Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет *Інфокомунікаціїі*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

# КВАЛІФІКАЦІЙНА РОБОТА
# Пояснювальна записка

Рівень вищої освіти *другий (магістерський)*

*Дослідження та порівняльний аналіз антивірусних програм*
(тема)

Виконав:
студент 2 курсу, групи *ІМІм-19-2*
*Вервейко В.В.*

Спеціальності *172 Телекомунікації та радіотехніка*
(код і повна назва спеціальності)
Тип програми *Освітньо-наукова*
(освітньо-професійна або освітньо-наукова)
Освітня програма *Інформаційно-мережна інженерія*
(повна назва освітньої програми)
Керівник *доц., к.т.н. Чеботарьова Д.В.*
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ _____
(підпис) (прізвище, ініціали)

2021 р.

Не містить відомостей, заборонених до відкритого публікування

Студент _____ *Вервейко В.В.*
( підпис ) (прізвище та ініціали)

Керівник _____ *Чеботарьова Д.В.*
( підпис ) (прізвище та ініціали)

Харківський національний університет радіоелектроніки

Факультет *Інфокомунікацій*
(повна назва)

Кафедра *Інформаційно-мережної інженерії*
(повна назва)

Рівень вищої освіти *другий (магістерський)*

Спеціальність *172 Телекомунікації та радіотехніка*
(код і повна назва)

Тип програми *Освітньо-наукова*
(освітньо-професійна або освітньо-наукова)

Освітня програма *Інформаційно-мережна інженерія*
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри ІМІ_____
(підпис)
“____” _____2021 року

# ЗАВДАННЯ
## НА КВАЛІФЛКАЦІЙНУ РОБОТУ

Студентові *Вервейко Владиславу Володимировичу*
(прізвище, ім’я, по батькові)

1. Тема роботи *Дослідження та порівняльний аналіз антивірусних програм*
затверджені наказом університету від 12 березня 2021 року № 350*Ст*
2. Термін подання студентом роботи до екзаменаційної комісії *18 травня 2021 р.*
3. Вихідні дані до роботи
*Дослідити сучасні комп’ютерні віруси та антивірусні програми, проаналізувати сучасні тенденції розвитку антивірусних програм в Україні та світі, розглянути особливості ураження комп’ютерів вірусами та методи організації антивірусної безпеки. Виконати порівняльний аналіз сучасних антивірусних програм.*

4. Перелік питань, що потрібно опрацювати в роботі
*Вступ*
*1. Аналіз розвитку антивірусних програм*
*2. Основні характеристики вірусів*
*3. Організація антивірусної безпеки*
*4. Порівняльний аналіз антивірусних програм*
*Висновки*

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) *Слайди у форматі Power Point (назва, мета і задачі роботи, аналіз розвитку антивірусних програм, хакерські атаки на Україну, класифікація вірусних програм, джерела вірусів, ознаки зараження комп'ютера вірусами, методи і технології захисту від шкідливих програм, вимоги до антивірусних програм, класифікація антивірусних модулів, завдання антивірусних програм, порівняльний аналіз антивірусних програм, розрахунок ймовірності захисту, вибір найбільш переважного варіанту антивірусної програми, висновки)*

## КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів атестаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1 | *Ознайомлення із завданням. Уточнення ТЗ* | *14.03.21* | *виконано* |
| 2 | *Підбір літератури за темою роботи* | *15.03-25.03.21* | *виконано* |
| 3 | *Виконання розділу 1* | *18.03-25.03.21* | *виконано* |
| 4 | *Виконання розділу 2* | *26.03-04.04.21* | *виконано* |
| 5 | *Виконання розділу 3* | *05.04-27.04.21* | *виконано* |
| 6 | *Виконання розділу 4* | *28.04-7.05.21* | *виконано* |
| 7 | *Оформлення пояснювальної записки* | *08.05-10.05.21* | *виконано* |
| 8 | *Оформлення презентаційного матеріалу,* | *11.05-18.05.21* | *виконано* |
| | *підготовка до захисту у ЕК* | | |
| | | | |
| | | | |
| | | | |
| | | | |

Дата видачі завдання *13.03.2021 р.*

Студент _____ *Вервейко В.В.*
( підпис ) (прізвище та ініціали)

Керівник роботи _____ *Чеботарьова Д.В.*
( підпис ) (прізвище та ініціали)

# РЕФЕРАТ

Пояснювальна записка: 68 с., 27 рис., 4 табл., 22 джерела, 2 додатки.

Об'єкт дослідження – антивірусні програми.

Мета роботи – дослідження сучасних антивірусних та вірусних програм, порівняльний аналіз антивірусних програм.

Результати – в роботі досліджено сучасні комп’ютерні віруси та антивірусні програми, проаналізовано сучасні тенденції розвитку антивірусних програм в Україні та світі, розглянуто особливості ураження комп’ютерів вірусами та методи організації антивірусної безпеки. Виконано порівняльний аналіз сучасних антивірусних програм та вибір найбільш переважної антивірусної програми з використанням умовного критерію переваги.

АНТИВІРУСНА ПРОГРАМА, КОМП’ЮТЕРНИЙ ВІРУС, АТАКА, КІБЕРБЕЗПЕКА, ЗАХИСТ, ПЕРСОНАЛЬНИЙ КОМП’ЮТЕР

# THE ABSTRACT

Explanatory note: 68 p., 27 fig., 4 tabl., 22 sources, 2 app.

The object of the study is the antivirus programs

The purpose of the work is the research of modern anti-virus and virus programs, comparative analysis of anti-virus programs.

Results - modern computer viruses and anti-virus programs are studied in the work, modern tendencies of development of anti-virus programs in Ukraine and the world are analyzed, features of defeat of computers by viruses and methods of organization of anti-virus security are considered. A comparative analysis of modern antivirus programs and the selection of the most preferred antivirus program using the conditional criterion of preference.

ANTI-VIRUS PROGRAM, COMPUTER VIRUS, ATTACK, CYBER SECURITY, PROTECTION, PERSONAL COMPUTER

ЗМІСТ

С.

AVS (Anti-Virus Safety) – антивірусна безпека;
КС – комп`ютерна система;
ОС – операційна система;
ПЕОМ – персональна електро обчислювальна машина;
ПЗ – програмне забезпечення;
ПК – персональний комп`ютер;
ПНП – потенційно небажана програма;
ПНПЗ – потенційно небажане програмне забезпечення.

# ВСТУП

В наш час все більш популярним стає використання комп’ютерів, інтернету, соціальних мереж, електронних сервісів, електронних фінансових системам тощо. Все це дозволяє швидко і ефективно задовольняти потреби людства. Але окрім великих переваг цифровізації та інформатизації суспільства існує багато загроз. Можливість втрати або спотворення даних, електронний шпіонаж, шахрайство, шантаж та навіть кібертероризм стали чи не головними викликами сучасної безпеки. Однією з основних причин цих негативних явищ є комп’ютерні віруси.

На тлі все більшої популярності інтернету, все досконалішими стають і вірусні програми. Потенційною жертвою кібер-злочинців є фактично кожен користувач. Щодоби у світі з'являється 100 тисяч нових вірусів. Їх створюють хакери - висококваліфіковані програмісти, які займаються несанкціонованим проникненням в комп'ютерні мережі, бази даних та зломом програмного забезпечення. Саме тому актуальною робота, присвячена дослідженню антивірусних програм.

За останні роки з боку Російської Федерації проти України здійснено понад 7 тисяч кібератак. Їхня головна мета – дестабілізувати ситуацію в державі. Такі кібератаки наносять непоправної шкоди різним галузям (електропостачання, інфокомунікації, банківські та фінансові операції), крім того сприяють величезним фінансовим збиткам. РФ постійно організовує кібернетичні операції проти об'єднання критичної інфраструктури, приватного сектору, а також інфокомукаційних систем Збройних Сил України. Всі ці факти підтверджують актуальність даної роботи.

Метою даної роботи є дослідження сучасних вірусних і антивірусних програм та порівняльний аналіз антивірусних програм.

