ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2021, № 5 (95)

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ ТА МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ

УДК 004.4

Д. С. АСТАХОВ[1*], Н. О. ЛИСЕНКО[2*], В. Б. МАЗУРЕНКО[3*], А. І. ФЕДОРОВИЧ[4*]

[1*]Каф. «Радіоелектронна автоматика», Дніпровський національний університет імені Олеся Гончара, пр. Гагаріна, 72, Дніпро, Україна, 49000, тел. +38 (056) 374 98 22, ел. пошта astakhov.ds@gmail.com, ORCID 0000-0002-8636-1776
[2*]Каф. «Радіоелектронна автоматика», Дніпровський національний університет імені Олеся Гончара, пр. Гагаріна, 72, Дніпро, Україна, 49000, тел. +38 (056) 374 98 22, ел. пошта LysenkoNA@ukr.net, ORCID 0000-0001-6865-6207
[3*]Каф. «Радіоелектронна автоматика», Дніпровський національний університет імені Олеся Гончара, пр. Гагаріна, 72, Дніпро, Україна, 49000, тел. +38 (056) 374 98 22 ел. пошта mazurenko_v@yahoo.com, ORCID 0000-0001-8340-012X
[4*]Каф. «Радіоелектронна автоматика», Дніпровський національний університет імені Олеся Гончара, пр. Гагаріна, 72, Дніпро, Україна, 49000, тел. +38 (056) 374 98 22, ел. пошта sonya.sokolovskaya@gmail.com, ORCID 0000-0003-0752-7190

Аналіз сучасного антивірусного програмного забезпечення в задачах кібербезпеки

Мета. Наше дослідження спрямовано на отримання узагальнених знань щодо сучасного антивірусного програмного забезпечення (ПЗ), яке як є один із аспектів кібербезпеки є об'єктом постійних дискусій щодо доцільності його використання. **Методика.** Для отримання даних автори провели огляд світової літератури з теми роботи з використанням повнотекстових і реферативних баз даних. Розглянуто сигнатурні та евристичні методи роботи антивірусного програмного забезпечення, а також умовний поділ цих продуктів на: програми-детектори, програми-лікарі, програми-ревізори, програми-фільтри, програми-імунізатори. **Результати.** Контент-аналіз публікацій із проблем антивірусного програмного забезпечення доводить численність досліджуваних аспектів, зокрема щодо спроможності такого програмного забезпечення не тільки розпізнавати загрозу, але й бути здатним знищити її. Для виконання цього завдання антивірус повинен мати такі функції: регулярне (або в режимі реального часу) сканування системних файлів і програм; сканування вмісту месенджерів та електронної пошти; повне сканування комп'ютера за командою користувача; моніторинг вхідного та вихідного мережевого трафіка; усунення наслідків роботи шкідливого ПЗ. Крім того, порівняльний аналіз найбільш популярного антивірусного ПЗ дає можливість виявити недоліки та переваги кожного з них. **Наукова новизна.** Набув подальшого розвитку системний та узагальнювальний аналіз наявного та найбільш поширеного антивірусного програмного забезпечення, що надає можливість звичайним користувачам усвідомлено роботи вибір щодо встановлення таких програмних пакетів. **Практична значимість.** Отримані результати щодо можливостей наявного ПЗ дають змогу коригувати безпеку роботи в інтернет-мережі. Крім того, викладене розвіює міфи, поширювачі яких, пропонують користувачам узагалі не захищати свої комп'ютери від шкідливого програмного забезпечення. Наше дослідження також може бути корисним під час вивчення дисципліни «Основи тестування програмного забезпечення», організації науково-практичних семінарів, курсів підвищення кваліфікації тощо.

