DOI: https://doi.org/10.32782/2524-0072/2022-43-51

УДК 004.491.22

СУЧАСНІ МЕТОДИ БОРОТЬБИ З КОМП'ЮТЕРНИМИ ВІРУСАМИ

MODERN METHODS OF FIGHTING COMPUTER VIRUSES

Антоненко Надія Василівна
кандидат економічних наук, доцент,
Національного транспортного університету
ORCID: https://orcid.org/0000-0003-1478-6668

Дігтяр Яна Сергіївна
студентка,
Національного транспортного університету
ORCID: https://orcid.org/0000-0003-3705-7396

Крикун Надія Олександрівна
студентка,
Національного транспортного університету
ORCID: https://orcid.org/0000-0002-0066-7919

Antonenko Nadiia, Dihtyar Yana, Krykun Nadiia
National Transport University

Стаття присвячена актуальним питанням використання сучасних методів боротьби з комп'ютерними вірусами. Детально розглянуто різноманітні методи виявлення шкідливих програм в контексті вимог комп'ютерної безпеки. Визначено механізм дії файлового і бутового вірусу. Наведена класифікація шкідливого програмного забезпечення, що передбачає поділ вірусів на класи. Особливу увагу в статті приділено механізму зараження окремих комп'ютерів, а також комп'ютерних мереж бутовими і файловими вірусами. В результаті виконання дослідження систематизовані способи виявлення вірусів при роботі пристроїв як без антивірусних програм, так із ними. Названі найбільш популярні та ефективні антивірусні програми, що рекомендовані фахівцями до використання в Україні. Відзначено, що основною невирішеною проблемою, яка потребує подальших розвідок, залишається розробка нових підходів до створення сучасного механізму захисту комп'ютерної техніки і інформаційного середовища від шкідливих програм і кібератак.

Ключові слова: кіберзагроза, комп'ютерний вірус, кібербезпека, захист інформації, антивірусна програма.

The article is devoted to topical issues of using modern methods of combating computer viruses. The classification of malicious software is given, which involves the division of viruses into the classes of file and boot viruses. Various methods of detecting malicious programs in the context of computer security requirements are considered in detail. The mechanism of action of the file and boot virus has been determined. The purpose of the article is the analysis, systematization and grouping of modern methods of combating computer viruses that penetrate devices and networks with the aim of infecting and disrupting the performance of computers and systems. A set of well-known scientific methods and techniques was used to achieve the set goal of the research and to solve the relevant tasks: the abstract-logical method – for generalization, formulation of conclusions and recommendations. The method of logical synthesis was used to theoretically substantiate the importance of studying the problems of protecting modern programs from computer viruses. The methods of analysis and synthesis made it possible to determine the peculiarities of the use of modern antivirus programs in Ukraine. The article pays special attention to the mechanism of infection of individual computers, as well as computer networks, with boot and file viruses. It has been found out how devices are infected with a file-boot virus called DIR. Separately, the article considers the problem of the influence of a number of viruses on computer software. As a result of the research, methods of virus detection were systematized during the operation of devices both without antivirus programs and with them. The most popular and effective antivirus programs recommended by specialists for use in Ukraine are named. The practical value of the article lies in the definition, systematization and justification of modern methods of combating computer viruses. It was noted that the main unsolved problem, which requires further research, remains the development of new approaches to the creation of a modern mechanism for protecting computer equipment and the information environment from malicious programs and cyber attacks.

Keywords: cyber threat, computer virus, cyber security, information protection, antivirus program.

Постановка проблеми та її зв'язок з важливими науковими чи практичними завданнями. З того часу, як комп'ютери увійшли у побут сучасної людини, Інтернет-мережа стала невід'ємною частиною її життєдіяльності. Але, саме глобальна комп'ютерна мережа є джерелом небезпечних вірусів, що можуть зруйнувати будь-які засоби захисту обчислювальної техніки. На сьогоднішній день людством ще не створена така антивірусна програма, що могла би забезпечити стовідсотковий захист техніки від кібератак, проте існує величезна кількість способів виявлення небезпечного вірусу і без спеціального програмного забезпечення.