# 1 АНАЛІЗ РОЗВИТКУ АНТИВІРУСНИХ ПРОГРАМ

## 1.1 Еволюція антивірусних програм

Поява перших комп’ютерних вірусів відбулася наприкінці 70-х рр XX століття. Вже у 1981 р. з’явилися вірусні програми, що представляли серйозну загрозу даним. А у 1984 р. Енді Хопкінсом були створені найперші антивірусні програми: CHK4BOMB і BOCHK4BOMB. Програма CHK4BOMB виконувала сканування тексту модуля завантаження для виявлення підозрілих ділянок і текстових повідомлень в коді. Програма BOCHK4BOMB здійснювала перехоплення записів і форматування, що виконувалося через BIOS. Небажану операцію можна було як заборонити, так і дозволити. Перша антивірусна програма для захисту від атак вірусів була створена Джі Вонгом в 1985 р і носила назву DRPROTECT. Вона блокувала всі операції (форматування, запис), що виконуються через BIOS. При виявленні будь-якої операції було потрібне перезавантаження системи.

Антивіруси до 90-років були своєрідним набором зразків вірусних кодів, які зберігаються безпосередньо в самій програмі. У антивірусі передбачався пошук в файлах збережених зразків. Але подібні зразки не шифрувалися авторами, тому антивірусні програми при скануванні один одного знаходили їх і відносили до вірусів. Згодом інтерес до антивірусних програм стали проявляти великі компанії, що мають в наявності величезний штат програмістів.

У 1992 р. створено новий антивірус MtE, який є доступним як для досвідчених, так і для починаючих програмістів. MtE виступав в ролі генератора поліморфного (постійно мінливого) коду. Поліморфні віруси з'являлися буквально кожен день. Виправити ситуацію зміг емулятор коду, завдяки якому антивірусна програма обходила стороною зашифровану частину і підбиралася до самого вірусу. Першою подібною програмою з емулятором коду є AVP (створена програмістом Касперським). Ця прогрмама ефективно боролася зі зростаючою кількістю вірусів. Одночасно з'явилися і системи захисту (поведінковий блокатор, статистичний аналіз, евристичний аналізатор і криптоаналіз), принцип роботи яких використовується і до цього дня.

Поява багатозадачної системи Windows і складних програм посилило вимоги, що пред'являються до антивірусних програм, одним із завдань яких була організація перевірки файлів при зверненні до них. Швидке поширення Інтернету і поява вірусів, що маскуються під стандартні програми, підштовхнуло розробників антивірусного програмного забезпечення на впровадження файерволів. Сьогодні також продовжується боротьба з вірусними програмами. В даний час відомо про наявність близько 60 компаній, що займаються розробкою нових антивірусів як платного, так і безкоштовного характеру [1].

## 1.2 Сучасні тенденції розвитку антивірусних програм

Сучасні віруси здатні знищувати, пошкоджувати або викрадати дані, погіршувати або повністю унеможливлювати працездатність операційної системи пристрою. Крім того комп'ютерні віруси мають здатність до прихованого самопоширення.

З розвитком таких технологій, як блокчейн, онлайн-транзакції, платформи для обміну цифровими файлами, різновид кіберзагроз постійно зростає. Згідно зі звітом Verizon про витік даних, опублікованому в 2020 році, 86% всіх порушень було скоєно на фінансовому ґрунті, 22% - було пов'язано з фішингом. З них 37% - це крадіжка і використання облікових даних [2].

Фахівці IT-безпеки формулюють тенденції в розвитку кібербезпеки, і фактори, такі як напрями в бізнесі, впровадження технологій і нормативних вимог, допомагають їм в цьому: підприємства переносять послуги і дані в хмару, моделі штучного інтелекту і машинного навчання перебувають на піку свого розвитку, держави вводять нові нормативні вимоги [3].

Організації, що займаються питаннями кібербезпеки, уважно стежать за тенденціями розвитку її технологій і знаходять інноваційні способи вбудовування функцій безпеки в продукти для протидії загрозам [3]. Основні тенденції розвитку кібербезпеки, в тому числі і антивірусних програм, наведено на рис. 1.1.

Як перспективу розвитку антивірусних програм вчені припускають, що антивірусні програми еволюціонують в бік розробки інструментів прогнозування вірусних атак. Співробітник британської лабораторії компанії

Hewlett-Packard Метью Вільямсон припускає, що антивірус може відслідковувати стабільність роботи системи відповідно до встановлених адміністратором прав і правил. І хоча вже є кілька програм, які працюють по цьому принципу (наприклад, антивірус Viguard), вирішити проблему на рівні рядових користувачів вони поки не можуть [4].

Рисунок 1.1 – Основні тенденції розвитку кібербезпеки та антивірусних програм

До основних факторів, що сприяють сьогодні швидкому розвитку ринку кібербезпеки та антивірусних програм, відносяться наступні:

- швидке розгортання веб-і хмарних додатків;
- постійно зростаюча потреба підприємств у зниженні ризиків і строгому дотриманні нормативних вимог;
- збільшення частоти кібератак в усьому світі.

## 1.3 Законодавство України з питань вірусів та антивірусних програм

До нормативно-правової бази, що регулює галузь забезпечення кібербезпеки, відносяться документи, наведені на рис. 1.2.

Рисунок 1.2 – Нормативно-правова база галузі кібербезпеки України

В законодавстві України [5, 6] визначені основні терміни даної галузі, що наведені на рис. 1.3.

Рисунок 1.3 – Основні терміни галузі забезпечення кібербезпеки

Одним з основних законів в галузі боротьби з комп'ютерними вірусами є Закон України «Про основні засади забезпечення кібербезпеки України» [5].

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 [5].

## 1.4 Вірусні атаки на Україну

Останні роки Україна переживає інформаційну війну, одним з доказів якої є величезна кількість кібератак на українські мережі, компанії, підприємств, банки тощо. 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 (електропостачання, інфокомунікації, банківські та фінансові операції), крім того сприяють величезним фінансовим збиткам. РФ постійно організовує кібернетичні операції проти об'єднання критичної інфраструктури, приватного сектору, а також інформаційно-телекомукаційних систем Збройних Сил України [6].

23 грудня 2015 року в Івано-Франківську до диспетчерів "Прикарпаттяобленерго" почали надходити дзвінки про знеструмлення споживачів. Підстанції області одна за одною виходили з ладу, а диспетчери не мали змоги контролювати цей процес. Про те, що це хакерська атака стало зрозуміло за кілька хвилин [6]. Зловмисники встигли вимкнути понад 10 підстанцій. Знеструмленими залишились 100 населених пунктів Прикарпаття, ще понад дві сотні частково втратили живлення майже на годину, а без світла залишились понад 200 тисяч українців. Відімкнення такої величезної кількості електромереж відбулося вперше у світі. Вже потім фахівці з'ясували з ладу системи управління вивів запущений ззовні вірус під назвою BlackEnergy. У його використанні були помічені російські хакери.

Наймасштабніша хакерська атака з боку Російської федерації проти України відбувалась у 2017 р. Основні моменти даної атаки наведено на рис.1.4.

Рисунок 1.4 – Наймасштабніша хакерська атака з боку РФ проти України

Як видно з рис. 1.4, все почалося з компрометації системи оновлення програми M.E.Doc. Згодом фахівці назвали це втручання в роботу комп'ютерних мереж і чи не найбільшою кібератакою за останні роки. Тоді Україна виявилась не готовою – компанії кілька днів відновлювали втрачену інформацію, збитки оцінили у 10 мільярдів доларів, а спіймати хакерів так і не вдалося [7].

Варто також відмітити вірус Bad Rabbit - шифрувальник, який в жовтні 2017 р. атакував київське метро та аеропорт Одесса. Він маскувався під поновлення Adobe Flash. За розблокування одного персонального комп'ютера вірус вимагав 6500 гривень, які потрібно було відправити на рахунок творців «кролика» протягом 48 годин. Що буде у разі відмови внести гроші, не уточнювалося,а Bad Rabbit відправився далі, напавши на комп'ютери в Туреччині та Німеччині. За словами експертів декількох компаній, які зазнали атаки «кролика», він являє собою доопрацьовану версію вірусу NotPetya. Вихідний код цих двох програм, в результаті перевірки, збігся на 13%. NotPetya,який був створений у 2017 році і атакував комп'ютери в 65 країнах світу, торкнувшись, в тому числі, енергетичний і банківський сектори України. Обидва віруси відрізняються тим, що не знищують інформацію на комп'ютері, а тільки шифрують її.

