УДК 004.056.5 + 6(09)
DOI https://doi.org/10.32782/cusu-hist-2026-1-25

Кондратьєв Віталій,
аспірант кафедри історії науки та українознавства,
Національний технічний університет
«Харківський політехнічний інститут»,
vitalij.kondrateev.96@gmail.com,
ORCID ID: 0000-0002-0647-136X

ПЕРШІ КОМП'ЮТЕРНІ ВІРУСИ: ПОЧАТОК ІСТОРІЇ КІБЕРЗАГРОЗ (1970-ті – ПОЧАТОК 1990-х РОКІВ)

У статті досліджено виникнення та еволюцію перших комп'ютерних вірусів у контексті історії розвитку кіберзагроз, із фокусуванням на періоді 1980-х років. Розглянуто теоретичні передумови створення самореплікативних програм, починаючи з концепцій самовідтворюваних автоматів Джона фон Неймана. Проаналізовано наукову діяльність Фреда Коена, який у 1983 році вперше формалізував поняття комп'ютерного вірусу та експериментально довів потенційну небезпеку вірусних програм. Висвітлено історію створення та поширення перших вірусів: Creeper (1971), Reaper (1971), Elk Cloner (1982), Brain (1986), Jerusalem (1987), Cascade (1987), а також мережевого черв'яка Morris (1988). Охарактеризовано технічні особливості ранніх вірусів, механізми їх функціонування та наслідки поширення. Окрему увагу приділено трансформації мотивації авторів вірусів – від академічних експериментів до навмисного завдання шкоди. Досліджено соціально-економічні наслідки вірусних епідемій 1980-х років, зокрема формування антивірусної індустрії, зміну корпоративних підходів до інформаційної безпеки та виникнення нових соціальних практик взаємодії з комп'ютерними системами. Встановлено взаємозв'язок між принципами, закладеними в ранніх комп'ютерних вірусах, та сучасними кіберзагрозами. Обґрунтовано важливість вивчення історії перших вірусів для розуміння фундаментальних принципів функціонування шкідливого програмного забезпечення та розробки ефективних стратегій кіберзахисту в сучасних умовах. Представлено ключові уроки з історії ранніх комп'ютерних вірусів, які мають практичне значення для сучасних фахівців із кібербезпеки. Проведене дослідження заповнює існуючу в українській історіографії прогалину щодо історичного аналізу витоків кіберзагроз, систематизуючи та контекстуалізуючи розвиток комп'ютерних вірусів як важливого феномену в історії науки і техніки.

Ключові слова: *інформаційні технології, історія науки й техніки, кібербезпека, кіберзагрози, комп'ютер.*

Із розвитком обчислювальних технологій і зростанням їхнього впливу на повсякденне життя постало одне з найважливіших питань сучасності – безпека цифрових даних. На самому початку 1980-х років комп'ютерні віруси були ще невідомим явищем, але їх поява змінила уявлення про безпеку.

Комп'ютерний вірус – це тип шкідливого програмного забезпечення, здатного самостійно відтворюватися, вбудовуючи власні копії в інші програми, файли або системні області комп'ютера без відома та згоди користувача. Подібно до біологічних вірусів, комп'ютерні віруси не можуть функціонувати самостійно і потребують «хазяїна» – певної програми або операційної системи – для свого розповсюдження та функціонування. Здатність до самореплікації є ключовою характеристикою, що відрізняє віруси від інших типів шкідливого програмного забезпечення.

Комп'ютерні віруси розроблені для різноманітних цілей: від відносно нешкідливих жартів та демонстрації технічних можливостей до серйозних кібератак, спрямованих на викрадення даних, шпигунство або спричинення матеріальних збитків. Незалежно від мотивації їхніх творців, віруси стали невід'ємною частиною цифрової реальності, суттєво вплинувши на розвиток інформаційних технологій та кібербезпеки.

Дослідження історії перших комп'ютерних вірусів має фундаментальне значення для розуміння еволюції кіберзагроз та розробки ефективних стратегій захисту. Подібно до того, як медична наука вивчає патогенез хвороб для ефективної боротьби з ними, дослідження початкових форм комп'ютерних вірусів дозволяє зрозуміти базові принципи їх функціонування, методи поширення та механізми атак.

Останнім часом опубліковано чимало досліджень щодо історії комп'ютерних вірусів. Зокрема аспірант кафедри кримінального права та процесу Державного податкового університету В. А. Лавренюк розглядає історію та розвиток комп'ютерних вірусів з точки зору кримінального права. Він наводить деякі історичні факти, пов'язані з кримінальною комп'ютерною активністю у світі, починаючи з 1960-х років. У статті розглядаються ключові етапи становлення комп'ютерних злочинів як соціального явища, а також їхні сучасні форми, які включають несанкціонований доступ до даних, фінансові шахрайства, атаки на критичну інфраструктуру та поширення шкідливого програмного забезпечення (Лавренюк В. А., 2024). Дослідження В. І. Цукрука, студента факультету інформаційних технологій та комп'ютерної інженерії Вінницького національного технічного університету, розкриває етимологію назв комп'ютерних вірусів і під якою назвою вони відомі в України (Цукрук В. І., 2017). Історія кібервійни, але вже як складову політичного процесу, висвітлює авторка з Національного університету «Одеська юридична академія» Ю. В. Завгородня. Вона наголошує, що терміни «троянський кінь» і «комп'ютерний вірус» стали відомі в 1980-ті роки. Події, які зараз відбуваються в Україні через напад росії, авторка характеризує як першу світову кібервійну. Аналіз кіберзагроз в умовах ведення інформаційної війни здійснює аспірант кафедри конституційного, адміністративного та фінансового права Хмельницького університету управління та права імені Леоніда Юзькова Я. П. Мазур (Мазур Я. П., 2024). Автори з Національного університету оборони України (Машталір В., 2024) розглядають сучасний етап кібербезпеки. Енергетична галузь як об'єкт кіберзагроз та забезпечення її життєдіяльності обговорюється у статті наукових співробітників Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України (Стежко С. М., 2021).