З огляду на крайню необхідність захисту комп'ютерної системи від вірусних загроз актуальним питанням сьогодення є задача розроблення сучасних методів запобігання та видалення шкідливих кодів і програм. Таким чином, тема статті є нагальною, своєчасною і такою, що відповідає найважливішим потребам сучасності.

Аналіз останніх досліджень і публікацій. Питання комп'ютерних вірусів, методів їх виявлення та способів ліквідації розглядали такі відомі вчені, як Л. І. Поліщук [1], М. Д. Василенко [2], В. О. Рачук [2], В. М. Слатвінська [2], Д. О. Ричка [3], П. О. Юзик [4]. Заслуговує на увагу дослідження Л. І. Поліщук [1], яка детально висвітила проблему впливу ряду вірусів на програмне забезпечення комп'ютерної техніки, а також розглянула міфи про віруси, що функціонують у теперішній час. М. Д. Василенко [2], В. О. Рачук [2] і В. М. Слатвінська [2] присвятили свої дослідження темі виявлення шкідливих програм в контексті вимог комп'ютерної безпеки. Д. О. Ричка [3] і П. О. Юзик [4] у своїх роботах запропонували комплекс заходів щодо захисту бази даних від кіберзагроз і визначили напрямки боротьби із комп'ютерними вірусами.

Втім, як свідчить аналіз наукових робіт, потребує подальшої уваги і досліджень розробка нових підходів до створення сучасного механізму захисту комп'ютерної техніки і інформаційного середовища від шкідливих програм і кібератак.

Виділення невирішених раніше частин загальної проблеми. Найбільше часу в роботі адміністратора комп'ютерних мереж займає процес захисту від несанкціонованого доступу до конфіденційної інформації і заходи боротьби зі шкідливими програмами і вірусами. На сьогоднішній день недостатньо обґрунтованими залишаються методи комплексної протидії шкідливому програмному забезпеченню, які використовують фахівці з комп'ютерної вірусології.

Формулювання цілей статті (постановка завдання). Метою статті є аналіз, систематизація і групування сучасних методів боротьби з комп'ютерними вірусами, що проникають на пристрої та в мережі з метою зараження і порушення працездатності комп'ютерів і систем.

Виклад основного матеріалу дослідження з повним обґрунтуванням здобутих наукових результатів. В результаті дослідження основних видів шкідливого програмного забезпечення виявлено велику кількість програм, які перешкоджають роботі комп'ютера, збирають конфіденційну інформацію або отримують доступ до приватних комп'ютерних систем. Дослідники М. Д. Василенко, В. О. Рачук, В. М. Слатвінська в своїй статті [2] назву «шкідливі програми» пояснюють терміном «malware», утвореним від двох англійських слів: «malicious» («зловмисний») і «software» («програмне забезпечення»). Проте, частіше за все, шкідливе програмне забезпечення представлено зловмисними програмними засобами, одними із представників яких є віруси. Вітчизняний розробник антивірусних програм Д.О. Ричка характеризує поняття комп'ютерного вірусу, як «спеціально створеної програми, яка сама здатна приєднуватися до інших програм і у разі запуску спричиняє різні негативні наслідки (псує файли і каталоги, перекручує інформацію) та створює інші перешкоди у роботі ЕОМ» [3].

Перейдемо до класифікації шкідливого програмного забезпечення. Майже всі комп'ютерні віруси можна поділити на два класи: файлові та бутові. Одним із найпоширеніших способів зараження вірусом файлу є дописування тіла вірусу у кінець цього файлу. При запуску такого файлу вірус завантажувального сектора відразу отримує управління комп'ютером. В момент зараження вірус зчитує необхідну інформацію з первісного завантажувача та зберігає її у своєму коді. Крім завантажувальних вірусів, останнім часом почали поширюватися віруси, що перезаписують початок файлу і не змінюють його довжину. Вищезазначена програма надалі вже не виконуватиме своїх функцій, а буде лише заражати інші файли. Відомо, що існують віруси, які можуть записувати своє тіло у два різні файли (рис. 1).