# 2 ОСНОВНІ ХАРАКТЕРИСТИКИ КОМП’ЮТЕРНИХ ВІРУСІВ

Перша масова епідемія комп'ютерного вірусу сталася в 1986 р., коли дискети перших масових ПК заражав вірус Brain.

Дуже швидко комп’ютерні віруси почали розвиватися з 1994р. У січні 1994р. з’явився вірус Shifter, що заражав об’єктні модулі (OBJ-файли). У квітні 1994 р. було створене сімейство вірусів SrcVir, що заражають вихідні тексти програм. У червні 1994 р. з’являється складний поліморфний вірус OneHalf, що викликав глобальні проблеми в усьому світі. OneHalf заражав завантажувальні сектори дисків й COM/EXE-файли, збільшуючи їхній розмір на 3544, 3577 або 3518 байта, залежно від модифікації. При кожному перезавантаженні зараженого комп’ютера зашифровувалися два останніх незашифрованих раніше циліндри жорсткого диска. Це тривало доти, поки весь вінчестер не виявлявся зашифрованим. Однак при першій же спробі лікування, вся інформація на вінчестері ставала недоступною, без можливості відновлення.

У лютому 1995 р. стався відомий інцидент у корпорації Microsoft - перед випуском нової ОС Windows 95 була розіслана демонстраційна дискета, заражена завантажувальним вірусом Form. Копії цього диска одержали 160 бета-тестерів, один із яких не полінувався провести антивірусну перевірку.

Наймасштабнішою шкідливою програмою останніх років можна назвати вірус-хробак WannaCry, який шифрує всю інформацію, що знаходиться на комп'ютері, а за її розшифровку вимагає гроші, причому, через три дні бездіяльності з боку потерпілого, він збільшує необхідну суму в два рази, а через тиждень - шифрує файли назавжди.

Він почав роботу з британської лікарні напавши на її комп'ютери, потім попрямував в Іспанію і Португалію, загальмувавши роботу телефонних компаній, а пізніше добрався і до країн СНГ, де паралізував роботу комп'ютерів Міністерства внутрішніх справ і Слідчого комітету цих країн. Всього цей вірус завдав шкоди близько 500 тис. комп'ютерів в 74 країнах світу, причому на поширення у нього пішло всього дві години. Це була, можливо, найбільша вірусна атака в історії людства. За даними компанії Microsoft за створенням WannaCry стоїть уряд Північної Кореї.

Серед вірусів також можна відзначити Black Hat Europe (2018 р.), який може вразити будь-яку версію Windows, при цьому залишаючись невидимим для антивірусів, оскільки його код знаходиться в оперативній пам'яті, не залишаючи слідів на жорсткому диску.

Найбільш дивним з комп'ютерних вірусів є вірус, який атакує комп'ютери, шифруючи дані на них, а для розшифровки просить пограти в корейську гру PUBG, пропонуючи також альтернативний варіант - ввести код. Після цього починається розшифровка файлів. Якщо людина вибирає перший варіант, то йому достатньо просто запустити гру, і вірус залишає поле бою. Цей вірус схожий на оригінальний спосіб реклами.

## 2.1 Класифікація вірусних програм

В даний час відомо понад 50 тисяч комп’ютерних вірусів. Для системи віруси можуть бути від зовсім нешкідливими, які крім саморозмноження загрози не становлять, а можуть бути фатальними, що призводять до краху всієї системи.

Класифікацію комп’ютерних вірусів за принципом дії наведено на рис. 2.1.

Рисунок 2.1 – Класифікація комп’ютерних вірусів за принципом дії

Взагалі, існує декілька класифікацій комп'ютерних вірусів [8 – 12]. Найбільш відомими є класифікації вірусних програм за середовищем існування (рис. 2.2), за способом зараження (рис. 2.3), за ступенем впливу (рис. 2.4) та за особливостями алгоритмів (рис. 2.5).

Рисунок 2.2 – Класифікація вірусних програм за середовищем існування

Рисунок 2.3 – Класифікація вірусних програм за ступенем впливу

Рисунок 2.4 – Класифікація вірусних програм за способом зараження

Рисунок 2.5 – Класифікація вірусних програм за особливостями алгоритмів

Крім того існують інші різновиди вірусних програм: зомбі, шпигунські програми (фітинг, фармінг), мобільні віруси тощо.

Знання класифікації комп'ютерних вірусів дозволяє оцінити ступінь загрози, метод боротьби і рівень необхідного захисту програмнго забезпечення від шкідливих впливів.

2.2 Ураження комп’ютерів вірусами

Ознаки зараження комп'ютера вірусами наведено на рис. 2.6.

Рисунок 2.6 - Ознаки зараження комп'ютера вірусами

На даний момент існує велика кількість джерел, звідки можливе отримання вірусу:

- 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 зовнішній диск (зокрема флеш-пам’ять);
- програмні продукти, придбані нелегальним шляхом.

Віруси легко поширюються у вкладках повідомлень електронної пошти і миттєвих повідомлень. Віруси можуть поширюватися під виглядом забавних

картинок, вітальних листівок, аудіо- та відеофайлів. Крім того, їх можна завантажити з Інтернету разом з неліцензійним програмним забезпеченням або іншими файлами і програмами.

Якщо не вживати заходів щодо захисту від вірусів, то наслідки зараження можуть бути дуже серйозними.

Виникають ситуації, коли раптом з`являються дратівливі реклами, різко падає продуктивніст комп’ютера, відбувається зависання або проблеми з файловою системою. В більшості випадків саме віруси стають причиною падіня швидкості роботи ПК та погіршення його працездатності.

При зараженні комп'ютера перш за все важливо виявити вірус. Для цього необхідно знати про основні ознаки прояву вірусів. Існує 11 основних видів відображення вірусів на роботі ПК, що наведені на рис. 2.7.

Для профілактики розвитку шкідливого зараження треба дотримуватись наступних правил:

- не клікати по спливаючим вікнам;
- не відповідати на небажані повідомлення;
- проявляти особливу пильність при завантаженні безкоштовних додатків з різних сайтів.

Якщо збої в роботі ПК викликані шкідливим зараженням, треба виконати повне сканування системи антивірусом або антивірусним сканером.

Неважливо, який різновид має вірус і як він потрапив на комп'ютер, перш за все слід видалити його і запобігти подальшому зараженню.

Рисунок 2.7 – Основні види відображення вірусів на ПК

## 2.3 Особливості різних видів вірусних програм

Кількість нових комп’ютерних вірусів постійно зростає. Для мінімізації шкоди та втрати даних в багатьох країнах приймають спеціальні закони про боротьбу з комп’ютерними злочинами та виконують розробку спеціальних антивірусних програм та технічних засобів захисту від комп’ютерних вірусів.

Програмні віруси характеризуються своїми особливими відмінностями та характеристиками. Основні види вірусних програм наведено на рис. 2.8.

Рисунок 2.8 – Особливості різних вірусних програм

# 3 ОРГАНІЗАЦІЯ АНТИВІРУСНОЇ БЕЗПЕКИ

## 3.1 Методи організації антивірусної безпеки

Політика антивірусної безпеки завжди була вирішальною компонентою в системах захисту інформації в комп'ютерних системах (КС) і мережах. Вона передбачає забезпечення надійного та ефективного захисту проти будь-яких вірусних атак (потенційно загрозливих, реальних, перспективних) [13]. Поява в антивірусах евристичного режиму виявлення нових вірусів з невідомими їх сигнатурами та алгоритмами деструктивних дій надало можливість використовувати цей режим для імовірної кількісної оцінки стану антивірусної безпеки [13]. З 1999 р. регулярно виконуються огляди та тестування брендів антивірусного захисту (табл. 3.1).

