**УДК 004**

**М.Грищенко, магістр гр. КІ-24М,**
*Центральноукраїнський національний технічний університет*

# ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ МЕРЕЖЕВОГО АНТИВІРУСНОГО КОМПЛЕКСУ ДАТА-ЦЕНТРУ

У статті розроблено програмне забезпечення, яке призначено для системи мережевого антивірусного комплексу дата-центру. Метою розробки є дослідження та принципи побудови системи мережевого антивірусного комплексу дата-центру. Об’єктом дослідження є процес мережевого антивірусного комплексу дата-центру. Предметом дослідження є методи мережевого антивірусного комплексу дата-центру. Методи дослідження базуються на методах теорії побудови комп’ютерних мереж, теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи мережевого антивірусного комплексу дата-центру. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

**мережа, антивірус, дата-центр**

**Постановка проблеми.** Масове використання комп'ютерів, а також швидкий розвиток комп'ютерних мереж (зокрема мережі Інтернет) сприяли появі й поширенню шкідливих програм – комп'ютерних вірусів. Віруси часом роблять роботу на комп'ютері неможливою. Вони, залежно від ситуації, можуть завдати значної шкоди як інформації, так і самому комп'ютеру.

Незважаючи на поширену думку, центри обробки даних не є «куленепробивними» від хакерських атак. Ви можете бути в більшій небезпеці, якщо володієте сервером, оскільки кіберзлочинці нападуть на вас з усією силою. На ринку є чимало антивірусних продуктів, але не всі вони підходять для центру обробки даних. Гарна новина полягає в тому, що з найкращим антивірусом ви можете перестати турбуватися про будь-які зовнішні загрози.

Іншими словами, центр обробки даних – це обладнання, яке зберігає інформацію (для бізнесу, урядів тощо). Крім того, той факт, що до цих даних можна отримати доступ з будь-якого куточка світу, перетворює центри обробки даних на корисний інструмент. Усі уповноважені сторони можуть отримати ту саму інформацію, фактично не відвідуючи місцезнаходження центру обробки даних. Однак, оскільки інформація вільно передається між різними комп’ютерами, це полегшує злочинцям її отримання.

**Аналіз останніх досліджень і публікацій.** При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи мережевого антивірусного комплексу дата-центру.

**Мета й завдання дослідження.** Метою роботи є дослідження та принципи побудови системи мережевого антивірусного комплексу дата-центру.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем мережевого антивірусного комплексу дата-центру.
– Дослідження системи мережевого антивірусного комплексу дата-центру.
– Програмна реалізація системи мережевого антивірусного комплексу дата-центру.

*Об’єктом дослідження* є процес мережевого антивірусного комплексу дата-центру.

*Предметом дослідження* є методи мережевого антивірусного комплексу дата-центру.

*Методи дослідження* базуються на методах теорії побудови комп'ютерних мереж, теорії захисту інформації, методах математичної статистики, методах розробки програмного забезпечення.

**Виклад основного матеріалу. Класифікація комп'ютерних вірусів**

Вся наявна розмаїтість комп'ютерних вірусів можна класифікувати по різних ознаках, – наприклад по середовищу перебування, по руйнівних можливостях, по особливостях побудови й т.д.

За способом зараження:

– резидентні – віруси, що залишають в оперативній пам'яті свою резидентну (постійну) частина, що потім перехоплює звертання до програм, що заражаються, і впроваджується в них;

– нерезидентні – віруси, які не заражають оперативну пам'ять і проявляються лише при запуску інфікованої програми.

По цілісності:

– монолітні – віруси, програми яких являють собою єдиний блок;

– розподілені – віруси, програми яких розділені на частини, що містять інструкцію з відтворення вірусу (наприклад, одна якась частина заражає комп'ютер, а потім завантажує з Інтернету інші частини, що виконують шкідливу дію).

**Інші шкідливі програми**

Крім розглянутих вище комп'ютерних вірусів, існують і інші види шкідливих програм. Серед них, наприклад, можна назвати:

– мережні хробаки – шкідливі програми, які поширюються по комп'ютерних мережах, обчислюючи адреси мережних комп'ютерів і розсилаючи по цих адресах свої копії;

– троянські програми («троянські коні», квазивіруси) – шкідливі програми, які не здатні до самопоширення, а маскуються під якусь корисну або цікаву програму, руйнують завантажувальний сектор і файлову систему або збирають і пересилають своєму творцеві інформацію, що не підлягає розголошенню (наприклад, ваші особисті паролі);

**Антивірусні програми**

Антивірусні програми призначені для захисту комп'ютерів від більшості вірусів, хробаків і «троянських коней», які можуть видаляти файли, одержувати доступ до особистих даних або використовувати заражену систему як засіб атаки на інші комп'ютери.