Також віруси можуть своє тіло розмістити у середині файлу. Останнім часом почали

з'являтись віруси, які записують своє тіло до файлу «плямами». Такі віруси знаходять порожні місця і вставляють туди своє тіло, при цьому довжина файлу може суттєво збільшуватись. Віруси, які заражають Boot-сектор вінчестера називають бутовими вірусами. Вони розміщують свій початок у Boot-секторі, а решту тіла записують до вільних кластерів і помічають їх як погані. Саме у вільному кластері вірус може розмістити справжній запис Boot-сектора і у подальшому може передати йому управління (рис. 2).

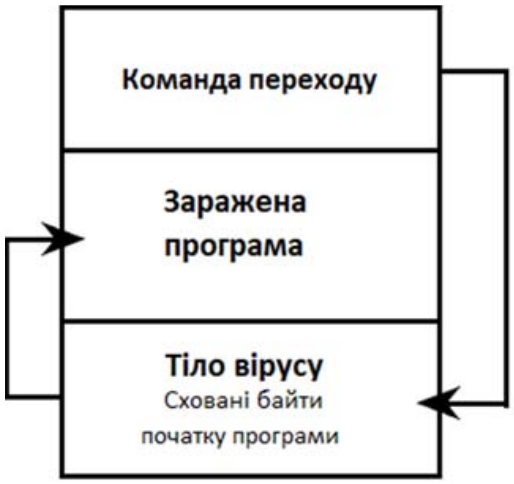

Рис. 1. Схема дії файлового вірусу

Джерело: авторська розробка

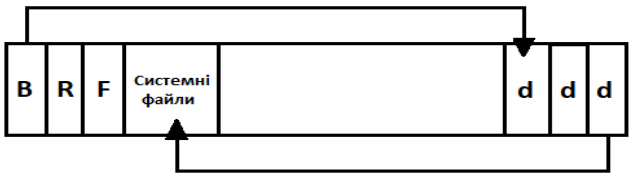

Рис. 2. Схема дії бутового вірусу

Джерело: авторська розробка

Сьогодення характеризується тим, що в комп'ютерних мережах широко розповсюджені окремі віруси, які можуть заражати як Boot-сектори, так і файли. Ці віруси носять назву файлово-бутові. Крім цих вірусів є й такі, механізм зараження яких суттєво відрізняється від вищезазначених.

Одним із перших в комп'ютерних мережах з'явився файлово-бутовий вірус під назвою DIR. Його дія полягає у наступному: для всіх виконуваних файлів посилання на початок у таблиці розміщення файлів здійснюється заміна посилання на тіло вірусу, при цьому вірус знаходиться на диску. Тому, при запуску програми спочатку управління одержує вірус, а вже потім програма.

В таблиці 1 наведені назви найбільш розповсюджених файлових і бутових вірусів.

В процесі роботи пристроїв та мережі дія кожного з вірусів проявляється по-різному: в одній ситуації це можуть бути різні візуальні ефекти, що заважають працювати з системою, а в інших – дія вірусу може призвести до цілковитої втрати інформації та повного блокування системи. Більшість вірусів потрапляють до комп'ютера через програми з розширенням .exe та .com. Хоча в останній час все більше і більше вірусів потрапляють до системи через електронну пошту.

Прикладами вірусів, що призвели до величезних збитків, можна назвати:

– вірус «Sasser», який знищив картографічну систему Британської берегової охорони та завдав збитків на 500 млн доларів. Розробником цього вірусу виявився підліток з Німеччини, якого затримали завдяки одному із його друзів – він планував отримати винагороду у 250 тис. доларів від Microsoft [5];

– вірус «Nimda». Ще нещодавно він був найпоширенішим в інтернет-середовищі і завдав сумарно збитків на 635 млн. доларів. Цей вірус викликав перебої в інтернет-з'єднаннях [5];

– вірус «Chernobyl». Його створив студент із Тайваню. Від цього вірусу постраждало