Метод прогнозування антивірусної безпеки КС за вимогами запропонованих правил AVS (Anti-Virus Safety) полягає у послідовності здійснення наступних етапів:

– здійснюється прогнозування;

– визначаються об'єкти антивірусного захисту КС;

– визначається аналітичний метод кількісної оцінки ризику антивірусної безпеки;

– здійснюється прогнозування антивірусної безпеки КС та її кількісне експертне оцінювання.

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 [13]. Перш за все це визначення загроз та видів вірусів, визначення об'єктів антивірусного захисту та комплектів антивірусних програм для кожного з них.

Модель політики антивірусної безпеки КС наведено на рис. 3.1.

Таблиця 3.1 - Можливості світових брендів антивірусних програм

| Найменування антивірусної програми | Фірма-провайдер, її адреса | Відсоток 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, 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 |

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 [13]. Спеціальними вірусами визначаються різні шкідливі програми – конструктори вірусів, генератори вірусних атак, вірусні утиліти тощо [13]. Перспективними визначаються New-віруси, Win32-віруси, DoS-віруси, Mobil-віруси, Spiware-віруси, віруси проактивних деструктивних дій тощо [13].

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, блокиратори поведінки, статистичні методи [13].

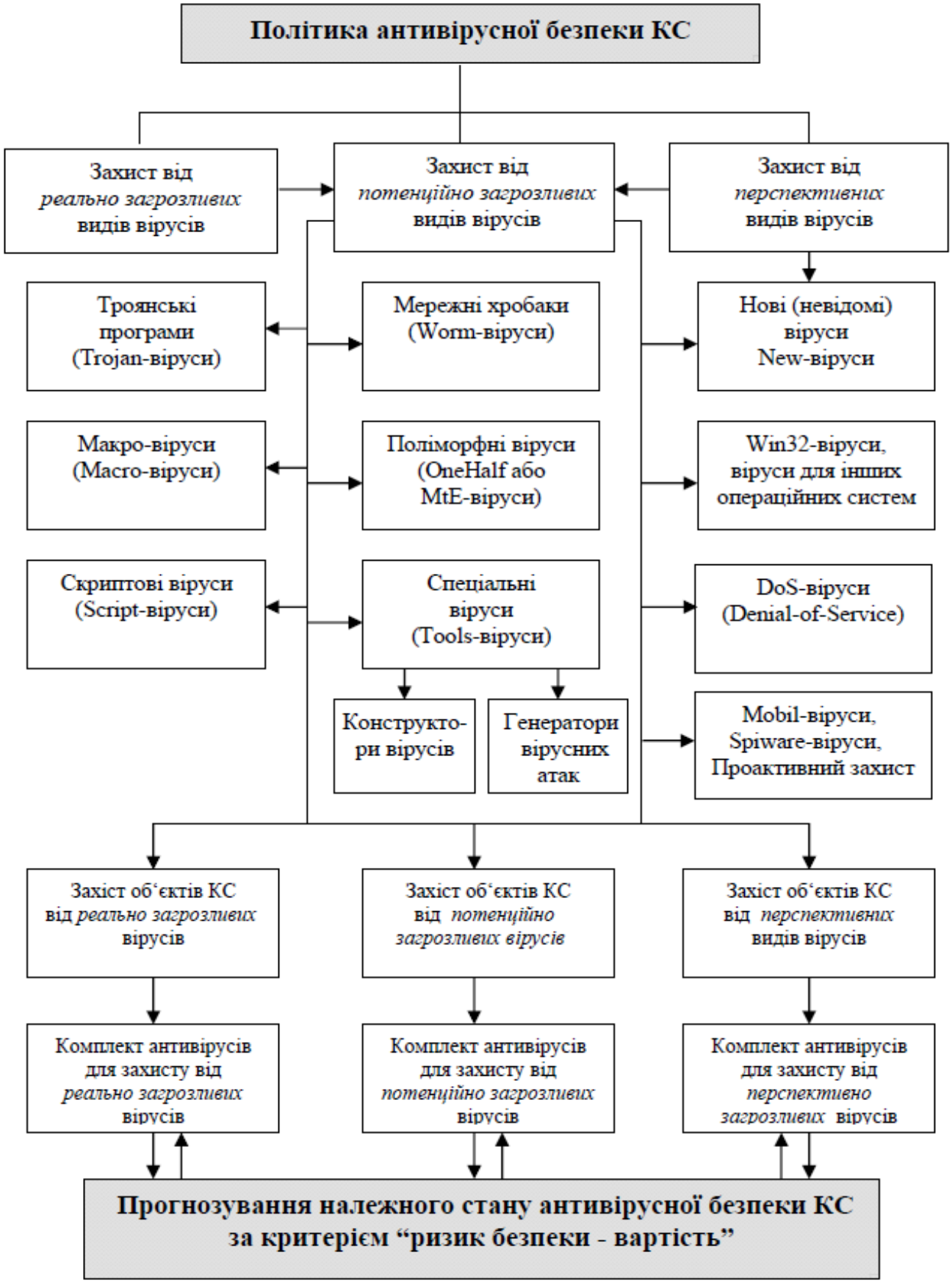

Рисунок 3.1 – Модель політики антивірусної безпеки КС

Далі визначаються об‘єкти антивірусного захисту КС. Політика антивірусної безпеки кожного об‘єкту КС повинна забезпечуватись на рівні не менш заданого за критерієм "ризик антивірусної безпеки-вартість" [13].

Вона реалізується вибором антивірусів за їх можливостями згідно з даними довідкових таблиць антивірусного захисту КС, тестових рейтингів і балів та прогнозуванням антивірусної безпеки методом AVS-правил, тобто використанням певного аналітичного методу і математичних співвідношень [13].

Метод AVS-правил є подальшим розвитком відомих моделей і правил захисту Biba (1977 р.), GougenMeseguer (1982 р.), Sutherland (1986 р.), Clark-Wilson (1989 р.), при цьому модель Кларка-Вильсона вважається однією з найкращих щодо підтримки цілісності інформаційних систем [13]. Метод AVS-правил забезпечує прогнозування антивірусної безпеки КС за даними значень показника Pn в табл. 3.2, які постійно і регулярно доповнюються та оновлюються AVS-фахівцями.

Аналітичний метод кількісної оцінки ризику антивірусної безпеки для кожного з видів вірусів визначається згідно з моделлю політики антивірусної безпеки (рис. 3.1).

Далі здійснюється прогнозування антивірусної безпеки КС та її кількісне експертне оцінювання методом AVS-правил за математичними виразами (3.1) – (3.4) для основних видів вірусів згідно з моделлю політики антивірусної безпеки (рис. 3.1). Модель політики антивірусної безпеки повинна постійно доповнюватись та удосконалюватись.

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

, (3.1)

де *Pn* – імовірність виявлення і знешкодження відомих і невідомих вірусів n-ю антивірусною програмою за результатами її тестових випробувань згідно з даними табл. 3.2;

*N* – кількість антивірусів в робочому комплекті, яким забезпечується

антивірусний захист робочої станції/ПЕОМ [13].

Таблиця 3.2 – Можливості антивірусних програм світових брендів

| Найменування антивірусної програми | Розробник | Постачальник | Вартість (доларів) | 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 | так (мережний антивірус) | 11,4 | 99 % (0.99) |
| McAfee VirusScan 7.02.6000 | Network Associates Technology | компанія "ЦЕБІТ" | 64 | так (мережний антивірус) | 7,08 | 95 % (0.95) |
| RAV AntiVirus Desktop 8 | GeCAD Software (Румунія) | Через Веб-сайт виробника | 29 | так (мережний антивірус) | 6,85 | 94 % (0.94) |
| PandaAntivirus Platinum 7.04.00 | Panda Software | Через Веб-сайт виробника | 75 | так (мережний антивірус) | 4,5 | 90 % (0.9) |
| PCcillin 2003 | Trend Micro (Китай) | компанія "ЦЕБІТ" | 55 | так (мережний антивірус) | 11,75 | 87 % (0.87) |
| NAV Antivirus 2003 Version 9.00.40 | Symantec | компанія "ЦЕБІТ" | 45 | так (мережний антивірус) | 10,01 | 82 % (0.82) |
| DrWeb for Windows Version 4.29b | ЗАО "Діалог Наука" | компанія "ЦЕБІТ" | 66 | так (мережний антивірус) | 7,04 | 81 % (0.81) |
| UNA 1.61.0.97 | Український націон. центр | Український націон. центр | 25 | так (мережний антивірус) | 4,2 | 72 % (0.72) |
| AVG 6.0 AntiVirus System | GriSoft Inc. (Чехія) | Через Веб-сайт виробника | 40 | так (мережний антивірус) | 12,2 | 52 % (0.52) |

Аналогічно співвідношенню (3.1) оцінюється ризик антивірусної безпеки від атак Linux-вірусів, мережних хробаків, троянських програм, макро-вірусів, скриптових вірусів, спеціальних вірусів, поліморфних вірусів, DoS-вірусів, нових невідомих вірусів та мобільних вірусів.

