УДК 004.9.056.5

***Коваленко Д.М.***
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

***Олещенко Л.М.***
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

***Юрчишин В.Я.***
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

# ДЕЯКІ ПИТАННЯ БЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

*Проаналізовано еволюцію та природу комп'ютерних вірусів. Розглянуто аналогію між комп'ютерними та біологічними екосистемами. Виділено основні відмінності між біологічними та комп'ютерними вірусами. Розглянуто можливі напрямки використання знань про імунну систему людини та механізми боротьби з хворобами для зміцнення стійкості комп'ютерних систем до дії різного типу комп'ютерних вірусів. На основі аналогії комп'ютерних вірусів із живими екосистемами виділено перспективи розвитку нових технологій для підтримання оптимального функціонування комп'ютерних систем і мереж.*

***Ключові слова:*** *інформаційна безпека, комп'ютерний вірус, шкідливе програмне забезпечення, антивірусна програма, вразливості, аналогія, операційна система, BLAST, Welchia, ДНК, РНК, біологічна екосистема, реплікація, інфікування, імунітет.*

**Постановка проблеми.** Тема інформаційної безпеки стала сьогодні однією з найголовніших, оскільки будь-які порушення в роботі обчислювальних систем із кожним роком стають для людства все більш небезпечними. Однією з актуальних проблем, пов'язаних зі «здоров'ям» комп'ютерів, є проблеми їх захисту від комп'ютерних вірусів і хакерських нападів.

У кібербезпеці можна виділити два основні типи загроз. Першим типом є викрадення інформації з метою скористатися результатами чужої праці. Метою другого типу є бажання проникнути у ваше оточення і якомога більше його зруйнувати. Людство має багато інструментів для боротьби з цими загрозами. Стосовно інформаційної безпеки, перша складова частина пов'язана з шифруванням і засекреченням інформації, вона має найбільші напрацювання й у цій статті не розглядатиметься. Друга пов'язана з навмисним пошкодженням інформаційних систем комп'ютерними вірусами й однією з найактуальніших проблем, пов'язаних із захистом від шкідливих програм [2–5]. На наш погляд, вивчення природи комп'ютерних вірусів і їх аналогії з живими екосистемами може дати людству відповіді на численні питання та сприяти розвитку нових технологій для підтримання оптимального функціонування комп'ютерних систем і мереж. Тому розглянемо більш детально ці питання.

**Викладення основного матеріалу дослідження.** *Еволюція та природа комп'ютерних вірусів.* Комп'ютерний вірус – це шкідлива програма, здатна до створення своїх функціонально ідентичних копій. Віруси вміють розмножуватися, мутувати і заражати інші комп'ютерні програми.

Вперше слово «комп'ютерний вірус» використав Фред Коен (Fred Cohen). У ті роки можливість існування вірусів розглядалася тільки теоретично, й алгоритми їх функціонування описувалися не мовами програмування, а термінами системи команд математичних формалізмів типу «машини Тюрінга» або нормальних алгоритмів Маркова. Коен розглянув тільки ті можливості «машини Тюрінга», дані яких (на магнітній стрічці) призначені для подальшої інтерпретації і самі є програмами [6; 7]. Ф. Коен вивчав саморозмножуючі комп'ютерні «механізми» з теоретичних позицій, довів можливість існування саморозмножую-

чих програм у захищених операційних системах (далі – ОС) і продемонстрував декілька практичних реалізацій для комп'ютерів VAX під управлінням ОС UNIX, розглядаючи цю проблему в ідеалізованій ОС без будь-яких дефектів. Наявність «дірок» в ОС збільшувала масштаби епідемії. Автори перших вірусів самостійно відкривали невідомі особливості ОС і вчилися користуватися ними. Але пізніше (1988 р.) почала складатися ситуація, коли виявлялися не тільки самі віруси, але і їх ретельно прокоментовані вихідні тексти.