Таблиця 1

Приклади файлових і бутових вірусів

№ з/п	Назва груп вірусів	
	Файлові віруси	**Бутові віруси**
1	Вірус VIENNA (Відень)	Вірус PING PONG
2	Вірус CASCADE (Каскад, водоспад)	Вірус STONED (Закам'янілий)
3	Вірус BLACK FRIDAY (Чорна п'ятниця)	Вірус BRAIN (Мозок)
4	Вірус DARK AVENGER (Чорний месник)	Вірус DINAMO (назва не потребує перекладу)

Джерело: узагальнено авторами на основі [1; 2; 3; 4]

більше, ніж 500 тис. комп'ютерів по всьому світу, а збитки оцінені в 1 млн. доларів [5];

– вірус «Melissa». Він діяв через відправку заражених документів Word всім, хто був зареєстрований в контактах користувача. У 1999 році «Melissa» завдала збитків у 1,2 млрд доларів [5];

вірус «MyDoom». Цей вірус є найбільш руйнівним за всю історію існування мережі Інтернет. Збитки від нього сягнули суми у 38 млрд. доларів [5].

Хакери, що розробляють ці шкідливі програми, маскують загрозливу програму під безпечну. Тому, необхідно швидко аналізувати ситуацію і оперативно приймати рішення щодо використання сучасних методів боротьби з усіма видами комп'ютерних загроз.

Насьогодні існує декілька способів виявлення вірусів, коли система працює без антивірусу [6]. Перший – це перевірка диспетчера процесів, оскільки найчастіше вірус маскується саме під безпечний процес і здійснює зараження пристрою. Щоб виявити вірус потрібно відкрити список запущених служб і додатків, уважно переглянути його і відключити непотрібні системні служби Windows (рис. 3).

Вірус може мати назву, що складається із беззмістовного набору літер і цифр. Ще одним способом виявлення вірусу є аналіз автозавантаження комп'ютера. Більша кількість вірусів запускається разом із системою і блокує її або активує свої власні функції. Щоб виявити вищезазначені віруси потрібно відкрити вікно «Виконати» за допомогою комбінації клавіш клавіатури Win+R, потім відкритти конфігуратор Microsoft шляхом вводу команди «msconfig». При виконанні цих дій необхідно перевіряти та завершувати підозрілі процеси, що виконує пристрій (рис. 4).

Як свідчить досвід, використання наведених вище методів виявлення вірусів є недостатньо ефективною процедурою і для більш успішної боротьби з кіберзагрозами необхідно дотримуватись ряду наступних правил [7].

Рекомендується постійно робити копії важливих документів та файлів, або ж всього диска відразу.

При встановленні нової програми чи скачуванні файлу потрібно обов'язково перевіряти їх антивірусними засобами.

Для діагностики та виявлення вірусів необхідно використовувати лише перевірені ліцензовані антивірусні програми.

При проведенні повної очистки комп'ютера від вірусів потрібно провести форматування жорстких дисків або здійснити інсталяцію операційної системи.

Масове поширення вірусів і серйозність наслідків їх впливу на комп'ютерну систему змусило користувачів звернутися до спеціальних методів та засобів боротьби з ними. Тож розглянемо способи виявлення небезпечних вірусів [8]. Одним з найпростіших методів пошуку вірусів є сканування – воно здійснюється програмним сканером, що переглядає файли і шукає вірус. Програма фіксує лише ті віруси, які були виявлені при скануванні раніше, то ж для ефектного використання даного методу потрібно регулярно оновлювати антивірусну програму. Однією з відомих програм-сканерів є «Cezurity» – безкоштовний сервіс, що дозволяє легко і швидко виявляти шкідливі програми.