Таким чином, згідно з (3.1) прогнозується ризик антивірусної безпеки кожного об‘єкту КС вибором антивірусів та їх кількості в антивірусному комплекті згідно з даними табл. 3.1 і табл. 3.2. Такі таблиці мають регулярно доповнюватись та уточнюватись. Вартість антивірусу оцінюється окремо при її наявності у довідкових таблицях за результатами тестових випробувань, а також за іншими даними [13].

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:

(3.2)

(3.3)

$$Rкс = 1 – Pкс, \tag{3.4}$$

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;
*Pп* – показник згідно формули (3.1);
*Rкс* – ризик антивірусної безпеки КС.

## 3.2 Методи і технології захисту від шкідливих програм

Для захисту від шкідливих програм і комп'ютерного шахрайства існують і застосовуються різні методи боротьби з ними. Це методи юридичні, освітні та технічні.

У всіх комп'ютеризованих країнах прийняті закони, що забороняють створення і поширення вірусів і інших типів шкідливих програм. Часто подібні злочини скоюються технічними грамотними фахівцями, і це досить серйозно ускладнює розслідування злочину. Саме тому, юридичними методами можна знизити загальний рівень комп'ютерної злочинності - але повністю перемогти не можна.

Другим важливим методом захисту від комп'ютерних зловмисників є утворення користувачів, з'ясування і суворе дотримання основних правил поведінки в мережі. Всього є три основних правила, які працюють як для домашніх, так і для корпоративних ПК (рис. 3.2).

Рисунок 3.2 – Правила захисту від вірусних атак

## 3.3 Вимоги до антивірусних програм

Кількість і різноманітніття вірусів дуже великі. Тому для швидкого та ефективного виявлення вірусів, антивірусна програма повинна відповісти вимогам, що наведені на рис. 3.4.

Рисунок 3.4 – Вимоги до антивірусних програм

# 4 ПОРІВНЯЛЬНИЙ АНАЛІЗ АНТИВІРУСНИХ ПРОГРАМ

## 4.1 Різновиди та типи антивірусних програм

Антивірусні програми використовують два певних принципи роботи з шкідливим ПЗ, які наведено на рис. 4.1.

Рисунок 4.1 - Принципи роботи з шкідливим ПЗ, що використовують антивірусні програми

Класифікацію антивірусних модулів, які входять в склади різних антивірусних програм, наведено на рис. 4.2.

Антивірусні програми поділять на чисті антивіруси і антивіруси подвійного призначення.

Чисті антивіруси відрізняються наявністю антивірусного ядра, яке виконує функцію сканування за зразками. Принциповим в цьому випадку є те, що лікування можливе у випадку, якщо вірус є відомим. Чисті антивіруси, в свою чергу, поділяються на дві категорії за типом доступу до файлів: антивірусні програми, що здійснюють контроль при доступі або на вимогу користувача.

Програми подвійного призначення - це програми, які використовуються як в антивирусах, так і в ПЗ, яке не є антивірусом. Різновидом програм подвійного призначення є поведінкові блокатори, що аналізують поведінку інших програм і блокують їх при виявленні підозрілих дій.

Рисунок 4.2 – Класифікація антивірусних модулів

Антивірусні програми захищають ПК від вірусів та шкідливого ПЗ. Антивірусні модулі захисту перевіряють всі файли в режимі реального часу, тобто як тільки файли потрапляють на комп'ютер. Модуль веб-захисту

намагається запобігти доступ до шкідливих сайтів. Антивірусний сканер на вимогу користувача перевіряє всі локальні дані на наявність можливих заражень.

Використання антивірусних програм, зовсім не означає, що комп'ютер захищений на сто відсотків. Інколи необхідне повне перевстановлення ОС, що впорається з виниклою інфекцією набагато швидше і якісніше, ніж перевірка і лікування антивірусною програмою.

Основні завдання антивірусних програм наведено на рис. 4.3.

Рисунок 4.3 - Основні завдання антивірусних програм

## 4.2 Актуальні антивірусні програми

Виділимо 8 найактуальніших антивірусів які будуть розглянуті у данній роботі. Часто користуючись основою цих антивірусів з`являються прототипи, які несуть захист користувачам.

BullGuard Internet Security - антивірусний комплекс від англійської компанії Bullguard (рис. 4.4). Програма поєднує в собі антивірус, мережний екран і утиліту резервного копіювання. Bullguard також надає 5 ГБ місця на власному сервері для зберігання резервних копій. Як антивірусний движок використовується такий від компанії BitDefender і файрвол Outpost [14].

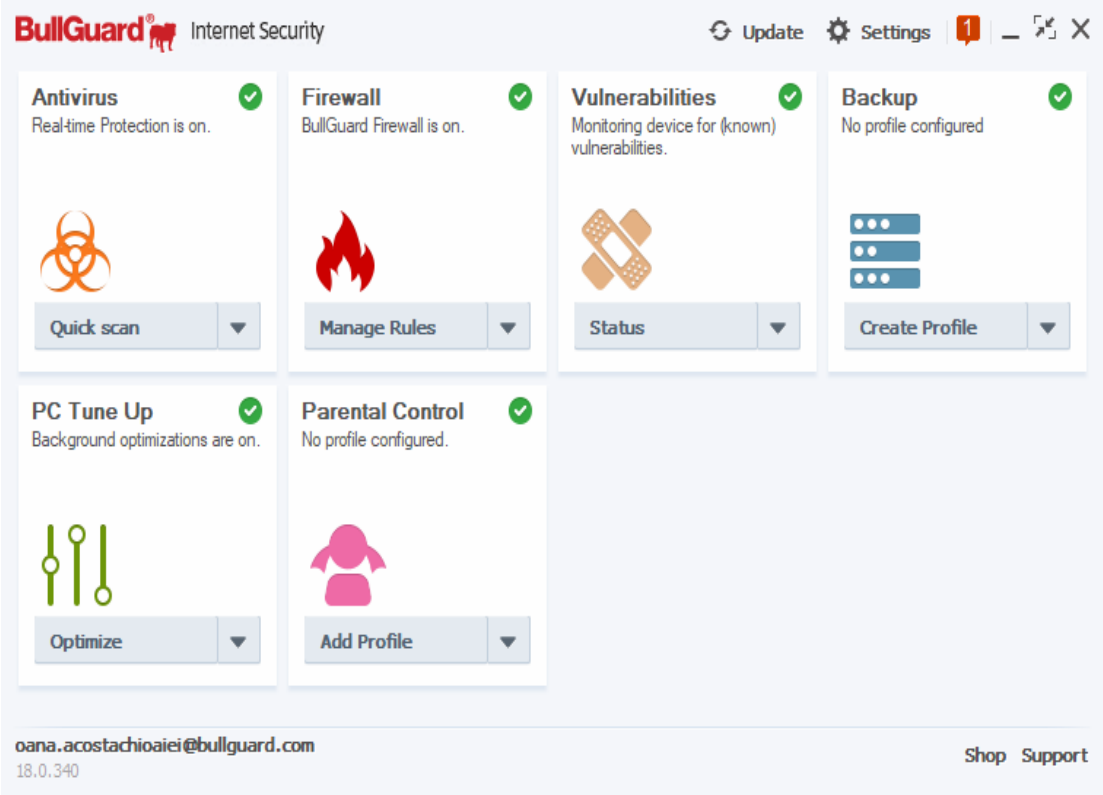


Рисунок 4.4 - BullGuard Internet Security

Bullguard Internet Security складається з наступних компонентів :

- антивірус і антишпигун на движку BitDefender
- мережевий екран;
- фаєрвол від Outpost;
- антиспам;
- утиліта резервного копіювання;
- батьківський контроль;
- оптимізація системи [14].