Ключові слова: програмне забезпечення (ПЗ); інформаційна загроза; антивірус; сингулярний метод; евристичний метод

Вступ

У процесі розвитку людства постійно відбувалися різні політичні та економічні процеси, безліч воєн і конфліктів. І в сучасному світі цей процес не припиняється ні на мить. Сьогодні набагато рідше можна побачити відкрите протистояння якихось країн чи корпорацій, але їх боротьба проходить на інформаційному фронті щодня. І ця боротьба – це не лише боротьба за

doi: https://doi.org/10.15802/stp2021/253290

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2021, № 5 (95)

людську лояльність, а й протистояння, приховане від очей звичайних людей, із метою отримати перевагу над супротивником. Про це свідчать нові й нові повідомлення про злами великих компаній або відомств цілих країн [9].

Комп'ютер може зберігати та обробляти достатньо велику кількість інформації, яка в наш час є одним із найдорожчих ресурсів. У міру розвитку та модернізації комп'ютерних систем і програмного забезпечення зростає обсяг і підвищується вразливість даних, що зберігаються в них. Сьогодні можна з упевненістю констатувати, що комп'ютерні віруси залишаються однією з найпоширеніших причин спотворення та знищення життєво важливої інформації, що може призвести до фінансових та часових втрат. За даними [6], зростає частка заражень шкідливим програмним забезпеченням. Три чверті атак на юридичних осіб та 62 % атак на приватних осіб супроводжувалися зараженнями шкідливим програмним забезпеченням.

Таким чином, актуальність поставленої проблеми визначається як її теоретичним, так і прикладним значенням.

Мета

Щодня з'являються нові й нові загрози. Однією з таких загроз є шкідливе програмне забезпечення (далі ПЗ). На противагу йому прогрес у сфері захисту інформації сприяє постійному розвитку та вдосконаленню антивірусного ПЗ. Наше дослідження спрямовано на отримання узагальнених знань щодо сучасного антивірусного програмного забезпечення, як один з аспектів кібербезпеки є об'єктом постійних дискусій щодо доцільності його використання.

Методика

Для отримання необхідних даних автори провели огляд світової літератури з теми дослідження із використанням повнотекстових і реферативних баз даних. Таким чином, теоретичною базою дослідження стали наукові статті, що висвітлюють: 1) питання доцільності використання антивірусного ПЗ; 2) досвід у впровадженні антивірусних програм та їх перевага й недоліки.

Не існує єдиної системи класифікації та найменування вірусів (хоча спроба створити стандарт була зроблена на зустрічі CARO 1991 року).

Прийнято поділяти віруси за:

1) об'єктами, що уражаються (файлові віруси, завантажувальні віруси, протиантивірусні віруси, скриптові віруси, макровіруси, мережеві черв'яки);

2) способом зараження (перезаписувальні віруси, віруси-компаньйони, файлові черв'яки, віруси-ланки, паразитичні віруси, віруси, що вражають вихідний код програм);

3) операційними системами та платформами, що уражаються (DOS, Microsoft Windows, Unix, Linux та інші);

4) активністю (резидентні віруси, нерезидентні віруси);

5) технологіями, які застосовують віруси (нешифровані/шифровані віруси, поліморфні віруси, стелс-віруси (руткіт та буткіт));

6) деструктивними можливостями (нешкідливі віруси, безпечні віруси, небезпечні віруси, дуже небезпечні віруси);

7) мовою, якою написаний вірус (асемблер, мова програмування високого рівня, скриптова мова, інші).

Існує безліч методів виявлення вірусів, до основних слід віднести сигнатурні та евристичні.

Сигнатурні методи – це точні методи виявлення вірусів, основою яких є порівняння файла зі зразком вірсу. Суть сигнатурного аналізу полягає у виявленні елементів, характерних для шкідливого ПЗ, у файлах, які сканують. Такий метод не придатний для захисту від нових вірусів, оскільки їх сигнатури ще виділено [8].

Евристичні методи – це приблизні методи виявлення шкідливого ПЗ, що дозволяють, із певною часткою ймовірності, зробити припущення, що файл заражений. Евристичний аналіз заснований на припущенні про схожість нових вірусів на якийсь із раніше виявлених. Виявлення сигнатур за такого методу є приблизним, що робить його більш універсальним, але менш точним [8].