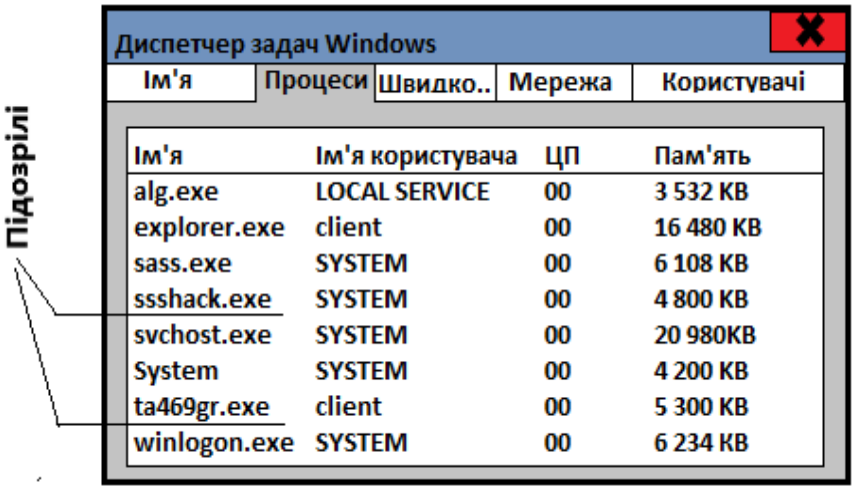

Рис. 3. Перевірка диспетчера процесів

Джерело: авторська розробка

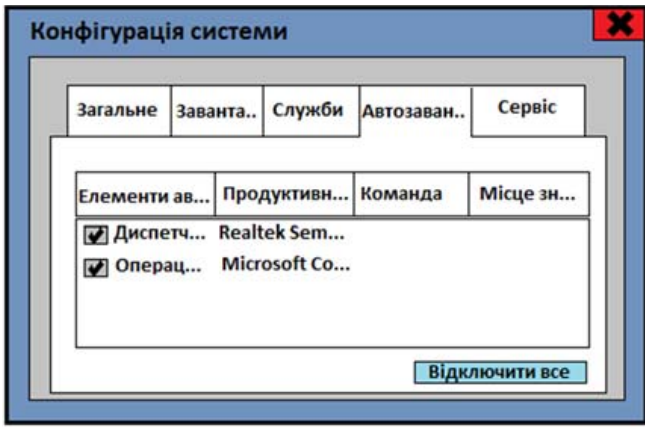

Рис. 4. Перевірка конфігуратора

Джерело: авторська розробка

Наступним способом пошуку вірусів є метод виявлення змін, що базується на використанні програм-ревізорів. Зазвичай ці програми запам'ятовують характеристики всіх файлів, каталогів, обсяги встановленої оперативної пам'яті. Головною перевагою методу є те, що ці програми виявляють практично всі типи вірусів, а також надають інформацію про невідомий раніше шкідливий програмний засіб. В якості прикладу можна назвати програму-ревізор «Adinf.»

Далі розглянемо евристичний аналіз, який почав використовуватися в недалекому минулому як метод виявлення змін. Цей метод виявляє усі можливі віруси і не вимагає попередньої обробки та збору інформації. Сутність евристичного аналізу полягає в перевірці даних пристрою і виявленні в них команд, характерних для вірусів. Евристичним- аналізатором є програма «Aidstest».

Ще одним методом пошуку вірусів є метод дії резидентних сторожів, який базується на завантаженні програмою інших антивірусних програм з метою перевірки підозрілих програм і файлів. Але істотним недоліком цього методу є великий відсоток помилкових виявлень, що заважає роботі користувача. Прикладом резидентного сторожу є програма «Vsafe».

Далі охарактеризуємо метод апаратно-програмних антивірусних засобів, сутність якого полягає в тому, що в систему встанов-

Таблиця 2

Популярні та ефективні антивірусні програми, що рекомендовані до використання в Україні

№ з/п	Назва антивірусної програми	Країна-розробник	Переваги та недоліки програми
1.	**Avira Antivirus Premium**	Німеччина	*Переваги:* Має високі показники виявлення шкідливих програм, безкоштовна версія діє протягом одного місяця. Захищає від усіх вірусів, виявляє будь-які загрози. *Недоліки:* безкоштовна версія не забезпечує доступ до служби підтримки клієнтів
2.	**ESET NOD32 Platinum**	Словаччина	*Переваги:* Має функцію захисту платежів, виконує «батьківський контроль», здійснює захист мережі WI-FI, має функцію USB-контролю. В програму вбудований антиспам-фільтр. *Недоліки:* антивірусні пакети ESET можуть пропускати деякі загрози
3.	**Panda Free Antivirus**	Україна	*Переваги:* Безкоштовно забезпечує відмінний рівень безпеки. Має додаткові функції, такі як VPN, Gaming Mode і Process Monitor. *Недоліки:* ПК залишається вразливим через відсутність захисту від програм-вимагачів