Антивірусні програми звичайно використовують два різних методи для виконання своїх завдань:

1) сканування (перегляд) файлів для пошуку вже відомих вірусів, для яких у вірусній базі (щовходить у комплект антивірусної програми спеціальної БД) є інформація про характерні фрагменти вірусного програмного коду (сигнатурах вірусів);

2) виявлення підозрілого поводження будь-якої програми, що схоже на поводження зараженої програми («евристичне сканування»).

Антивірусне програмне забезпечення складається з пакета програм, які виявляють, запобігають розмноженню й видаляють комп'ютерні віруси й інші шкідливі програми.

При виборі антивірусної програми необхідно враховувати наступні параметри, яким антивірус повинен відповідати:

1. Сталість і надійність роботи. Цей параметр є визначальним. При стабільній роботі антивірусної програми немає відчуття, що якісь заражені файли залишилися непоміченими.

2. Великий обсяг і постійне відновлення вірусної бази. Сюди ж ставиться вміння програми швидко пізнавати види вірусів працювати з файлами різних типів (архівами, документами), і здійснювати автоматичну перевірку всіх нових файлів у міру їхнього копіювання.

3. Швидкість роботи антивірусу й додаткові функції. До додаткових функцій можна віднести наявність евристичного сканування й можливість лікування заражених файлів (коли віруси з них віддаляються, а файли приводяться у вихідний стан, що був до їхнього зараження).

4. Підтримка різних програмою багатьох операційних систем – багатоплатформеність. При роботі в мережному варіанті немаловажним є також наявність в антивірусної програми серверних модулів, призначених для адміністрування, і наявність можливості роботи на різних серверах.

**Захист робочого столу**

У минулому захист робочих столів був єдиною «сферою», де використовувалися антивіруси. Сьогодні він все ще має вирішальне значення для захисту центрів обробки даних, але має великий недолік. Річ у тім, що для його роботи кожен кінцевий користувач повинен регулярно оновлювати своє програмне забезпечення. Крім того, важко відстежувати їх усі, що наражає центр на небезпеку.

Сучасні антивіруси для комп'ютерів мають численні автоматичні сповіщення. Люди часто забувають про них, відкладають їх або ігнорують, що, знову ж таки, робить всю систему вразливою. Ось як працює захист комп'ютера: антивірус сканує диски та оперативну пам'ять (RAM), шукаючи шкідливий код у базі даних.

Також, щойно система виявляє потенційно небезпечний файл/програму, користувач отримує сповіщення. Далі користувач може вибрати одну з наступних дій: видалення вірусу, спроба очищення файлів/програм або поміщення їх у карантин. Це все, що вам потрібно знати про антивірусний захист робочого столу. Він не ідеальний, але й донині центри обробки даних включають його як надійний рівень захисту.

**Захист сервера**

У цьому випадку антивірусне рішення працює на рівні поштового сервера. Це означає, що більшість шкідливих кодів будуть знищені ще до того, як вони потраплять на комп'ютери користувачів. На жаль, навіть за наявності антивіруса, що захищає сервери, вірусам все ж вдається потрапити в мережу. Захист сервера так само важливий, як і захист робочого столу, але в більшості випадків він є «бонусом», і саме тому міжнародні компанії його використовують.

Якщо ви покладаєтеся лише на антивірус сервера, а шкідливе програмне забезпечення потрапляє на робочі столи, ніщо не завадить йому пошкодити/знищити конфіденційні бізнес-дані. Тому вам потрібно використовувати все це разом, включаючи наступний (і останній) захист – на рівні «шлюзу». Він працює подібно до захисту сервера, але має дещо інший підхід.

**Захист шлюзу**

Ідея полягає в тому, щоб зупинити шкідливе програмне забезпечення в найвіддаленішій точці, задовго до того, як воно отримає шанс досягти мережі. Поки віруси/пошкоджені повідомлення тримаються на відстані, вони не зможуть завдати жодної шкоди центру обробки даних. Шлюзи існують не так давно, але вони вже довели свою ефективність як захист на рівні серверів і робочих столів.