Однак, попри актуальність висвітлення тематики кіберзагроз, сучасні українські історики науки й техніки залишають це питання без уваги. Автори зосереджуються переважно на вибраних аспектах історії перших комп'ютерних вірусів. Дослідники за кордоном також майже не зацікавлені в науковому історичному висвітленні цього питання. Стаття авторів з Індії (Bhargava P., 2022) наводить доволі багато фактів з історії комп'ютерних вірусів за період 1980–2020-х років, проте через обмеження розмірів статті вкрай лімітовано висвітлюється період витоків кіберзагроз.

Таким чином, цілісного історичного дослідження, яке б представляло інформацію щодо витоків кіберзагроз в світі, на сьогодні немає.

Метою статті є дослідження виникнення та розвитку перших комп'ютерних вірусів як складової історії кіберзагроз, з акцентом на ідентифікацію ключових етапів становлення цього феномену та висвітлення імен осіб, які відіграли провідну роль у створенні перших вірусів або вивченні їх дії, зокрема у контексті формування наукового підґрунтя сучасної кібербезпеки.

Аналіз ранніх зразків шкідливого програмного забезпечення дає можливість простежити не лише технічну еволюцію вірусів, але й трансформацію мотивів їх створення – від академічних експериментів та технічних демонстрацій до інструментів кібершпигунства та кіберзлочинності. Крім того, вивчення перших вірусів висвітлює процес формування антивірусної індустрії та методологій кібербезпеки, які створили основу для сучасних підходів до захисту інформаційних систем. Розуміння історії комп'ютерних вірусів також сприяє розвитку прогностичних моделей для передбачення майбутніх напрямків еволюції кіберзагроз.

Підґрунтя для розвитку комп'ютерних вірусів було закладене задовго до появи персональних комп'ютерів та інтернету. Математик та один із піонерів обчислювальної техніки Джон

фон Нейман наприкінці 1940-х років розробив теоретичну модель самовідтворюваних автоматів, що стала першим науковим підходом до розуміння потенційної можливості створення програм, здатних до саморепродукції. У своїй праці «Теорія і організація складних автоматів» (1949) фон Нейман описав концепцію «універсального конструктора» – теоретичного пристрою, здатного відтворювати самого себе (Von Neumann J., 1966). Хоча його дослідження було спрямоване здебільшого на розвиток теорії автоматів та вивчення штучного життя, воно створило теоретичний фундамент для розуміння процесів самореплікації в обчислювальних системах.

У 1952 році фон Нейман розвинув свої ідеї у лекції «Теорія самовідтворюваних автоматів», яка була опублікована посмертно у 1966 році завдяки зусиллям його колеги Артура Беркса. У цій роботі було представлено перше формальне доведення можливості існування самовідтворюваних машин у обчислювальному середовищі. Концепція фон Неймана про самовідтворювані автомати мала глибокі філософські та технічні наслідки. Вона продемонструвала, що програми не лише можуть виконувати певні функції, але й потенційно відтворювати себе, використовуючи ресурси обчислювального середовища. Саме ця фундаментальна можливість згодом стала технічною основою для створення комп'ютерних вірусів.

Хоча теоретичні основи самовідтворюваних програм були закладені Нейманом у 1940–50-х роках, формальне визначення та систематичне дослідження комп'ютерних вірусів як окремого класу програмного забезпечення відбулося значно пізніше – у 1983 році, завдяки роботам аспіранта Університету Південної Каліфорнії Фреда Коена. Під керівництвом професора Леонарда Адлемана Ф. Коен провів перші науково обґрунтовані експерименти з вірусоподібними програмами та сформулював визначення комп'ютерного вірусу, яке стало канонічним у галузі кібербезпеки. У своїй новаторській дисертації «Комп'ютерні віруси – теорія і експерименти» Ф. Коен визначив комп'ютерний вірус як програму, яка може інфікувати інші програми, модифікуючи їх таким чином, щоб включити в себе можливо еволюціонуючу копію самої себе (Cohen F., 1987). Це визначення вперше чітко відокремило віруси від інших типів шкідливого програмного забезпечення та підкреслило ключову характеристику вірусів – здатність до саморепродукції.

Експериментальна частина роботи Ф. Коена включала створення простої вірусної програми для системи VAX 11/750, що працювала під управлінням Unix (Cohen F., 1987). Під час контрольованого експерименту, проведеного 03 листопада 1983 року, програма змогла отримати повний контроль над системою протягом усього восьми годин, демонструючи швидкість та ефективність вірусного поширення навіть у ранніх комп'ютерних системах. Важливо зазначити, що експеримент проводився в ізольованому середовищі з дозволу університету і виключно в дослідницьких цілях.

Ф. Коен також зробив значний внесок у теоретичне розуміння вірусів, довівши декілька фундаментальних теорем щодо їхніх властивостей, зокрема:

1. Неможливість створення абсолютно надійного алгоритму виявлення вірусів.

2. Неможливість точного визначення, чи є довільна програма вірусом, без її фактичного виконання.

3. Можливість створення вірусів, які неможливо виявити за допомогою статичного аналізу коду (Cohen F., 1987).

