варченко М.А., 123
Вервейко В.В., 110

Г

Герус М.А., 68
Гонгарь І. А., 78
Греков І. С., 24

Д

Давиденко Н.В., 112
Дікаленко Д. Д., 36
Добринін К.І., 56
Дученко П.Ю., 153

Є

Єрмолаєв А.А., 88

Ж

Жирна Г.А., 155

З

Запороєв Д.І., 123

К

Каницька І.В., 167
Кепещук Д. Т., 141
Кононов В.Б., 149
Кононова О.А., 149
Коржов И.М., 161
Корнейцова Н.В., 32
Красюкова В.В., 70
Куліченко В.В., 121
Курлан О.О., 90
Кухарчук М.М., 30

Л

Ларіонов В.В., 72
Лісняк О.О., 12
Луценко М.И., 157
Лялічев В. Д., 102