Ідея створення реплікуючих сутностей зародилася ще в 50-х рр. минулого століття. Американці проводили дослідження зі створення і розповсюдження в ЕОМ таких програмних продуктів. Одна з таких робіт проводилася на IBM 650. Сутності могли розмножуватися, мутувати, знищувати (поїдати) одне одного. «Їжею» для таких сутностей були ненульові елементи. Цим самим людина безпосередньо долучилася до моделювання живої матерії і до небезпечної гонитви за лідерством у цьому напрямку. Саме тому у світі зараз проводиться такий великий масштаб антивірусних робіт із залученням найдосвідченіших фахівців і величезних ресурсів. Для фоннеймановської архітектури обчислювальних систем програмний код і дані не розрізнені, й очікувати тут на суттєві здобутки марно. У сучасних процесорах та ОС робляться спроби розділити код і дані введенням ознак виконуваного коду і захисту від запису для різних ділянок пам'яті. Але поки ці ознаки можна довільно «вмикати» і «вимикати», принципових заборон існуванню вірусів нема. Вони з'являться, якщо обчислювальна система реалізована за правилами альтернативної архітектури, наприклад, «гарвардської». Згідно з цією архітектурою, код і дані мають бути розділені фізично й існувати в різних масивах пам'яті. Відповідно, процесор повинен працювати з двома комплектами системних магістралей – шин адреси, даних і вводу – виводу. Це накладно, але такий принцип вже використовується в мікроконтролерних системах. Повсюдне введення «гарвардської» архітектури означає корінний перегляд практики програмування і взагалі використання комп'ютерної техніки.

**Метою статті** є пошук можливих напрямків використання знань про імунну систему людини та механізми боротьби з хворобами для підвищення стійкості комп'ютерних систем до дії різного типу комп'ютерних вірусів.

*Використання аналогії між комп'ютерними та біологічними екосистемами.* Комп'ютери можна порівняти з живими екосистемами. Крихітні Unix-програми підтримують роботу масивних додатків на основі графічного інтерфейсу, приховані процеси обертаються в тандемі, щоб створити інформацію. Оскільки людство створило штучні джунглі з транзисторів і обчислень, у ньому також було створено віруси.

Комп'ютерний вірус, незважаючи на те, що він є продуктом людської творчості, є природною і, можливо, необхідною частиною мережевої обчислювальної екосистеми. Віруси уповільнюють процеси, пошкоджують дані, можуть завдати фізичної шкоди (як у випадку з w32.Stuxnet), а також зберігатися в чіпах PRAM і BIOS. Вони можуть перетинати екологічні кордони, як, наприклад, у випадку USB-переходу stuxnet або AppleiPod, випадково завантаженого за допомогою вірусів Windows, вони стають більш стійкими. Віруси, включені за допомогою поліморфних або метаморфічних движків, створені для обфускації антивірусного програмного забезпечення (далі – ПЗ), що дозволяє більш широко розповсюджувати і сповільнювати конструктивний відгук із боку тих, хто займається цим захистом. Віруси діють шляхом зараження хоста і використання його механізмів для відтворення та інших цілей.

У живому світі бактерії становлять собою одноклітинні організми, які процвітають у різних органічних середовищах, викликаючи ряд ефектів в одному і тому ж вигляді. Наприклад, бактерії служать основним механізмом, що сприяє розпаду в біологічних системах (наприклад, бактерії, які допомагають перетравлювати їжу). Відомі випадки спроб створити «корисні» віруси. У середині 90-х рр. існувала прихована битва (різного роду), поширена у мільйонах системах по всьому світу. Вірус BLAST і хробак Welchia були двома вірусами з різними намірами. Blast (w32/Lovesan.worm) був шкідливим вірусом, який заразив системи Windows через незахищений механізм віддаленої системи вікна, хробак Welchia заражав системи за тим же механізмом, але його корисне навантаження, яке повинне бути запущене за успішної інфекції, було серією корисних патчів для ПЗ Windows. Він також фіксував механізм входу і через деякий час знищувався. Незважаючи на цей добрий намір, Welchia створив проблеми для багатьох користувачів: зіпсував системні конфігурації, прив'язав мережевий трафік і перезапустив системи, коли була встановлене його корисне навантаження [8; 9].

У живих системах бактерії виконують роль здорового розпаду та стійкості до опору господаря проти довкілля. Існує припущення щодо

можливості створення ПЗ та ОС, які були б сприйнятливі до вірусів, хоча б для боротьби з надлишком застарілих систем, що виникають за більш дешевих обчислень і більшого доступу. Можливо, мережа комп'ютерів також може мати хороші відносини в галузі охорони здоров'я й обслуговування один з одним, внаслідок чого всі стають сильнішими.

Знання про біологічні віруси можуть допомогти визначити маршрути, які були зроблені розробниками вірусів. За аналогією до біологічних вірусів як живих організмів, що складаються з ДНК або РНК всередині білкового покриття, їх кіберпросторові аналоги (комп'ютерні програми) паразитують на своєму хості і можуть відтворюватися лише всередині цього хоста.