Ці теоретичні висновки мали надзвичайно важливе значення для розвитку антивірусної галузі, оскільки вони встановили фундаментальні обмеження на можливості виявлення та захисту від вірусів. Фактично, Ф. Коен показав, що ідеальний антивірус неможливий у принципі, і захист від вірусів завжди буде змаганням між зловмисниками та фахівцями з безпеки. Слід зазначити, що практична історія комп'ютерних вірусів розпочалась значно раніше теоретичного осмислення цього феномену. Умовно можна виділити два етапи: перший – 1970-ті – середина 1980-х рр., пов'язаний з появою експериментальних та локальних вірусів; другий – кінець 1980-х – початок 1990-х рр., що характеризується поширенням мережевих вірусів та черв'яків.

Задовго до того, як Ф. Коен формально визначив поняття комп'ютерного вірусу, у 1971 році розробник на ім'я Боб Томас із компанії BBN Technologies створив програму, яка згодом стала вважатися першим у світі комп'ютерним вірусом і відкрила перший з окреслених етапів їх становлення. Програма отримала назву «Creeper» і була розроблена не як шкідливе програмне забезпечення, а як експериментальний проєкт для демонстрації мобільності програмного коду в мережевому середовищі.

Creeper функціонував у мережі ARPANET – попередниці сучасного інтернету, що поєднувала переважно наукові та військові установи США. Програма була створена для комп'ютерів, що працювали під управлінням операційної системи TENEX (Denning P. J., 1988). Її основною функцією було пересування між комп'ютерами мережі, демонструючи тим самим концепцію мобільного програмного забезпечення.

Механізм роботи Creeper був простим, але революційним для свого часу. Програма підключалася до віддаленого комп'ютера через мережу, копіювала себе на цей комп'ютер і запускала там свою копію. Після успішного копіювання, залежно від версії, оригінальна програма або видаляла себе з вихідного комп'ютера, або продовжувала працювати паралельно з новоствореною копією.

Ключовою особливістю Creeper була відсутність шкідливих намірів – програма не пошкоджувала файли, не викрадала інформацію і не перешкоджала роботі системи. Єдиним помітним ефектом її присутності було відображення на терміналі інфікованого комп'ютера повідомлення: «I'M THE CREEPER: CATCH ME IF YOU CAN» («Я ПОВЗУН: СПІЙМАЙ МЕНЕ, ЯКЩО ЗМОЖЕШ») (Hiruni Ch., 2024).

Важливо відзначити, що Creeper не відповідав усім характеристикам сучасного визначення комп'ютерного вірусу, оскільки він не «інфікував» інші програми, вбудовуючи в них свій код. Натомість, він просто копіював себе як окрему програму на інші комп'ютери. З цієї точки зору, Creeper більше нагадував мережевого черв'яка, ніж класичний комп'ютерний вірус (Kephart J. O., 1991). Однак, враховуючи, що чітке розмежування між різними типами шкідливого ПЗ було сформульоване лише в 1980-х роках, історично Creeper прийнято вважати першим комп'ютерним вірусом.

У відповідь на розповсюдження Creeper мережею ARPANET, у тому ж 1971 році програміст Рей Томлінсон створив програму під назвою «Reaper» (Hiruni Ch., 2024). Ця програма стала першим у світі антивірусом, хоча й надзвичайно спеціалізованим.

Reaper був розроблений за тим самим принципом, що й Creeper – він міг самостійно переміщуватися між комп'ютерами мережі ARPANET. Однак його метою було не розповсюдження, а пошук і знищення копій Creeper. Коли Reaper знаходив екземпляр Creeper на комп'ютері, він видаляв його і продовжував пошук на інших машинах мережі.

Механізм роботи Reaper був досить простим. Він використовував ті ж мережеві протоколи, що й Creeper, для пошуку комп'ютерів у мережі ARPANET. Потім він сканував кожну машину на наявність характерних ознак коду Creeper і, виявивши вірус, видаляв його. Після цього Reaper переходив до наступного комп'ютера.

Цікаво, що Reaper не лише знищував Creeper, але й виправляв будь-які зміни, які той вносив до системи. Це робило його не просто програмою видалення, а справжнім «лікувальним» засобом – характеристика, яка згодом стала ключовою для антивірусного програмного забезпечення.

Попри свою примітивність порівняно з сучасними вірусами та антивірусними рішеннями, Creeper і Reaper мали надзвичайно важливе значення для розвитку комп'ютерної безпеки. Вони показали, що програми можуть самостійно поширюватися мережею і що для боротьби з такими програмами можуть бути створені спеціалізовані захисні механізми.

У 1982 році, коли персональні комп'ютери тільки починали входити в масове використання, 15-річний школяр Річард Скрента створив програму, яка стала першим відомим вірусом для

персональних комп’ютерів. Вірус отримав назву «Elk Cloner» і був розроблений для комп'ютерів Apple II – одних із найпопулярніших персональних комп’ютерів того часу (Levy S., 2020).

Elk Cloner мав революційну для свого часу структуру, яка згодом стала типовою для багатьох комп'ютерних вірусів. Він складався з двох основних компонентів:

Резидентний модуль – частина вірусу, яка завантажувалася в оперативну пам’ять комп’ютера при запуску інфікованої дискети і залишалася там протягом усього сеансу роботи комп'ютера.

Поширювальний модуль – код, відповідальний за інфікування нових дискет, вставлених у комп’ютер протягом сеансу.

Алгоритм дій Elk Cloner був надзвичайно ефективним для свого часу. Вірус інфікував завантажувальний сектор дискет операційної системи Apple DOS 3.3. Коли комп’ютер завантажувався з інфікованої дискети, вірус спочатку активувався, а потім передавав управління операційній системі, яка продовжувала нормальний процес завантаження. Користувач не помічав нічого незвичайного, тоді як вірус вже функціонував у фоновому режимі.