Kaspersky Internet Security (рис. 4.5) - лінійка програмних продуктів, розроблена компанією «Лабораторія Касперського» на базі «Антивірус Касперського» для комплексного захисту домашніх персональних комп'ютерів і мобільних пристроїв в реальному часі від відомих і нових загроз [15].

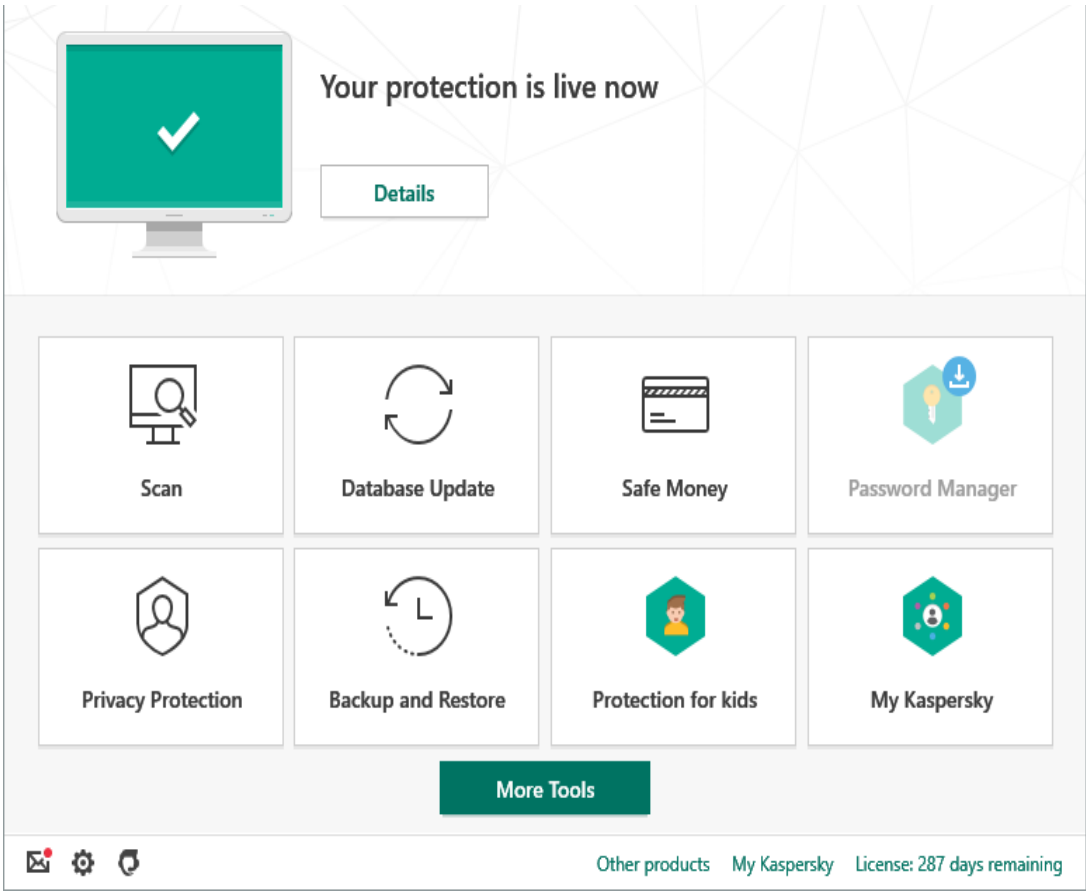


Рисунок 4.5 – Kaspersky Internet Security

У продукті реалізовані наступні основні функції:

1) гібридний антивірусний захист в реальному часі, який поєднує в собі можливості:

- традиційних сигнатурних технологій;
- сучасних технологій (проактивні евристичні методи);
- хмарних технологій;

2) захист від експлойтів для запобігання використання вразливостей на комп'ютері;

3) функція відкоту, що дозволяє усунути наслідки діяльності шкідливих програм;

4) кошти від інтернет-шахрайства (зокрема, фішингу та кейлоггеров) для підвищення ступеня захисту особистих даних та іншої цінної інформації;

5) захист даних при виконанні фінансових операцій в інтернеті:

- користуванні системами онлайн-банкінгу;
- користуванні платіжними системами (зокрема, PayPal);

- здійсненні покупок в інтернеті;

6) захист від мережних атак хакерів;

7) контроль змін (повідомляє про підготовлювані зміни параметрів браузера, в тому числі викликаних установкою рекламних програм, панелей інструментів);

8) захист від збору даних (забороняє сайтам відстежувати сценарії користування інтернетом і збирати особисті дані);

9) контроль інтернет-трафіку (допомагає оптимізувати витрати при підключенні до інтернету через Wi-Fi, 3G і 4G) [15].

NortonLifeLock (рис. 4.6) - американська компанія, що створює ПЗ в галузі інформаційної безпеки, в тому числі і антивірусні програми [16].


Рисунок 4.6 – NortonLifeLock

AhnLab V3 Internet Security (рис. 4.7) - комплексний антивірус, заснований на хмарних технологіях і повнофункціональним рішенням безпеки для захисту комп'ютера та інформації від постійно виникаючих електронних інтернет-загроз і мережевих атак [17].

AhnLab V3 Internet Security надає необхідні функції для здійснення безпеки інформації на комп'ютері і обмеження доступу до системних ресурсів.Комплексне рішення також запобігає установку небажаних програм і шкідливих інтернет-загроз в вашу систему, пропонуючи розширені настройки захисту.Основні переваги AhnLab V3 Internet Security: захист системи від впливу в режимі реального часу, управління політиками мережевої безпеки, фільтрація шкідливого веб-змісту і вкладень електронної пошти, оптимізація системи, система самозахисту V3 і технологія TrueFind для виявлення прихованих загроз – руткітів [17].

Avast (рис. 4.8) — антивірусна програма для ПК на базі ОС Windows, macOS та Linux, а також для смартфонів і планшетів на базі Android та iOS. Розроблена компанією AVAST Software, яка була заснована 1991 р. в Чехії. Головний офіс компанії знаходиться у Празі. Випускається у вигляді кількох версій: платних Pro, Internet Security і Premier та безкоштовної Free для некомерційного використання [18].