Подібно до біологічного вірусу, який повинен мати правильну специфіку господаря і тканини, щоб закріпитися, комп'ютерний вірус повинен бути сумісний із системою, щоб закріпитися у ній. Вірус, черв'як або троянський кінь можуть, як і ВІЛ (вірус імунодефіциту людини), бути прихованими і стати активними через деякий проміжок часу. Ці три класи комп'ютерних шкідливих програм також можуть мати сотні варіантів і модифікованих версій, які аналогічні мікробній різноманітності. Подібно до того, як імунна система людського тіла виходить з-під контролю і починає руйнувати себе (аутоімунна хвороба), комп'ютери також можуть стати жертвою таких захворювань.

Біологічні віруси «крадуть» вірулентні гени інших вірусів і стають більш злоякісними. Це також відбувається й у разі шкідливого ПЗ комп'ютера. Всього за тиждень після вересневого нападу на Сполучені Штати був випущений небезпечний черв'як Nimda, який об'єднав найпотужніші стратегії двох інших програм хробака і поширився швидше, ніж будь-який інший попередній черв'як. Природа розвинула імунітет, який захищає рослини і тварин від широкого спектру патогенів. У кишечнику кожної людини є природна мікрофлора, яка забезпечує частковий захист від інфекцій. Чи можемо ми розробити «доброякісні» комп'ютерні віруси, які можуть безперешкодно поширюватися через Інтернет, автоматично блокувати записи для злоякісних вірусів, оновлювати антивірусні програми або інактивувати наявні віруси? Мікробіологи можуть допомогти програмістам боротися з вірусами – комп'ютерний імунітет може бути дорогим, але в кінцевому підсумку ризики і витрати можуть бути виправдані. Існує припущення, що, навпаки, вивчення комп'ютерних шкідливих програм може допомогти контролювати появу інфекційних захворювань у людей. Інтернет може бути гарною моделлю для вивчення розвитку інфекцій і того, як вони поширюються у нашому світі. Швидкість еволюції віртуальних патогенів дозволяє стежити за процесом мутації і вибору в реальному часі [10].

Порівняння між комп'ютерними і людськими вірусами потрібне для того, щоб дослідники могли краще розуміти, чому імунна система людини набагато краще бореться з вірусами, ніж антивірусні системи.

Атака «Відмова в обслуговуванні» (DoS) схожа на дію ВІЛ, тому що обидва спрямовані на перевантаження системи. ВІЛ атакує імунну систему, роблячи людину більш вразливою до певних захворювань. Комп'ютерні віруси, такі як W32 / Sality, також використовують цю стратегію, встановлюючи шкідливу програму в якості авторизованого додатку для обходу брандмауера Microsoft. Дослідники також вказали, що і люди, і комп'ютери заражають себе. Комп'ютери можуть заразитися, відвідавши веб-сайт і завантаживши шкідливу програму, вбудовану в сайт, який намагається встановити себе на комп'ютери.

Відомо, що біологічні віруси, такі як вірус грипу, змінюються після реплікації. Коли віруси реплікуються, вони мутують. Таку поведінку можна порівняти з тим, як працюють віруси Conficker і Koobface. Це кошмар для аналітиків безпеки, тому що кожен реплікований зразок значно відрізняється від свого попередника. Однією з важливих відмінностей між цими поліморфними вірусами є те, що комп'ютерні віруси тільки змінюють форму (змінюється тільки пакет, код залишається незмінним). Комп'ютерні віруси, подібні до Conficker, також інкубують, ховаючись у системах, щоб атакувати пізніше, що можна порівняти з грипом.

Розглянемо основні відмінності між біологічними і комп'ютерними вірусами. Якщо хтось напише програмний код вірусу грипу, файл, який містить код цього вірусу, буде не більшим 22 КБ. Комп'ютерні віруси набагато більші. Дослідники відзначають, що біологічні віруси не можуть застосовувати методи, зіставні з методами шифрування й антидетонації. У цьому разі виникають серйозні проблеми з виготовленням ліків, що усувають такі варіації вірусу. Існує гіпотеза, що людські та комп'ютерні віруси можуть сходитися в майбутньому. Більшість людських вірусів ДНК або РНК-коду містять основні генетичні інструкції для усіх відомих живих організмів [9; 10]. За словами дослідників [9; 10], межа між цифровим і

біологічним світом розмивається, цитуючи кібернетичний протез як хороший приклад. Вони відзначають, що у деяких людей є кілька електронних пристроїв у їх тілі, наприклад, кардіостимулятор, стимулятори мозку і кохлеарні імплантати. Як тільки ці пристрої будуть взаємодіяти із зовнішніми машинами, що в більшості випадків необхідно в якийсь момент, теоретично вони можуть стати вразливими для комп'ютерних вірусів.