Особливо цікавим аспектом Elk Cloner був його поетичний «корисний вантаж». Після 50 завантажень з інфікованої дискети вірус активував своє корисне навантаження: на екрані з’являвся гумористичний текст (Levy S., 2020): *Elk Cloner: The program with a personality It will get on all your disks It will infiltrate your chips Yes, it's Cloner! It will stick to you like glue It will modify RAM too Send in the Cloner!*

З технічної точки зору вірус був дуже компактним – займав менше 400 байт, що було важливо для розміщення в обмеженому просторі завантажувального сектора дискети.

Поява Elk Cloner мала значний вплив на комп’ютерну спільноту початку 1980-х років, хоча цей вплив суттєво відрізнявся від реакції на сучасні вірусні загрози. Оскільки вірус був скоріше жартом, ніж шкідливою програмою, його поширення не спричинило серйозних економічних збитків або втрати даних. Однак він викликав цілу гаму реакцій серед користувачів комп’ютерів Apple II – від здивування і захоплення до роздратування і стурбованості.

Важливим наслідком появи Elk Cloner стало усвідомлення потенційної вразливості персональних комп’ютерів до несанкціонованого програмного коду. Якщо раніше безпека комп'ютерних систем розглядалася переважно в контексті великих корпоративних або державних систем, то тепер стало очевидно, що і персональні комп’ютери потребують захисту.

Справжній розквіт епохи комп’ютерних вірусів розпочався з появою і масовим поширенням персональних комп’ютерів архітектури IBM PC (Ludwig M., 1995), поклавши початок другому з виділених етапів – часу мережевих вірусів та черв'яків. Якщо Apple II, для якого було створено Elk Cloner, залишався відносно нішевим продуктом, то IBM PC та його клони швидко стали домінуючою платформою на ринку персональних комп’ютерів.

Перший широко відомий вірус для IBM PC з’явився у 1986 році і отримав назву «Brain». Його творцями стали пакистанські брати Басіт та Амджад Фарук Алві, які керували магазином комп’ютерного обладнання у Лахорі (Solomon A., 1993). За словами самих братів, вірус було створено для відстеження піратського використання програмного забезпечення, яке вони розробляли.

Brain був завантажувальним вірусом, який інфікував завантажувальний сектор дискет. Коли комп’ютер завантажувався з інфікованої дискети, вірус завантажувався в оперативну пам’ять і залишався активним протягом усього сеансу роботи. Він відстежував звернення до дискет і, коли виявляв неінфіковану дискету, записував на неї свою копію (Highland H. J., 1988).

Однією з особливостей Brain було те, що вірус змінював мітку інфікованих дискет на «(c) Brain». Крім того, він містив текстове повідомлення з іменами, адресою та телефонними номерами його авторів – незвичайний крок, який свідчив про те, що брати Алві не сприймали своє творіння як злочин.

Текст повідомлення був таким:

Welcome to the Dungeon
(c) 1986 Basit & Amjad (pvt) Ltd.
BRAIN COMPUTER SERVICES

730 NIZAB BLOCK ALLAMA IQBAL TOWN
LAHORE-PAKISTAN
PHONE: 430791,443248,280530.
Beware of this VIRUS....
Contact us for vaccination...

Це повідомлення залишалося прихованим у коді вірусу і не відображалося користувачам, але могло бути виявлено при аналізі завантажувального сектора спеціальними утилітами.

Попри те, що Brain не був розроблений з метою завдання шкоди (він не видаляв файли і не пошкоджував дані), сам факт його існування та масового поширення мав значні наслідки. Інфіковані дискети поширювалися по всьому світу через звичайний обмін програмами між користувачами, а згодом і через продаж програмного забезпечення, що постачалося на дискетах, які були інфіковані ще на етапі виробництва. За деякими оцінками, протягом двох років після своєї появи він інфікував десятки тисяч комп'ютерів у різних країнах світу. Це змусило комп'ютерну індустрію та користувачів вперше серйозно задуматися про проблему комп'ютерних вірусів та необхідність захисту від них.

Brain також став причиною першої масштабної «епідемії» комп'ютерних вірусів, що привернула увагу медіа. У 1988 році про нього повідомляли такі видання, як The New York Times, що вивело проблему комп'ютерних вірусів за межі спеціалізованих технічних журналів і зробило її предметом суспільного обговорення (Lewis P. H., 1988).

Феномен Brain також висвітлив проблему міжнародного характеру комп'ютерних загроз. Вірус, створений у Пакистані, швидко поширився по всьому світу, демонструючи, що географічні кордони не є перешкодою для програмного коду. Це стало передвісником глобалізації кіберзагроз, яка досягла повного розвитку з поширенням інтернету в 1990-х роках.

Слідом за Brain з'явилася ціла плеяда вірусів для IBM PC, кожен з яких вносив нові елементи в еволюцію шкідливого програмного забезпечення. У 1987 році з'явився вірус Jerusalem, який став одним із перших, що мав виражену деструктивну функцію. Він був запрограмований на видалення всіх запущених програм у п'ятницю 13-го числа і став одним з перших прикладів вірусу з логічною бомбою – зловмисним кодом, що активується за певних умов (Malicious Life by Cybereason, 2017).

Майже одночасно з Jerusalem з'явився вірус Cascade, який отримав свою назву через візуальний ефект, який він створював: символи на екрані «падали» каскадом, формуючи купу внизу екрана. Cascade був одним з перших файлових вірусів, який інфікував виконувані файли, а не завантажувальні сектори. Він також був одним із перших шифрованих вірусів, що ускладнювало його виявлення антивірусним програмним забезпеченням.