Інтеграція антивірусного програмного забезпечення в мережеве обладнання є серцем і душею підходу шлюзу. На рівні шлюзу антивірус сканує всі вхідні повідомлення, шукаючи будь-які потенційні загрози. Крім того, коли він виявляє заражені повідомлення, він або зупиняє їх, поміщає в карантин, або видаляє їх. На думку експертів, це прогресивне рішення є дуже перспективним і, найімовірніше, стане новою нормою в найближчі роки.

Завдяки інтегрованим продуктам, вбудованим безпосередньо в мережі, захист центрів обробки даних від зовнішніх загроз стане набагато комфортнішим. Вам слід знати, що уряди різних країн також використовують підхід «центр обробки даних/сервер», і це одна з причин, чому безпека кінцевих точок стає важливою частиною світу, в якому ми зараз живемо.

Антивірусний комплекс дата-центру – це не тільки антивірус і антишпигун. Він визначає й нейтралізує різні види небажаного ПЗ.

Основні переваги:

– Невимогливість до ресурсів – відмінно працює на настільних ПК, ідеальний для роботи на ноутбуках.

– Можливість установки на заражену машину й лікування ураженої системи.

– Коректна перевірка «на лету» вхідної й вихідної пошти по протоколах SMTP, POP3, IMAP, NNTP.

– Захист від шпигунських, рекламних програм, хакерських утиліт і програм-дозвонщиків.

– Висока частота відновлень вірусних баз – до декількох разів у годину! Відновлення виробляється з локальних серверів мережі.

Масове поширення комп'ютерних вірусів, а також активне обговорення в пресі планів інформаційної війни із залученням хакерів для придушення ворожих систем керування й передачі даних привели до того, що питання про створення засобів протидії й захисти здобуває нову якість. На думку ряду закордонних експертів, держава, що програла в інформаційній війні, буде відкинуто у своєму розвитку на багато десятиліть.

Сьогодні вже ясно, що традиційні методи побудови систем захисту інформації не принесуть бажаного результату. Треба шукати принципово нові підходи до рішення цієї проблеми. Справжня стаття покликана дати «інформацію до міркування» для розроблювачів антивірусних систем, щоб вони змогли глянути на свою предметну область із іншої сторони, а саме – з боку Природи, що створила, напевно, саму зроблену систему захисту – імунну систему організму.


Рисунок 1 – Структурна схема системи

Уже розроблений ряд алгоритмів, що дозволяють писати віруси, які принципово не можна виявити жодним з існуючих способів. Багато хто відзначають, що самоідентифікуємий довільним образом код одержати просто неможливо. У кожному разі, є тверді рамки, які дозволяють ту саму операцію реалізувати обмеженим числом способів. Способи ці відомі заздалегідь, що, у принципі, дозволяє перелічити всі ключові фрагменти вірусів, а значить – безпомилково їх розпізнати.

Однак якщо припустити, що архітектура процесора може бути довільною, або навіть динамічно синтезованої в процесі виконання, то досить написати емулятор відповідного

процесора – деяку віртуальну машину, що буде виконувати код вірусу, побудований на певних принципах.

Вірус, написаний на віртуальній машині, вимагає дуже багато часу для аналізу традиційними методами. Виходить, потрібні засоби автоматичної боротьби з такого роду деструктивними програмами. Питання лише в тім, на яких принципах повинна базуватися така антивірусна система? Відповідь виявляється дивно простою: на принципах імунної системи людини. Дійсно, у нашім організмі функціонує чудова система, здатна боротися з мільярдами хвороботворних антигенів.

Антивірусна технологія антивірусного комплексу дата-центру побудована на основі моделі імунної системи людини.

Очевидно, що створити систему захисту інформації комп'ютерної мережі по прямій подобі імунної системи людини практично неможливо, так у цьому й немає необхідності. Однак той факт, що імунна система досягла досконалості в боротьбі із хвороботворними й чужорідними антигенами, говорить про те, що багато принципів, що сформували імунну систему, досить ефективні й можуть бути використані з тим допущенням, що працювати вони будуть не з біохімічними антигенами, а з антигенами програмними, тобто інформаційними.

Поряд із цим останні досягнення в області створення багатоагентних інтелектуальних систем дозволяють сподіватися, що найближчим часом штучна імунна система буде створена і її ефективність не опуститься нижче ефективності її природного прототипу.

**Висновки**. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів мережевого антивірусного комплексу дата-центру. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем мережевого антивірусного комплексу дата-центру.