Усе антивірусне програмне забезпечення можна умовно поділити на такі види:

doi: https://doi.org/10.15802/stp2021/253290

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2021, № 5 (95)

– програми-детектори здійснюють пошук сигнатури вірусу (послідовності байтів характерної для конкретного вірусу) в оперативній пам'яті та файлах системи, результатом роботи такої програми буде відповідне повідомлення;

– програми-лікарі знаходять заражені вірусами файли та проводять «лікування», що полягає у видаленні з файла тіла програми вірусу, повертаючи файли у вихідний стан. Окремим видом є поліфаги – програми-лікарі, призначені для великої кількості вірусів;

– програми-ревізори запам'ятовують вихідний стан програм, каталогів та системних областей диска, а потім, із певною періодичністю або за командою користувача, порівнюють поточний стан із вихідним [3];

– програми-фільтри, також відомі як «сторожа», є невеликими резидентними програмами, призначеними для виявлення потенційно небезпечної активності, яка може бути шкідливим ПЗ. У разі виявлення такої активності «сторож» тимчасово блокує джерело загрози, пропонуючи користувачеві вибрати відповідну дію;

– програми-імунізатори запобігають зараженню файлів шляхом модифікації програми або розділу диска таким чином, щоб це не позначалося на їхній роботі, це робить такі файли невразливими для шкідливого ПЗ, що працює за принципом ідемпотентності. Цей факт обмежує можливості застосування такого виду антивірусного ПЗ [7].

Сьогодні на ринку ПЗ представлено багато різних продуктів, що також включають антивіруси. Таке ПЗ відрізняється як вендорами, а і функціоналом. Більшість програмних продуктів представлені у двох варіантах – платному та безкоштовному. Під час вибору антивірусу слід керуватися в першу чергу необхідним функціоналом, який у платних версіях набагато ширше представлений, а безкоштовної версії антивірусу буде достатньо для мінімального рівня захисту.

Як правило, платні антивіруси відрізняються від безкоштовних такими перевагами:

– пісочниця, що є ізольованим середовищем для запуску підозрілих програм, дозволяє частково відокремити головну операційну систему від виконуваної програми;

– батьківський контроль, що дозволяє обмежити функціонал ПК як загалом, так і окремих програм, таким чином, наприклад, убезпечивши використання ПК дитиною, що випливає із самої назви функції;

– функція перевірки та очищення системи, що дозволяє підтримувати стан ПК на оптимальному рівні;

– контроль мережі Wi-Fi – функція для фільтрації вхідного потоку даних з інтернету;

– захист від спаму, що дозволяє обмежити користувача від небажаних повідомлень та/або повідомлень.

Результати

Наведемо порівняльний аналіз найбільш популярних антивірусних програм, який містить інформацію про переваги та недоліки кожного із зазначених пакетів:

1. Kaspersky. Серед його переваг: 1) можливість використовувати з некомерційною метою повністю безкоштовний антивірус; 2) відмінні показники захисту системи в тестах незалежних лабораторій; 3) повноцінне використання антивірусної бази у безкоштовній версії; 4) зручні підписки на платні версії з підтримкою кількох пристроїв. До недоліків належать: 1) немає повноцінної технічної підтримки для користувачів Kaspersky Free; 2) обмежена функціональність у безкоштовній версії [6].

2. McAfee – це потужні інструменти та високий рівень безпеки. Серед його переваг: 1) доступність на всіх пристроях: комп'ютерах з Windows та MacOS, смартфонах з Android та iOS; 2) 30-денна пробна версія на передплату з 10 пристроями; 3) багата колекція додаткових функцій безпеки: фаєрвол, сканер вразливостей, файловий шредер, видалення тимчасових та непотрібних даних; 4) підписка McAfee LiveSafe з необмеженою кількістю пристроїв. Серед недоліків: 1) суперечливі результати в тестах незалежних лабораторій; 2) немає тривалих підписок.