У 1988 році з'явився вірус SCA (Soft Code Ata), який вважається першим поліморфним вірусом. Такі віруси можуть змінювати свій код при кожному новому інфікуванні, що робить їх надзвичайно складними для виявлення через сигнатурний пошук – основний метод, який використовували тогочасні антивірусні програми.

Наприкінці 1980-х років вірус Dark Avenger, створений болгарським програмістом, представив концепцію швидкого інфікування, відому як «Direct Action». Замість того, щоб чекати певної події або дати, цей вірус негайно починав інфікувати файли при запуску зараженої програми. Dark Avenger також містив механізм, який поступово пошкоджував дані на жорсткому диску, роблячи шкоду від вірусу більш підступною та складною для виявлення.

Варто відзначити вірус Michelangelo, який з'явився в 1991 році і отримав назву на честь художника Мікеланджело Буонарроті. Цей вірус був запрограмований на активацію 06 березня, в день народження митця, коли він перезаписував перші 100 секторів жорсткого диску, що робило комп'ютер непрацездатним (Snyder L. B., 1999). Michelangelo став причиною першої великої медіапаніки навколо комп'ютерних вірусів, коли в 1992 році ЗМІ прогнозували потенційне інфікування мільйонів комп'ютерів. Хоча ці прогнози виявилися значно перебільшеними, вірус дійсно завдав шкоди тисячам комп'ютерів по всьому світу.

Важливим етапом в еволюції вірусної загрози став черв'як Morris, створений аспірантом Корнельського університету Робертом Моррісом у 1988 році. Хоча технічно це був не вірус, а мережевий черв'як (програма, яка самостійно поширюється через мережу, використовуючи вразливості в мережевих протоколах і програмному забезпеченні), його поява мала величезне значення для розуміння потенціалу кіберзагроз (Spafford E. H., 1989). Черв'як Morris вразив приблизно 10% всіх комп'ютерів, підключених до тогочасного інтернету (близько 6000 машин), і спричинив перший великий мережевий збій (Chen T. M., 2004).

Таким чином, період з 1986 по 1991 роки можна розглядати як першу фазу розвитку комп'ютерних вірусів для IBM PC. За цей час віруси еволюціонували від відносно простих програм, що поширювалися через фізичні носії (як Brain), до складних самомодифікуючих конструкцій (як SCA) і руйнівних мережевих загроз (як черв'як Morris). Ця еволюція відобразила не лише технічний прогрес у програмуванні вірусів, але й зміну мотивації їхніх авторів – від експериментів і демонстрації технічних можливостей до навмисного завдання шкоди та вандалізму.

Однією з ключових особливостей цього періоду було те, що більшість вірусів створювалися індивідуальними програмістами, часто з метою самоствердження, демонстрації своїх навичок, або навіть як своєрідна форма цифрового графіті. Економічна мотивація, яка пізніше стала домінуючою в світі кіберзлочинності, в той час була майже відсутня.

Поширення комп'ютерних вірусів вплинуло на формування нових соціальних норм і практик використання комп'ютерів. Користувачі почали обережніше ставитися до програмного забезпечення невідомого походження, уникати обміну дискетами без попередньої перевірки, ретельніше контролювати доступ до своїх комп'ютерів. По суті, відбулася перша масова «соціалізація» користувачів у питаннях комп'ютерної безпеки (Бурячок В. Л., 2015).

У корпоративному середовищі поява вірусів стимулювала формування нових підходів до управління інформаційними технологіями. Якщо раніше питання IT-безпеки були переважно технічними і вирішувалися на рівні IT-відділів, то з поширенням вірусів та усвідомленням масштабу потенційних наслідків, вони перетворилися на стратегічні бізнес-питання, які потребували уваги на рівні вищого керівництва. Компанії почали впроваджувати політики інформаційної безпеки, проводити навчання співробітників з питань кібербезпеки, створювати спеціалізовані підрозділи для захисту інформаційних систем (Бурячок В. Л., 2015). Поступово сформувалася нова корпоративна культура, яка включала усвідомлення важливості інформаційної безпеки як невід'ємної частини бізнес-процесів.

Економічний вплив перших комп'ютерних вірусів був багатогранним. З одного боку, віруси спричиняли прямі збитки, пов'язані з втратою даних, простоєм комп'ютерних систем, витратами на відновлення працездатності інфікованих систем. З іншого боку, необхідність захисту від вірусів створила передумови для формування нової галузі економіки – індустрії кібербезпеки.

Щодо прямих збитків, то вони були досить значними навіть у випадку ранніх вірусів. Наприклад, черв'як Morris у 1988 році, за оцінками GAO (Government Accountability Office), спричинив збитки в розмірі від 10 до 100 мільйонів доларів США. Ці збитки включали витрати на відновлення систем, втрати через простій комп'ютерів та мереж, оплату робочого часу IT-спеціалістів, які займалися ліквідацією наслідків (Shoch J. F., 1982).

Один з ключових уроків, який можна отримати з історії перших комп'ютерних вірусів, полягає в усвідомленні фундаментального взаємозв'язку між технологічним прогресом та розвитком загроз. Історія показує, що нові технології неминуче створюють нові уразливості, які можуть бути експлуатовані зловмисниками. Це розуміння є надзвичайно важливим для сучасних фахівців з кібербезпеки, які мають передбачати потенційні вразливості в нових технологіях ще на етапі їх розробки та впровадження.

Принципи, закладені в ранніх вірусах, таких як здатність до саморепродукції, приховування своєї присутності, модифікація коду для уникнення виявлення, залишаються актуальними і в сучасних кіберзагрозах, хоча і в більш складних та витончених формах. Сучасні шкідливі

програми, такі як розвинені постійні загрози (Advanced Persistent Threats, APT), використовують багато концепцій, які вперше з'явилися в ранніх вірусах, але з більшою складністю та ефективністю (Грищук Р. В., 2016).