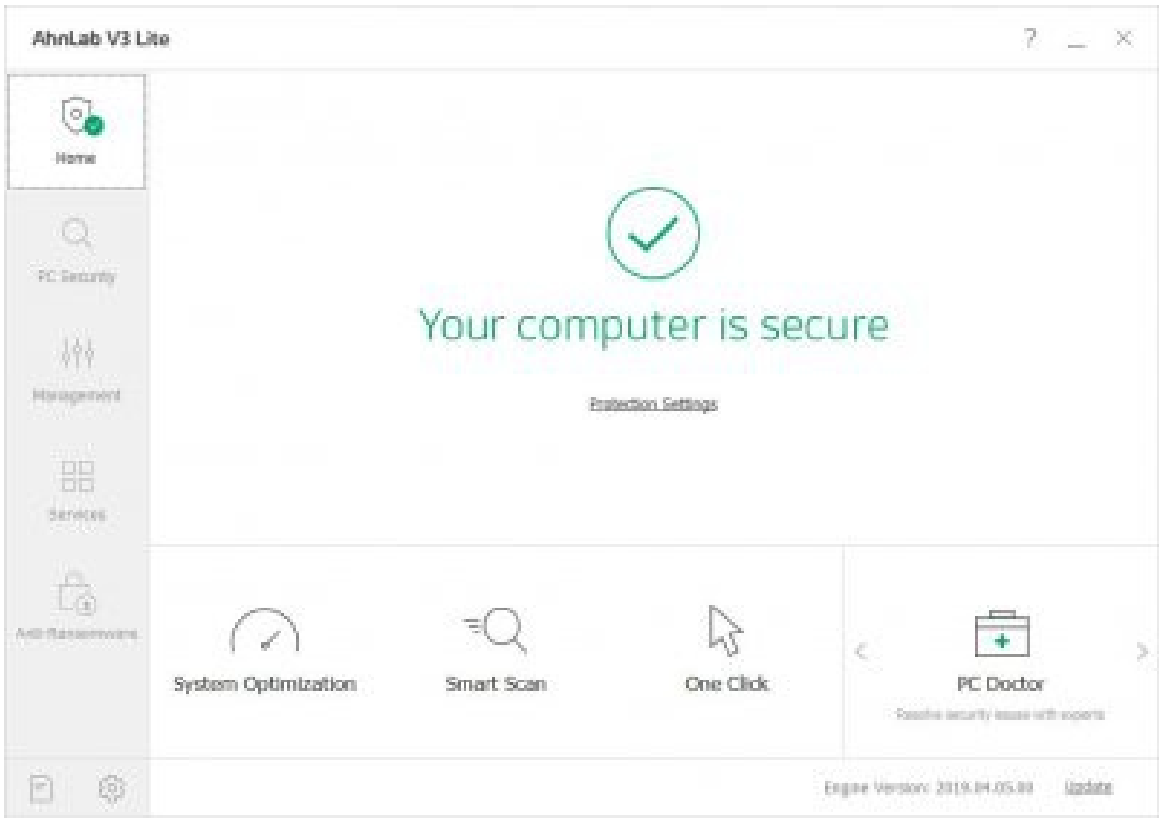


Рисунок 4.7 - AhnLab V3 Internet Security


Рисунок 4.8 - Avast Free AntiVirus

Avast вважається найпопулярнішим безкоштовним антивірусом та найбільшу долю ринку антивірусних програм. За даними розробників, понад 170 млн користувачів в світі використовують цю антивірусну програму [18].

AVG AntiVirus (рис. 4.9) — антивірусна програма, що розроблена чеською компанією AVG Technologies. Цей антивірус є доступним на платформах Microsoft Windows, OS X та Android. Антивірус має сканер файлів, має змогу перевіряти електронну пошту, виконувати моніторинг системи та містить пошуковий механізм Virus Stalker, сертифікований незалежними дослідницькими лабораторіями [19].

AVG Antivirus має декілька версій: комерційні (AVG Antivirus Pro і AVG Internet Security, що додатково містить у собі інструменти запобігання та захисту від Інтернет-атак) та безкоштовну (AVG Antivirus Free Edition).

Avira Antivirus Pro (рис. 4.10) - забезпечує комплексний захист настільних ПК (робочих станцій). Оптимальне рішення для персональних компьютеров в корпоративній мережі вашої організації [20].

Адміністраторська консоль Security Management Center дозволяє встановлювати, налаштовувати, автоматично оновлювати і контолювати Avira

Professional Security у всій локальній мережі прямо з робочого місця адміністратора. Також Avira Management Center дозволяє автоматично створювати дзеркало (актуальну копію) оновлень в локальній мережі, що економить інтернет-трафік у вашому офісі [20].

Рисунок 4.9 - AVG Internet Security

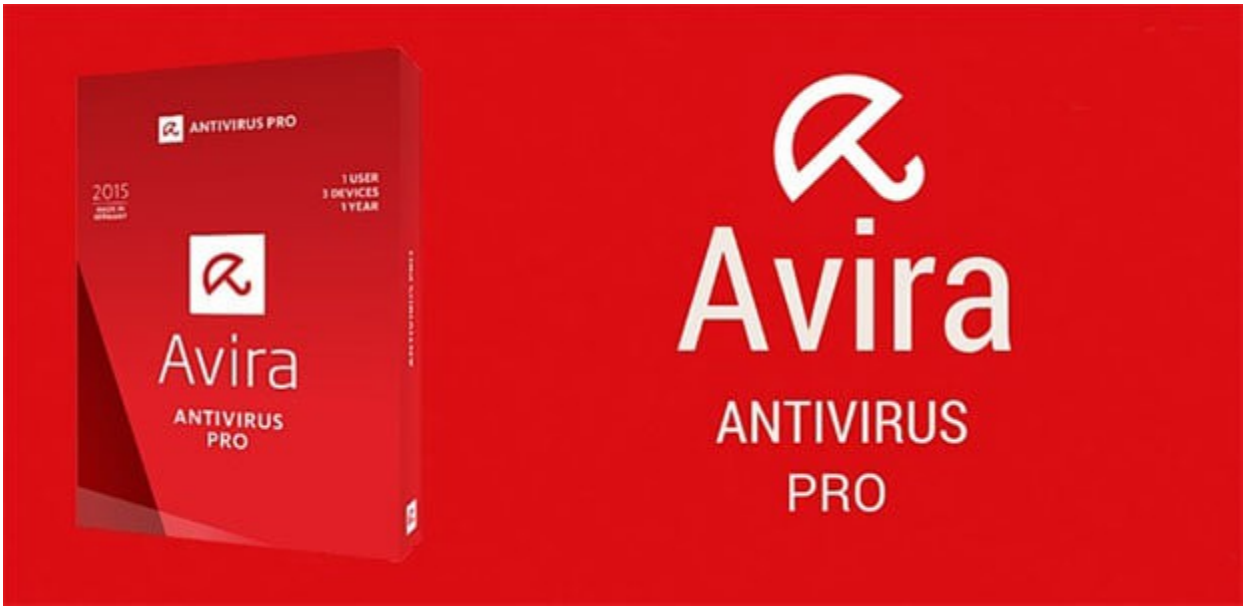


Рисунок 4.10 - Avira Antivirus Pro

Windows Defender (рис. 4.11) — програмний продукт компанії Microsoft, створений для того, щоб видаляти, поміщати в карантин або запобігати появі модулів шпигунського програмного забезпечення в ОС Windows. Цю антивірусну програму вбудовано в систему Windows Vista і вона є безкоштовно доступнию для завантаження при використанні різних версій Windows. Були також випущені версії програми, сумісні з більш ранніми ОС Windows [21].


Рисунок 4.11 - Microsoft Windows Defender

У програми Windows Defender є декілька способів запобігання зараження комп`ютера вірусами:

- захист у реальному часі (Windows Defender попереджає користувача, коли шпигунська програма намагається інсталювати або запустити себе на ПК або коли віруси намагаються змінити важливі налаштування Windows);
- параметри сканування (за допомогою Windows Defender можна шукати на комп'ютері шпигунські програми, регулярно задавати розклад сканування й автоматично видаляти все знайдене під час сканування) [21].

## 4.3 Порівняння антивірусних програм

Розглянуті антивірусні програми є різноманітними і кожна з них здатна допомогти як корпораціям, так і звичайним користувачам. Кожна з них має свої переваги та слабкі сторони.

Порівняємо антивірусні програми за наступними характеристиками:

– захист від вірусів;
– ефективність;
– зручність використання.

Критерій оцінювання візьмемо від 0 до 6.

0 – не функціонує

1 – функціонує, але не знаходить віруси

2 – функціонує, але знаходить прості віруси

3 – функціонує, але не оновлюються бази данних

4 – функціонує, але не протидіє складним вірусам

5 – функціонує, але бувають збої в роботі

6 – повністю функціонує у фоновому режимі

В результаті експериментальних досліджень було порівняно роботу розглянутих антивірусних програм та оцінено кожну з них за наступними якісними характеристиками: захист від вірусів, ефективність та зручність використання. Результати оцінювання антивірусних програм наведено в табл. 4.1.

Таблиця 4.1 – Результати оцінювання 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 |

Розрахунок ймовірностей захисту кожною антивірусною програмою виконано за допомогою формули :

, (4.1)

де – добуток всіх елементів рядка;

– загальна сума всіх добутків кожного рядка матриці ймовірностей;

$V_i$ – ймовірність захисту.

Розрахуємо загальну сумму всіх добутків кожної строки матриці ймовірностей:

=.

Розрахунок значення ймовірностей захисту виконано за формулою (4.1):

;

;

;

;

5;

;

;

.