Джерело: складено авторами на основі [9]

люється спеціальний контролер, який має доступ до загальної інформації і запам'ятовує області диска, зміна у яких недопускається. При виявленні програмою будь-яких заборонених дій або змін користувачу надсилається повідомлення та блокуються файли. Прикладом апаратно-програмного контролю від вірусів може стати комплекс «Sheriff».

Також до антивірусних програм відносять вакцини. Проте потрібно зауважити, що їх використання і раніше було мало популярне, а зараз взагалі програми-вакцини майже не використовуються, оскільки діють на обмежену кількістю вірусів. Дія вакцини нагадує дію віруса, наприклад, вірус VIENNA виставляє у зараженому файлі неправдивий час утворення – так само працює і вакцина.

Охарактеризувавши основні методи боротьби з комп'ютерними вірусами можна назвати найбільш популярні та ефективні антивірусні програми, що рекомендовані фахівцями до використання в Україні (таблиця 2).

Ознайомившись з перевагами і недоліками різноманітних антивірусних програм необхідно зазначити, що вони між собою мало чим відрізняються. Слід зауважити, що встановлення на комп'ютер тільки одного антивірусу є вкрай помилковим рішенням, оскільки у своєму розвитку віруси випереджають можливості антивірусних програм. Фахівці з кібербезпеки рекомендують використовувати декілька різних антивірусних пакетів одночасно.

Висновки. За результатами дослідження з'ясовано, що всі комп'ютерні віруси поділяються на файлові та бутові. В залежності від класу вірусу ІТ-фахівці пропонують різні способи їх пошуку, найпростішими з яких є перевірка диспетчера процесів та проведення аналізу автозавантаження комп'ютера. Серед найбільш ефективних методів пошуку вірусів можна зазначити наступні: метод сканування пристрою, евристичний аналіз, метод виявлення змін, що базується на використанні програм-ревізорів, метод дії резидентних сторожів, метод апаратно-програмних антивірусних засобів. Узагальнюючи результати дослідження слід зазначити, що усі загрози, що створюються вірусами, успішно ліквідуються антивірусними програмами, що потребують вчасного оновлення і обов'язкового ліцензування. До найбільш популярних та ефективних антивірусних програм, що рекомендовані фахівцями до використання в Україні, відносяться антивіруси Avira Antivirus Premium, ESET NOD32 Platinum Edition, *Panda* Free *Antivirus. Попри ряд недоліків ці антивірусні програми продуктивно працюють, здійснюючи пошук вірусів,* що проникають на пристрої та в мережі з метою зараження і порушення працездатності комп'ютерів і систем. Перспективою подальших досліджень може бути розроблення сучасних антивірусних засобів підтримки кібербезпеки різних за рівнем захисту інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Поліщук Л. І. Дослідження засобів боротьби з комп'ютерними вірусами для захисту інформаційно-комунікаційних систем. *Інформаційні технології та комп'ютерна інженерія.* Кіровоград : КНТУ, 2014. С. 173. URL: https://core.ac.uk/download/pdf/81587604.pdf (дата звернення: 23.10.2022).

2. Василенко М. Д., Рачук В. О., Слатвінська В. М. Шкідливі програми в контексті розуміння комп'ютерної вірусології та техніко-правової змагальності: міждисциплінарне дослідження. *Наукові праці Національного університету «Одеська юридична академія».* 2021. Том 29. С. 28–36.

3. Ричка Д. О. Комп'ютерні віруси – шкідливі програмні засоби, рушійна сила модифікації. *Науковий вісник Херсонського державного університету.,* 2018. Вип. 1. Т. 2. С. 89–93.