Наприклад, поліморфні віруси, які змінювали свій код при кожному новому інфікуванні для уникнення сигнатурного виявлення, стали попередниками сучасних технік ухилення від виявлення, таких як обфускація коду, шифрування та динамічна зміна характеристик шкідливого програмного забезпечення в реальному часі.

Модель розповсюдження ранніх вірусів через фізичні носії (дискети) еволюціонувала в сучасні методи поширення шкідливого ПЗ через інтернет, соціальну інженерію, фішинг, експлуатацію вразливостей веб-додатків та інші канали. Однак базовий принцип залишається тим самим – використання автоматизованих механізмів для максимально широкого розповсюдження шкідливого коду.

Досвід боротьби з першими вірусами значно вплинув на формування екосистеми обміну інформацією про загрози в спільноті фахівців з кібербезпеки (Грищук Р. В., 2016). Раннє усвідомлення того, що жодна організація не може самостійно протистояти всім кіберзагрозам, призвело до створення різноманітних платформ для обміну інформацією про нові загрози, вразливості та методи захисту. Сьогодні такі ініціативи, як CERT (Computer Emergency Response Team), форуми фахівців з безпеки, платформи для обміну індикаторами компрометації (IOC) є невід'ємною частиною глобальної системи кібербезпеки.

Історичний досвід боротьби з комп'ютерними вірусами має важливе значення для розуміння обмежень технічних рішень у сфері кібербезпеки. Фред Коен у своїх теоретичних роботах довів неможливість створення ідеального антивірусу, здатного виявити будь-який вірус. Це фундаментальне обмеження залишається актуальним і для сучасних систем безпеки, що змушує спеціалістів з кібербезпеки розробляти багаторівневі стратегії захисту, які комбінують різні підходи та технології (Ferbrache D., 1992).

Проведене дослідження дозволило встановити, що виникнення комп'ютерних вірусів у 1980-х роках стало закономірним результатом розвитку обчислювальної техніки та теоретичних досліджень у галузі самовідтворюваних систем. Концептуальне підґрунтя для появи вірусів було закладено ще в працях Джона фон Неймана про самовідтворювані автомати (1949), що засвідчує глибокий зв'язок між фундаментальною наукою та практичними проявами технологічного розвитку.

У ході дослідження визначено два ключові етапи становлення комп'ютерних вірусів як історичного феномену: перший – 1970-ті – середина 1980-х рр., пов'язаний з появою експериментальних та локальних вірусів, представлених такими програмами як Creeper, Reaper (1971) та Elk Cloner (1982); другий –кінець 1980-х – початок 1990-х рр., що характеризується поширенням мережевих вірусів та черв'яків, зокрема Brain (1986), Jerusalem (1987), Cascade (1987) та Morris (1988). Кожен із цих етапів відображає не лише технічну еволюцію шкідливого програмного забезпечення, але й трансформацію соціально-культурного контексту взаємодії суспільства з комп'ютерними технологіями.

Дослідження виявило трансформацію мотивації творців вірусів: від академічних експериментів та демонстрації технічних можливостей у ранній період до навмисного завдання шкоди наприкінці 1980-х років. Ця еволюція відображає загальні закономірності розвитку технологій, коли інструменти, створені з дослідницькою метою, згодом можуть бути використані для деструктивних цілей.

Доведено, що вірусні епідемії 1980-х років мали значні соціально-економічні наслідки, зокрема спричинили формування антивірусної індустрії, зміну корпоративних підходів до інформаційної безпеки та виникнення нових соціальних практик взаємодії з комп'ютерними системами. Ці процеси засвідчують, що історія комп'ютерних вірусів є невід'ємною складовою загальної історії науково-технічного прогресу XX століття.

Проведене дослідження заповнює існуючу в українській історіографії прогалину щодо історичного аналізу витоків кіберзагроз, систематизуючи та контекстуалізуючи розвиток комп'ютерних вірусів як важливого феномену в історії науки і техніки. Перспективи подальших досліджень полягають у вивченні еволюції комп'ютерних вірусів у 1990-х роках, коли поширення мережі Інтернет створило принципово нові умови для розвитку кіберзагроз.

Список літератури

Бурячок В. Л., 2015. Корченко О. Г. *Інформаційна та кібербезпека: соціотехнічний аспект*. Київ.

Грищук Р. В., 2016. Даник Ю. Г. *Основи кібернетичної безпеки*. Житомир.

Лавренюк В. А., 2024. Історія виникнення та розвитку комп'ютерних злочинів: вітчизняний та зарубіжний аналіз. *Актуальні проблеми вітчизняної юриспруденції*. № 6. 202–207.

Мазур Я. П., 2024. Основні кіберзагрози в умовах ведення інформаційної війни. *Адміністративне право і процес; фінансове право; інформаційне право*. 599–604.

Машталір В. 2024. Гук О., Мурасов Р., Фараон С., Лоза В. Кіберборотьба в умовах збройного протистояння: аналіз, стратегії та виклики. *Сучасні інформаційні технології у сфері безпеки та оборони*. № 49 (1). 93–104.

Стежко С. М., 2021. Фица В. М. Кібербезпека як важливий фактор забезпечення життєдіяльності вітчизняної енергетичної галузі. *Інформація і право*. №4 (39). 113–120.

Цукрук В. І., 2017. Етимологія назв комп'ютерних вірусів. *XLVI Науково-технічна конференція Інституту соціально-гуманітарних наук, Вінницький національний технічний університет*. [Електронний ресурс]: Режим доступу: https://conferences.vntu.edu.ua/index.php/all-hum/all-hum-2017/paper/viewFile/2264/ 1920 (14. 07. 2025).