В результаті розрахунків, виявилося із усіх розглянутих варіантів найвищі значення ймовірності захисту мають антивірусні програми №4 (AhnLab V3 Internet Security) та №6 (AVG Internet Security). Найменш ефективною антивірусною програмою виявився варінт №5 (Avast Free AntiVirus).

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

(4.2)

де - коефіцієнти відносної важливості показників якості, причому , - оцінки якісних характеристик.

Вводимо для кожної якісної характеристики коефіцієнти важливості (табл. 4.2).

Таблиця 4.2 – Коефіцієнти важливості

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

Розрахунок значень скалярної цільової функції для двох обраних варіантів виконується згідно (4.2) та має вигляд:

;

.

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

# ВИСНОВКИ

Збільшення швидкості передачі інформації, обсягів і значимості оброблюваних в обчислювальних мережах даних відкриває перед кіберзлочинцями все більш широкі можливості. Поширення по всьому світу шкідливого програмного забезпечення займає лічені дні або навіть години. Незважаючи на широкий асортимент антивірусних програм, постійно з'являються нові віруси. Для боротьби з новими вірусами необхідно створювати нові універсальні антивірусні продукти, що містимуть в собі переваги більш ранніх антивірусних програм. На сьогоднішній день, на жаль, відсутні такі антивірусні програми, які знешкоджували б негативну дію та гарантували б стовідсотковий захист від усіх видів програмних вірусів.

В роботі було розглянуто ряд питань, що стосуються сучасних вірусних і антивірусних програм та виконано порівняльний аналіз антивірусних програм.

В першому розділі виконано аналіз розвитку антивірусних програм, а також розглянуто Законодавство України з питань вірусних/антивірусних програм та проаналізовано вірусні атаки на Україну останніх років.

В другому розділі розглянуто основні характеристики комп'ютерних вірусів, зокрема класифікацію вірусних програм, особливості ураження комп'ютерів вірусами та особливості різних видів вірусних програм.

Третій розділ присвячено аналізу питань організації антивірусної безпеки. Розглянуто методи і технології захисту від шкідливих програм та вимоги до антивірусних програм.

В четвертому розділі виконано аналіз сучасних антивірусних програм: розглянуто різні види антивірусних програм, описано особливості найбільш актуальних антивірусних програм.

В роботі було виконано порівняльний аналіз наступних антивірусних програм: BullGuard Internet Security, Kaspersky Internet Security, NortonLifeLock, AhnLab V3 Internet Security, Avast Free AntiVirus, AVG Internet Security, Avira Antivirus Pro та Microsoft Windows Defender. В результаті експериментальних досліджень (тестувань) було порівняно роботу розглянутих антивірусних програм та оцінено кожну з них за наступними якісними характеристиками: захист від вірусів, ефективність та зручність використання.

Проведений аналіз дав наступні результати: найбільш переважний варіант антивірусної програми – AhnLab V3 Internet Security.

Результати роботи було апробовано на 25-му Міжнародному молодіжному Форумі "Радіоелектроніка і молодь у XXI столітті" на конференції "Перспективи розвитку інфокомунікацій та інформаційно-вимірювальні технології"та опубліковано тези доповіді [22] за тематикою кваліфікаційної роботи.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Догучаєв Б. М. Історія створення антивірусів [Електронний ресурс] / Б. М. Догучаєв – Режим доступу до ресурсу: https://pgu.ru/upload/iblock/eee/12.pdf.

2. Исаков Д. Рынок кибербезопасности 2021-2025: угрозы и инвестиционные возможности [Електронний ресурс] / Д. Исаков // MEGATRENDS. – 2021. – Режим доступу до ресурсу: https://megatrends.su / %D0%B1%D0%BB%D0%BE%D0%B3/cybersecurity/.

3. Главные тенденции в развитии решений для кибербезопасности [Електронний ресурс] // Kaspersky. – 2021. – Режим доступу до ресурсу: https://www.kaspersky.ru/resource-center/preemptive-safety/cyber-security-trends.

4. Якубенко С.С. Аналіз ринку антивірусних програм [Електронний ресурс] / С. С. Якубенко // Наукова конференція intkonf. – 2010. – Режим доступу до ресурсу: http://intkonf.org/yakubenko-ss-analiz-rinku-antivirusnih-program/.

5. Закон України «Про основні засади забезпечення кібербезпеки України» (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403) [Електронний ресурс] // Законодавство України. – 2020. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

6. Найгучніші хакерські атаки, які сколихнули всю Україну: вражаючі деталі [Електронний ресурс] // 24 канал. – 2018. – Режим доступу до ресурсу: https://24tv.ua/nayguchnishi_hakerski_ataki_yaki_skolihnuli_vsyu_ukrayinu_vrazhayuchi_detali_n1079849.

7. Хакерські атаки на Україну (2017) [Електронний ресурс] // wikipedia. – 2021. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Хакерські_атаки_на_Україну_(2017).

8. Каптерев А. И. Компьютерные вирусы и их классификация [Електронний ресурс] / А. И. Каптерев // Электронный ученик по информатике. – 2021. – Режим доступу до ресурсу: http://www.mediagnosis.ru/Autorun/Page6/11_1_.htm.

9. Файлові віруси [Електронний ресурс] – Режим доступу до ресурсу: https://sites.google.com/site/virusesvn/directory.

10. Стелс - віруси [Електронний ресурс] – Режим доступу до ресурсу: https://jak.koshachek.com/articles/stels-virusi-it.html.

11. Стелс-віруси [Електронний ресурс] – Режим доступу до ресурсу: http://um.co.ua/6/6-15/6-1575.html.

12. Троянський вірус [Електронний ресурс] – Режим доступу до ресурсу: http://naukam.triada.in.ua/index.php/konferentsiji/52-dvadtsyat-druga-vseukrajinska-praktichno-piznavalna-internet-konferentsiya/521-troyanskij-virus.

13. Шорошев В. Антивірусні програми світових брендів: порівняльна оцінка можливостей, рекомендації з їх вибору, новий метод прогнозування антивірусної безпеки / В. Шорошев. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2007. – вип. 1 (14). – С. 136–144.

14. Outstanding innovation, superior protection for your devices [Електронний ресурс] // BullGuard Internet Security 2021 Edition . – 2021. – Режим доступу до ресурсу: https://www.bullguard.com/products/bullguard-internet-security.aspx.

15. Kaspersky Internet Security 2021 [Електронний ресурс] // Kaspersky. – 2021. – Режим доступу до ресурсу: https://www.kaspersky.ru › internet-security.

16. Our Vision is to protect and empower people to live their digital lives safely [Електронний ресурс] // NortonLifeLock. – 2021. – Режим доступу до ресурсу: https://www.nortonlifelock.com/us/en/.

17. AhnLab V3 Internet Security [Електронний ресурс] // comss.ru. – 2021. – Режим доступу до ресурсу: https://www.comss.ru/page.php?id=884.

18. Avast Free Antivirus. Базовий захист — необтяжливий, ефективний та абсолютно безкоштовний [Електронний ресурс] // Avast. – 2021. – Режим доступу до ресурсу: https://www.avast.ua/free-antivirus-download#pc.

19. AVG Internet Security [Електронний ресурс] // AVG. – 2021. – Режим доступу до ресурсу: https://www.avg.com/ru-ru/internet-security#pc.

20. Avira Antivirus [Електронний ресурс] // Avira. – 2020. – Режим доступу до ресурсу: https://itpro.ua/product/aviraantivirprobus/?tab=description.

21. Захист ПК за допомогою Автономного Microsoft Defender [Електронний ресурс] // Microsoft. – 2021. – Режим доступу до ресурсу: https://support.microsoft.com/uk-ua/windows/захист-пк-за-допомогою-автономного-microsoft-defender-9306d528-64bf-4668-5b80-ff533f183d6c

22. Вервейко В. В. Аналіз видів захисту особистих даних використовуючи антивірусні програми / В. В. Вервейко. // Матеріали 25-го Міжнародного молодіжного Форуму "Радіоелектроніка і молодь у XXI столітті" Конференція "Перспективи розвитку інфокомунікацій та інформаційно-вимірювальні технології". – 2021. – Том 4. – С. 66–67.