У 2002 р. вчені змогли синтезувати поліовірус. Відтоді біотехнологія просунулася далі, що дозволило синтезувати бактерії, й організми генетично модифікуються майже щодня. Крім того, весь код синтетичної ДНК зберігається на комп'ютерах. У 2010 р. сумнозвісний вірус Stuxnet зміг проскочити через установку зі збагачення урану, захопити контроль над своїм ПЛК (програмований логічний контролер) і знищити його пристрій.

Дослідники намагаються знайти відповідь на питання, чи можливо розробити вірус зі шкідливими послідовностями ДНК, які могли б, коли вони були записані в біти, використовувати ці уразливості. Використання кодованого вірусу для впливу на біологію людини у військових цілях малоймовірно, оскільки комп'ютерний вірус набагато важче контролювати, ніж, наприклад, бактерії сибірської виразки. Звільнення вірусу може мати неприємні наслідки і заражати власну армію нації.

Віруси мають багато характеристик, і серед них – їх життєвий цикл. У біологічному контексті віруси є об'єктами, що складаються з генома в білковій оболонці (капсиді), оточеної в деяких типах вірусів мембраною. Їм потрібно проникнути у живу клітину (осередок хостингу), щоб вона могла відтворюватися. Комп'ютерні віруси, як і інші типи шкідливих програм, повинні вставляти свій власний код в іншу комп'ютерну програму, щоб реплікувати і виконуватися. Обидва типи вірусів не можуть копіюватися автономно. Тому перша проблема вірусів полягає у тому, щоб досягти свого хостингу або розміститися в ІТ-системі. Успішний механізм зараження є ключем до їх успіху. Порівняння з комп'ютерними вірусами може бути поширене на інші типи шкідливих програм. Фаза введення біологічних вірусів забезпечує їх захист від несприятливих умов (низька або висока температура, надмірна вологість тощо) і дозволяє їм виживати доти, поки вони не зможуть проникнути в господаря. Прикріплення вірусу до клітини-хазяїна є передумовою для його вторгнення. Потім генетичний матеріал вірусу вивільняється всередині клітини-господаря. Так само комп'ютерні віруси спочатку повинні отримати доступ до апаратних засобів або ПЗ цільового користувача. Первісна системна інфекція зазвичай виконується з використанням соціальної інженерії і вразливостей безпеки, часто за допомогою наявних у продажі наборів експлойтів, які часто зачіпають давно відомі уразливості.

Як тільки набір експлойтів або вірус може заразити хост-систему, починається другий етап, і завантажується корисне навантаження (дані, які виконуватимуть шкідливу активність) з вебсайту або запускає вбудоване корисне навантаження. Потім шкідливе ПЗ намагається зберегти хост-систему і знаходить файли або процеси з хорошими цілями. Всередині клітини-господаря вірус може залишатися бездіяльним (прихованим) або негайно почати реплікацію. Аналогічно комп'ютерні віруси, а також інші типи шкідливих програм можуть залишатися бездіяльними після зараження або почати реплікувати себе і поширюватися, щоб заражати інші хости або мережі.

У біології реплікація дозволяє вірусу виробляти численні копії свого геному й упаковувати ці нові копії в капсиди. У клітині господаря вірус продукує елементи, необхідні для його реплікації, використовуючи механізм клітин-господарів. Таким чином, заражена клітина-господар працює в інтересах вірусу. Після того, як зрілі нові віруси виходять за межі осередку хоста, вони вторгаються в інші осередки для нового циклу реплікації. Комп'ютерні віруси поміщають копію себе в інше ПЗ, зберігають свою актуальність в ОС або в інших ділянках диска або пам'яті. Таким чином, кожен хост має копію шкідливої програми, яка сама реплікуватиметься і поширюватися далі, заражаючи все більше комп'ютерів. Тригер є конкретною подією, яка призводить до виконання шкідливого коду комп'ютера, наявності інших програмних продуктів або файлу або конкретної дії користувача. Після активації за допомогою тригера комп'ютерний вірус виконує функцію, для якої він призначений: виконується етап виконання (виконується корисне навантаження). Це може бути руйнівним, наприклад, у разі видалення або пошкодження файлів на диску, шпигунства на стороні користувача у вигляді клавіатурних шпигунів, захоплень екрану або фільтрації даних.