Bhargava P., 2022. Choudhary R., Gupta A. A. Review Study on Computer Virus. *World Journal of Research and Review*. [Електронний ресурс]: Режим доступу: https://www.wjrr.org/download_data/WJRR1405018.pdf (15. 06. 2025).

Chen T. M., 2004. Robert J. M. *The Evolution of Viruses and Worms*. [Електронний ресурс]: Режим доступу: https://www.researchgate.net/publication/228869267_The_Evolution_of_Viruses_and_Worms (07. 07. 2025).

Cohen F., 1987. Computer Viruses: Theory and Experiments. *Computers & Security*. Vol. 6. 22–35.

Denning P. J., 1988. Computer Viruses. *American Scientist*. Vol. 76, No.3. 236–238.

Ferbrache D., 1992. *A Pathology of Computer Viruses*. Springer-Verlag.

Highland H. J., 1988. The Brain Virus: Fact and Fantasy. *Computers & Security*. Vol. 7, No. 4. 367–370.

Hiruni Ch., 2024. *From Creeper to Ransomware: The Evolution of Malware*. [Електронний ресурс]: Режим доступу: https://www.researchgate.net/publication/ 385891333_From_Creeper_to_Ransomware_The_Evolution_of_Malware (11. 07. 2025).

Kephart J. O., 1991. White S. R. Directed-Graph Epidemiological Models of Computer Viruses. *Proceedings of the IEEE Symposium on Security and Privacy*. 343–359.

Levy S., 2020. Crandall J. R. *The Program with a Personality: Analysis of Elk Cloner, the First Personal Computer Virus. arXiv:2007.15759v1 [cs.CR]*. [Електронний ресурс]: Режим доступу: https://arxiv.org/pdf/2007.15759 (10. 07. 2025).

Lewis P. H., 1988. Peripherals; Book Offers Medicine for Computer Viruses. *The New York Times*. November 1. Section C (Science Desk). 13. [Електронний ресурс]: Режим доступу: https://www.nytimes.com/1988/11/01/science/peripherals-book-offers-medicine-for-computer-viruses.html (30. 06. 2025).

Ludwig M., 1995. The Giant Black Book of Computer Viruses. *American Eagle Publications*.

Malicious Life by Cybereason: The Jerusalem Virus, 2017. Malicious Life, Episode 35. [Електронний ресурс]: Режим доступу: https://malicious.life/episode/ episode-35/ (20. 07. 2025).

Shoch J. F., 1982. Hupp J. A. The «Worm» Programs – Early Experience with a Distributed Computation. *Communications of the ACM*. Vol. 25, No.3. 172–180.

Snyder L. B., 1999. Responses to the Michelangelo Computer Virus Threat: The Role of Information Sources and Risk Homeostasis Theory. *Journal of Applied Social Psychology*. Vol. 29, No.5. 1011–1030.

Solomon A., 1993. *A Brief History of PC Viruses*. [Електронний ресурс]: Режим доступу: http://users.uoa.gr/~nektar/science/technology/a_brief_history_of_ viruses.htm (10. 06. 2025).

Spafford E. H., 1989. The Internet Worm Program: An Analysis. *Computer Communication Review*. Vol. 19, No.1. 17–57.

Von Neumann J., 1966. Theory of Self-Reproducing Automata. Urbana and London: University of Illinois Press. [Електронний ресурс]: Режим доступу: https://cba.mit.edu/events/03.11.ASE/docs/VonNeumann.pdf (15. 07. 2025).

Vitaliy Kondratiev

THE FIRST COMPUTER VIRUSES: THE BEGINNING OF THE HISTORY OF CYBER THREATS (1970S – EARLY 1990S)

The article investigates the emergence and evolution of the first computer viruses in the context of the history of cyber threats, focusing on the period of the 1980s. The theoretical prerequisites for creating self-replicating programs are examined, starting with John von Neumann's concepts of self-reproducing automata. The scientific work of Fred Cohen, who in 1983 first formalized the concept of a computer virus and experimentally proved the potential danger of viral programs, is analyzed. The history of creation and spread of the first viruses is covered: Creeper (1971), Reaper (1971), Elk Cloner (1982), Brain (1986), Jerusalem (1987), Cascade (1987), as well as the Morris network worm (1988). The technical features of early viruses, mechanisms of their functioning, and consequences of their spread are characterized. Special attention is paid to the transformation of virus authors' motivations – from academic experiments to deliberate harm. The socio-economic consequences of viral epidemics of the 1980s are investigated, including the formation of the antivirus industry, changes in corporate approaches to information security, and the emergence of new social practices in interaction with computer systems. The relationship between principles embedded in early computer viruses and modern cyber threats is established. The importance of studying the history of the first viruses for understanding the fundamental principles of malware functioning and developing effective cyber defense strategies in modern conditions is substantiated. Key lessons from the history of early computer viruses that have practical significance for modern cybersecurity specialists are presented. The conducted research fills an existing gap in Ukrainian historiography regarding the historical analysis of cyber threats' origins, systematizing and contextualizing the development of computer viruses as an important phenomenon in the history of science and technology.

Key words: *cybersecurity, cyber threats, computer, history of science and technology, information technologies.*

References:

Buriachok V. L., 2015. Korchenko O. H. *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt* [Information and cybersecurity: sociotechnical aspect]. Kyiv. (In Ukrainian).

Hryshchuk R. V., 2016. Danyk Yu. H. *Osnovy kibernetychnoi bezpeky* [Fundamentals of cybersecurity]. Zhytomyr. (In Ukrainian).