3. Захистник Windows – вбудований антивірус від Microsoft. Серед його переваг: 1) за замовчуванням вбудований у всі версії Windows 10, не потребує додаткового налаштування; 2) пропонує прості, але

doi: https://doi.org/10.15802/stp2021/253290

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2021, № 5 (95)

ефективні інструменти захисту від вірусів-шифрувальників; 3) глибока інтеграція із системою дозволяє отримати доступ до інших функцій безпеки Windows; 4) завжди захищає систему, якщо вимкнути його навмисно або встановити сторонній антивірус. До недоліків належать: 1) ускладнена процедура примусового вимкнення лише через редагування параметрів у системному реєстрі; 2) слабкий захист від малонебезпечних програм, які можуть зашкодити системі; 3) проблеми з визначенням фішингових сайтів; 4) погані результати у виявленні шкідливих посилань.

4. ESET NOD32 – антивірус для особистого та корпоративного використання. Серед його переваг: 1) відмінні результати в тестах незалежних організацій; 2) безкоштовні пробні версії антивірусу для всіх пристроїв; 3) відмінне поєднання вартості та функціональності; 4) висока швидкість сканування системи. До недоліків належать: 1) слабкі показники в тестах захисту від фішингових атак; 2) складний інтерфейс контролю під час купівлі передплати на кілька пристроїв.

5. Bitdefender – якісний та безкоштовний антивірус. Серед його переваг:1) використання у безкоштовній та платній версіях однакових технологій захисту; 2) відмінні показники захисту в тестах незалежних експертів; 3) можливість користуватися лише безкоштовною версією; 4) оптимізація в разі повторного сканування – час перевірки зменшується у кілька разів. До недоліків належать: 1) немає додаткових інструментів безпеки, доступних в інших комерційних антивірусах; 2) у безкоштовній версії не розпізнаються окремі небезпеки; 3) у безкоштовній версії немає файлового шредера та захисту від програм-вимагачів [10].

6. Sucuri – платформа для перевірки вебсайтів на віруси. Серед його переваг: 1) високий рівень захисту сайтів від зламу, потрапляння в чорний список Google та впровадження шкідливого коду; 2) боротьба з фішингом та SEO-спамом; 3) захист від DDoS, використання CDN, підтримка SSL-сертифікатів; 4) відновлення сайту після зламування в разі купівлі тарифу Pro або Business. Серед недоліків: 1) підходить тільки для веб-сайтів, не захищає операційні системи; 2) досить обмежена безкоштовна версія; 3) висока вартість тарифів, проте гарантія повернення коштів діє 30 днів [4].

7. Dr.Web – флагманський продукт компанії «Доктор Веб». Серед його переваг: 1) тестовий період на 3 місяці під час реєстрації на сайті антивірусу; 2) додатковий інструмент захисту від «атак нульового дня», який не конфліктує з іншими антивірусами; 3) використання хмарної системи моніторингу для швидкого реагування на небезпеку; 4) розширені функції забезпечення приватності: захист від несанкціонованого під'єднання до вебкамери та мікрофона, блокування шпигунських програм. До недоліків належать: 1) зниження швидкості завантаження файлів через їх постійні перевірки антивірусом; 2) поділ сигнатурної та несигнатурної частини на два окремі продукти з порівнянною вартістю підписки; 3) підтримка лише одного пристрою у всіх ліцензіях; 4) розробники проти участі їх продукту в тестах у сторонніх лабораторіях, тому складно знайти незалежні відомості про роботу антивірусу.

8. Avast – популярний безкоштовний антивірус. Серед його переваг: 1) підтримка пасивного режиму захисту, що дозволяє використовувати Avast у зв'язці з іншими антивірусами та запускати його лише для сканування системи; 2) високі бали в лабораторних тестах на різні типи загроз та продуктивність; 3) захист покупок від підроблених сайтів відомих компаній; 4) розширені інструменти захисту від шкідливих програм: перевірка на мережному рівні після завершення завантаження та перед запуском файла; 5) відмінний захист від атак фішингу. До недоліків належать: 1) безкоштовно доступні лише основні можливості. За додаткові інструменти та підтримку потрібно платити, але користувач дізнається про це лише після встановлення антивірусу; 2) автоматичне встановлення «Панелі інструментів Google» у всі браузери, від якої потрібно вручну відмовлятися в разі інсталяції антивірусу [4].