– Досліджена система мережевого антивірусного комплексу дата-центру.

– На основі отриманих результатів досліджень створена програмна реалізація системи мережевого антивірусного комплексу дата-центру. Розроблені алгоритми дозволяють успішно вирішувати завдання мережевого антивірусного комплексу дата-центру. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

## Список літератури


1. Smirnov, O., Kuznetsov, A., Kavun, S., Babenko, B., Nakisko, O., Kuznetsova, K., «Malware Correlation Monitoring in Computer Networks of Promising Smart Grids», 2019 IEEE 6th International Conference On Energy Smart Systems (2019 IEEE ESS), Kyiv, Ukraine April 17-19, 2019 P. 347-352.
2. Smirnov, O., Kuznetsov, A., Kovalchuk, D., Pastukhov, M., Kuznetsova, K., Prokopovych-Tkachenko, D., «Discrete Signals with Special Correlation Properties», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 618-629.
3. Smirnov, O., Kuznetsov, A., Kiian, A., Kuznetsova, K., Ivko, T., Prokopovych-Tkachenko, D., «Soft Decoding Based on Ordered Subsets of Verification Equations of Turbo-Productive Codes», CEUR Workshop Proceedings Volume 2353, CEUR Workshop Proceedings 2019, Pages 873-884.
4. Smirnov A.A., Kuznetsov A.A., Danilenko D.A., Berezovsky A., «The statistical analysis of a network traffic for the intrusion detection and prevention systems», Telecommunications and Radio Engineering. – Volume 74, Issue 1. – Begel House Inc. – 2015. – P. 61-78.
5. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New Technique for Hiding Data in Cover Images Using Adaptively Generated Pseudorandom Sequences». CEUR Workshop Proceedings Volume 2732, 2020, Pages 214-227.
6. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Книшук А.В. «Вступ до кібербезпеки»: навчальний посібник – Кропивницький: ЦНТУ – 2022. – 968 с.
7. Теорія та практика сучасного інформаційно-психологічного протиборства: навчальний посібник / [В.М. Петрик, С.О. Гнатюк, М.М. Присяжнюк та ін.]; за заг. ред. С.О. Гнатюка, В.М. Петрика та О.А Смірнова. – Полтава, 2022. – 334 с.
8. Smirnov O. Kuznetsov A., Zaicenko Yu., Pastukhov M., Oleshko O., Kuznetsova K., «Formation of Discrete Signals with Special Correlation Properties». International Conference on Information and Telecommunication Technologies and Radio Electronics, UkrMiCo 2019; Odessa; Ukraine; 9-13 September 2019. P.22-28.

9. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В., Поліщук Л.І. Інформаційна безпека в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2020. – 294 с.
10. О.А. Смірнов, П.С. Усік, «дослідження перспектив використання технологічних рішень в мережах 5g» у Кібербезпека та інформаційні технології: монографія. – Х. : ТОВ «ДІСА ПЛЮС», 2020.С. 122-135.
11. Смірнов О.А., Конопліцька-Слободенюк О.К., Смірнов С.А., Буравченко К.О., Смірнова Т.В. Поліщук Л.І. Проектування комп'ютерних систем та мереж. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2019. – 264 с.
12. Smirnov, O., Kuznetsov, A., Shekhanin, K., Chepurko, I. Detecting Hidden Information in FAT. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 412-429. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook)
13. Smirnov, O., Kuznetsov, A., Kuznetsova., K. Synthesis of Discrete Signals with Improved Correlation Properties. Монографія: In.: ISCI'2019: Information Security in Critical Infrastructures. Collective monograph. Edited by Ivan D. Gorbenko and Alexandr A. Kuznetsov, ASC Academic Publishing, USA, 2019, pp. 281-299. – ISBN: 978-0-9989826-8-7 (Hardback), ISBN: 978-0-9989826-9-4 (Ebook).
14. Смірнов О.А., Гнатюк С.О., Кавун С.В., Терейковський І.А., Жмурко Т.О., Смірнов С.А., Коваленко А.С. Основи безпеки в комп'ютерних мережах. Навчальний посібник – Кропивницький: вид. Лисенко В.Ф. 2018. – 177 с.
15. Смірнов О.А., Стасєв Ю.В., Бараннік В.В. Коваленко О.В., Доренський О.П., Дрєєв О.М., Вялкова В.І. Інформаційна безпека держави. Підручник – Кіровоград: РВЛ КНТУ, 2016. – 263 с
16. Смірнов О.А., Кавун С.В., Коваленко О.В., Дрєєв О.М. Мережні інформаційні технології. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 159 с.
17. Смірнов О.А., Кавун С.В., Коваленко О.В., Доренський О.П., Дрєєв О.М., Вялкова В.І. Комп'ютерні мережі. Навчальний посібник – Кіровоград: РВЛ КНТУ, 2016. – 233 с.
18. Смірнов О.А., Стасєв Ю.В. Бараннік В.В. Захист інформації в автоматизованих системах управління. Навчальний посібник – Харків: ХУПС, 2015. – 264 с.
19. Усік, П.С., Смірнова, Т.В., Буравченко, К.О., Смірнов, О.А., Улічев, О.С., Смірнов, С.А. «Дослідження технологій забезпечення кібербезпеки банківських систем з використанням штучного інтелекту». Кібербезпека: освіта, наука, техніка. 2025. Том 1 № 29. С.704–716, 2025
20. Kuznetsov, O., Frontoni, E., Kuznetsova, K., Arnesano, M., Smirnov, O. «A secure biometric authentication architecture for blockchain-driven cyber-physical systems». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 193–224.
21. Kuznetsov, O., Atzeni, G., Arnesano, M., Randieri, C., Smirnov, O. «Secure IoT-based smart wheelchair system: From implementation to security enhancement strategy». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 225–257.
22. Kuznetsov, O., Smirnov, O., Kuznetsova, T., Shaikhanova, A., Svatowsky, I. «Privacy-utility trade-offs in IoT networks: A comparative analysis of differential privacy mechanisms for sensor data aggregation». Security and Privacy of Cyber Physical Systems Emerging Trends Technologies and Applications, 2025, pp. 589–622.
23. Lakhno, V., Malyukov, V., Smirnov, O., Bebeshko, B., Chubaievskiy, V., Zhumadilova, M., Malyukova, I., Smirnov, S. «Multifactorial Model for Targeted Attacks Counteracting Within the Framework of a Multi-Step Quality Game with Fuzzy Information». 8th International Symposium on Intelligent Informatics, ISI 2023, 2025. vol 389. pp 377-389. Springer, Singapore.
24. Kuznetsov O., Frontoni E., Kuznetsova Y., Smirnov O., Moskovchenko I. «Trust-Based Security Architecture for Edge Computing: A Simulation Study of Dynamic Trust Evolution and Attack Detection». CEUR Workshop Proceedings, 2024, 3909, pp. 227–241.
25. Kuznetsov, O., Frontoni, E., Kryvinska, N., Chevardin, V., Smirnov, O. «Wireless Network Encryption Stream Ciphers, Computational Modeling, and Security Analysis». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 379–402.
26. Kuznetsov, O., Frontoni, E., Kryvinska, N., Smirnov, O., Imoize, G.L. «Computational Modeling of Enhanced Spread Spectrum Codes for Asynchronous Wireless Communication». Computational Modeling and Simulation of Advanced Wireless Communication Systems, 2024, pp. 403–447.
27. Ткаченко, О., Ільєнко, А., Улічев, О., Мелешко, Є., Смірнов, О. «Правові засади поширення інформаційних впливів в соціальних мережах». Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2024. № 2(26), С. 170–188.
28. Смірнова Т.В., Конопліцька-Слободенюк О.К., Буравченко К.О., Смірнов С.А., Кравчук О.В., Козірова Н.Л., Смірнов О.А. «Дослідження технологій забезпечення кібербезпеки хмарних сервісів IaaS, PaaS та SaaS». Кібербезпека: освіта, наука, техніка. 2024. №4(24), С. 6-27.
29. Вінтенко, Б., Миронець, І., Смірнов, О., Кравчук, О., Козірова, Н., Савеленко, Г., Коваленко, А. «Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки». Кібербезпека: освіта, наука, техніка. 2024. №3(23), С. 111-131.
30. Батрак О., Смірнова Т., Гнатюк В., Одарченко Р., Смірнов О. «Дослідження показників ефективності функціонування та перспектив розвитку систем IP-телефонії». Підводні технології, 2024, № 13, с. 28-35.
31. Kuznetsov, O., Kryvinska, N., Ilchenko, O., Smirnova, T., Ulianovska, Y. «Comparative Analysis of Cryptocurrency Trading Platforms Using the Analytic Hierarchy Process». CEUR Workshop Proceedings, 2023, 3628, pp. 106-115.