Lavreniuk V. A., 2024. Istoriia vynyknennia ta rozvytku komp'iuternykh zlochyniv: vitchyznianyi ta zarubizhnyi analiz [History of the emergence and development of computer crimes: domestic and foreign analysis]. *Aktual'ni problemy vitchyznianoi iurysprudentsii*. № 6. 202–207. (In Ukrainian).

Mazur Ya. P., 2024. Osnovni kiberzahrozy v umovakh vedennia informatsiinoi viiny [Main cyber threats in the conditions of information warfare]. *Administratyvne pravo i protses; finansove pravo; informatsiine pravo*. 599–604. (In Ukrainian).

Mashtalir V., 2024. Huk O., Murasov R., Faraon S., Loza V. Kiberborot'ba v umovakh zbroinoho protystoiannia: analiz, stratehii ta vyklyky [Cyber warfare in the conditions of armed confrontation: analysis, strategies and challenges]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony*. №49 (1). 93–104. (In Ukrainian).

Stezhko S. M., 2021. Fytsa V. M. Kiberbezpeka iak vazhlyvyi faktor zabezpechennia zhyttiediial'nosti vitchyznianoi enerhetychnoi haluzi [Cybersecurity as an important factor in ensuring the vital activity of the domestic energy industry]. *Informatsiia i pravo*. №4 (39). 113–120. (In Ukrainian).

Tsukruk V. I., 2017. Etymolohiia nazv komp'iuternykh virusiv [Etymology of computer virus names]. *XLVI Naukovo-tekhnichna konferentsiia Instytutu sotsial'no-humanitarnykh nauk, Vinnyts'kyi natsional'nyi tekhnichnyi universytet*. [Online]: Available from: https://conferences.vntu.edu.ua/index.php/all-hum/all-hum-2017/paper/viewFile/2264/1920 [Accessed: 14. 07. 2025]. (In Ukrainian).

Bhargava P., 2022. Choudhary R., Gupta A. A Review Study on Computer Virus. *World Journal of Research and Review*. [Online]: Available from: https://www.wjrr.org/download_data/WJRR1405018.pdf [Accessed: 15. 06. 2025]. (In English).

Chen T. M., 2004. Robert J. M. *The Evolution of Viruses and Worms*. [Online]: Available from: https://www.researchgate.net/publication/228869267_The_Evolution_ of_Viruses_and_Worms [Accessed: 07. 07. 2025]. (In English).

Cohen F., 1987. Computer Viruses: Theory and Experiments. *Computers & Security*. Vol. 6. 22–35. (In English).

Denning P. J., 1988. Computer Viruses. *American Scientist*. Vol. 76, No.3. 236–238. (In English).

Ferbrache D., 1992. *A Pathology of Computer Viruses*. Springer-Verlag. (In English).

Highland H. J., 1988. The Brain Virus: Fact and Fantasy. *Computers & Security*. Vol. 7, No4. 367–370. (In English).

Hiruni Ch., 2024. *From Creeper to Ransomware: The Evolution of Malware*. [Online]: Available from: https://www.researchgate.net/publication/385891333_From_ Creeper_to_Ransomware_The_Evolution_of_ Malware [Accessed: 11. 07. 2025]. (In English).

Kephart J. O., 1991. White S. R. Directed-Graph Epidemiological Models of Computer Viruses. *Proceedings of the IEEE Symposium on Security and Privacy*. 343–359. (In English).

Levy S., 2020. Crandall J. R. *The Program with a Personality: Analysis of Elk Cloner, the First Personal Computer Virus. arXiv:2007.15759v1* [cs.CR]. [Online]: Available from: https://arxiv.org/pdf/2007.15759 [Accessed: 10. 07. 2025]. (In English).

Lewis P. H., 1988. Peripherals; Book Offers Medicine for Computer Viruses. *The New York Times*. November 1. Section C (Science Desk). 13. [Online]: Available from: https://www.nytimes.com/1988/11/01/science/peripherals-book-offers-medicine-for-computer-viruses.html [Accessed: 30. 06. 2025]. (In English).

Ludwig M., 1995. The Giant Black Book of Computer Viruses. *American Eagle Publications*. (In English).

Malicious Life by Cybereason: The Jerusalem Virus. Malicious Life, Episode 35. [Online]: Available from: https://malicious.life/episode/episode-35/ [Accessed: 20. 07. 2025]. (In English).

Shoch J. F., 1982. Hupp J. A., 1982. The «Worm» Programs – Early Experience with a Distributed Computation. *Communications of the ACM*. Vol. 25, No. 3. 172–180. (In English).

Snyder L. B., 1999. Responses to the Michelangelo Computer Virus Threat: The Role of Information Sources and Risk Homeostasis Theory. *Journal of Applied Social Psychology*. Vol. 29, No5. 1011–1030. (In English).

Solomon A., 1993. *A Brief History of PC Viruses*. [Online]: Available from: http://users.uoa.gr/~nektar/science/technology/a_brief_history_of_viruses.htm [Accessed: 10. 06. 2025]. (In English).

Spafford E. H., 1989. The Internet Worm Program: An Analysis. *Computer Communication Review*. Vol. 19, No1. 17–57. (In English).

Von Neumann J., 1966. Theory of Self-Reproducing Automata. Urbana and London: University of Illinois Press. [Online]: Available from: https://cba.mit.edu/ events/03.11.ASE/docs/VonNeumann.pdf [Accessed: 15. 07. 2025]. (In English).

Дата першого надходження статті до видання: 02.02.2026
Дата прийняття статті до друку після рецензування: 18.03.2026
Дата публікації (оприлюднення) статті: 18.05.2026