**Висновки.** Сьогодення характеризується появою нових типів вірусів, які активно освоюють численні прогалини в програмах інформаційних систем. Кількість виявлених потенційних цілей для зараження вірусами збільшується з кожним роком, проте якість тестування програмного забезпечення

ще не досягло потрібного рівня. Розглянувши аналогії між біологічними та комп'ютерними вірусами, можемо припустити можливу користь і небезпеку нових форм матерії, які створює людство. Вивчення природи комп'ютерних вірусів може слугувати вивченню нових механізмів боротьби з хворобами. Механізми дії імунітету людини також можуть слугувати створенню нових технологій захисту комп'ютерних систем від дії шкідливого вірусного ПЗ. Сучасні ІТ-технології досягли такого рівня і таких масштабів, що їм під силу підтвердити припущення, що думка є матеріальною і що матерія зароджується з інформації. Неправильне використання вірусів може завдати непередбачуваної шкоди, а розумне їх застосування здатне породити нове покоління ЕОМ.

**Список літератури:**

1. Haris A. Khan, Ali Syed, Azeem Mohammad, Malka N. Halgamuge. Computer Virus and Protection Methods Using Lab Analysis. IEEE II International Conference on Big Data Analysis. 2017. P. 882–886.
2. Zhu Q., Yang X., Ren J. Modeling and analysis of the spread of computer virus. Communications in Nonlinear Science and Numerical Simulation. 2012. № 17 (12). P. 5117–5124.
3. Pham D.V., Syed A., Halgamuge M.N. Universal serial bus based software attacks and protection solutions. Digital Investigation. 2011. № 7 (3). P. 172–184.
4. Pham D.V., Halgamuge M.N., Syed A., Mendis P. Optimizing windows security features to block malware and hack tools on USB storage devices. Progress in electromagnetic research symposium. 2010. P. 350–355.
5. Vargas V., Syed A., Mohammad A., Halgamuge M.N. Pentaho and Jaspersoft: A Comparative Study of Business Intelligence Open Source Tools Processing Big Data to Evaluate Performances. Int. Journal of Advanced Computer Science and Applications (IJACSA). 2016. Vol. 7. № 10. P. 20–29.
6. Cohen F. Computer viruses: theory and experiments. Computers and Security. 1987. Vol. 6. P. 22–35.
7. Cohen F. Computational aspects of computer viruses. Computers and Security. 1989. Vol. 8. P. 325–344.
8. "Friendly" Welchia Worm Wreaking Havoc. URL: http://www.internetnews.com/ent-news/article.php/3065761/Friendly+Welchia +Worm+Wreaking+Havoc.htm/
9. Andrew LB Decay: Bacterial Computing. URL: http://andrewlb. com/2014/04/decay-bacterial-computing/.
10. Computer viruses vs biological viruses. URL: http://www. scienceinafrica.com/microbiology/.

**НЕКОТОРЫЕ ВОПРОСЫ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ**

*Проанализирована эволюция и природа компьютерных вирусов. Рассмотрено аналогию между компьютерными и биологическими экосистемами. Выделены основные различия между биологическими и компьютерными вирусами. Рассмотрены возможные направления использования знаний об иммунной системе человека и механизмы борьбы с болезнями для укрепления устойчивости компьютерных систем к действию различного типа компьютерных вирусов. На основе аналогии компьютерных вирусов с живыми экосистемами выделено перспективы развития новых технологий для поддержания оптимального функционирования компьютерных систем и сетей.*

***Ключевые слова:*** *информационная безопасность, компьютерный вирус, вредоносное программное обеспечение, антивирусная программа, уязвимости, аналогия, операционная система, BLAST, Welchia, ДНК, РНК, биологическая экосистема, репликация, инфицирование, иммунитет.*

**SOME SECURITY QUESTIONS IN INFORMATION SYSTEMS**

*The evolution and nature of computer viruses are analyzed. The analogy between computer and biological ecosystems is considered. The main differences between biological and computer viruses are highlighted. Possible directions of use of knowledge about the human immune system and mechanisms of struggle against illnesses for strengthening of stability of computer systems to action of various type of computer viruses are considered. Based on the analogy of computer viruses with living ecosystems, the prospects of the development of new technologies for maintenance of optimal functioning of computer systems and networks are highlighted.*

***Key words:*** *information security, computer virus, malware, antivirus program, vulnerabilities, analogy, operating system, BLAST, Welchia, DNA, RNA, biological ecosystem, replication, infection, immunity.*