4. Юзик О. П. Комп'ютерні віруси та боротьба з ними. *Комп'ютер у школі та сім'ї.* 2006. Вип. 6. С. 8–11.

5. Топ-10 комп'ютерних вірусів, які призвели до величезних збитків. URL: https://10guards.com/ua/articles/10-worst-computer-viruses-in-history (дата звернення: 23.10.2022).

6. Комп'ютерні віруси та методи боротьби з ними. URL: https://ua-referat.com (дата звернення: 26.10.2022).

7. Лисенко С. М., Щука Р. В. Аналіз методів шкідливого програмного забезпечення в комп'ютерних системах. *Вісник Хмельницького національного університету.* 2020. Вип. 2. С. 101–107.

8. Всі методи виявлення вірусів на компютері. URL: http://fastping.com.ua/2021/12/22/vsi-metodi-viyavlennya-virusiv-na-kompyuteri (дата звернення: 23.10.2022).

9. Рейтинг найкращих антивірусів — ТОП-10 програм. URL: https://itc.ua/ua/articles/reityng-antyvirusiv/ (дата звернення: 23.10.2022).

REFERENCES:

1. Polishchuk, L. I. (2014) Doslidzhennia zasobiv borotby z kompiuternymy virusamy dlia zakhystu informatsiino-komunikatsiinykh system [Research on means of combating computer viruses for the protection of information and communication systems]. *Informatsiini tekhnolohii ta kompiuterna inzheneriia – Information technology and computer engineering,* 173. Available at: https://core.ac.uk/download/pdf/81587604.pdf. (in Ukrainian)

2. Vasylenko, M. D., Rachuk, V. O., & Slatvinska, V. M. (2021) Shkidlyvi prohramy v konteksti rozuminnia kompiuternoi virusolohii ta tekhniko-pravovoi zmahalnosti: mizhdystsyplinarne doslidzhennia [Malware in the context of understanding computer virology and techno-legal adversarialism: an interdisciplinary study]. *Naukovi pratsi Natsionalnoho universytetu «Odeska yurydychna akademiia» – Scientific works of the National University "Odesa Law Academy"*, *29*, 28–36.

3. Rychka, D.O. (2018) Komp'juterni virusy – shkidlyvi proghramni zasoby, rushijna syla modyfikaciji [Computer viruses are malicious software, the driving force of modification]. *Naukovyi visnyk Khersonskoho derzhavnoho universytetu – Scientific Bulletin of Kherson State University, 1*(2), 89–93.

4. Iuzyk, O. P. (2006) Kopiuterni virusy ta borotba z nymy [Computer viruses and combating them]. *Kompiuter u shkoli ta simi – Computer in school and family, 6*, 8–11.

5. Top-10 kompiuternykh virusiv, yaki pryzvely do velycheznykh zbytkiv [Top 10 computer viruses that caused huge losses]. Available at: https://10guards.com/ua/articles/10-worst-computer-viruses-in-history (in Ukrainian)

6. Kompiuterni virusy ta metody borotby z nymy [Computer viruses and methods of combating them]. Available at: https://ua-referat.com. (in Ukrainian)

7. Lysenko, S. M., & Shchuka, R. V. (2020) Analiz metodiv shkidlyvoho prohramnoho zabezpechennia v kompiuternykh systemakh [Analysis of malware methods in computer systems]. *Visnyk Khmelnytskoho natsionalnoho universytetu – Bulletin of the Khmelnytskyi National University, 2,* 107–107.

8. Vsi metody vyiavlennia virusiv na kompiuteri [All methods of detecting viruses on a computer]. Available at: http://fastping.com.ua/2021/12/22/vsi-metodi-viyavlennya-virusiv-na-Kompyuteri. (in Ukrainian)

9. Reitynh naikrashchykh antyvirusiv – TOP-10 prohram [Rating of the best antiviruses – TOP-10 programs]. Available at: https://itc.ua/ua/articles/reityng-antyvirusiv. (in Ukrainian)