9. Norton Security – один із найстаріших та перевірених антивірусів. Серед його переваг:

doi: https://doi.org/10.15802/stp2021/253290

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2021, № 5 (95)

1) мультиплатформність – доступний на PC, Mac, мобільних пристроях з Android та iOS; 2) гарантія видалення вірусів із поверненням грошей за ліцензію, якщо система була заражена; 3) вбудований брандмауер, який контролює вхідний та вихідний трафік; 4) автоматичне резервне копіювання важливих файлів; 5) надання місця в захищеному хмарному сховищі. До недоліків належать: 1) додаткові можливості на кшталт батьківського контролю та менеджера паролів доступні лише в найдорожчому тарифі. В інших антивірусів ця функціональність введена в безкоштовну версію або як мінімум молодші редакції; 2) високі вимоги до ресурсів ПК (щоб не помічати уповільнення роботи системи, необхідно оптимізувати антивірус); 3) антивірус хороший, але дорогий, хоча часто бувають знижки.

10. Avira – антивірусне програмне забезпечення від німецьких розробників. Серед його переваг: 1) автоматичне видалення шкідливих програм, навіть якщо користувач не запускає сканування; 2) підтримка різних режимів сканування; 3) непогані оцінки в лабораторних тестах; 4) фокусування на антивірусних функціях без додавання великої кількості непотрібних інструментів; 5) періодично трапляються суттєві знижки на 3 місяці, інколи ж на перший рік використання; 6) є повністю безкоштовна версія, хоч і досить обмежена навіть в елементарних можливостях. Серед недоліків: 1) тривала процедура сканування системи (інші антивіруси перевіряють файли набагато швидше та не менш ефективно); 2) не справляється з блокуванням фінансових загроз; 3) у безкоштовній версії немає можливості додавати файли/папки у винятки, можна лише відновити, але це не завжди допомагає; 4) антивірус блокує цілком нешкідливі програми, тому, з урахуванням попередніх пунктів, його робота створює більше проблем, ніж приносить користі, висновок – безкоштовна версія Avira є неліквідом, краще вже Defender використовувати чи оплачувати підписку, де все працює; 5) висока вартість підписки Prime, у якій доступне під'єднання до 5 пристроїв на одному обліковому записі і є програми для Android та iOS [2].

У табл. 1 наведена узагальнена інформація щодо використання переліченого антивірусного програмного забезпечення.

Але існує невелика кількість антивірусного ПЗ, яке категорично не рекомендовано використовувати [7].

До таких програм належать:

– Malwarebytes, оскільки він непогано бореться з фішингом, шпигунами, але, власне, як антивірус досить посередній;

– eScan – слабкий антивірус, єдина перевага якого – зручний, простий інтерфейс;

– PC Matic – ним не варто користуватися: він незручний, порівняно з іншими складний у налаштуванні, неефективний;

– Bull Antivirus. Робота програми більше нагадує роботу спамного бота, що без кінця сипле вікнами з помилками та попередженнями;

– Sophos – найгірший антивірус 2019 року за однією із версій, з того часу нічого не змінилося;

– Element Anti-Virus – рекордсмен із помилкових спрацьовувань, блокує навіть порожні файли, не кажучи про все інше.

Звичайно, кожен користувач сам несе відповідальність за збереження своїх даних, і, зрозуміло, можна взагалі обійтися без антивірусного ПЗ, але для цього рівень компетентності користувача повинен бути вкрай високий [10]. Для ілюстрації цього на рис. 1 наведена статистика за 2019 рік, згідно з даними Microsoft Security Intelligence Report Volume 22. Діаграма відображає кількість комп'ютерів, на яких не встановлено антивірусне ПЗ (синій колір на діаграмі), встановлено та вимкнено (жовтий колір), встановлено, але не оновлювалено (зелений колір) та відкладено (коричневий колір).

doi: https://doi.org/10.15802/stp2021/253290

ISSN 2307–3489 (Print), ISSN 2307–6666 (Online)

Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2021, № 5 (95)

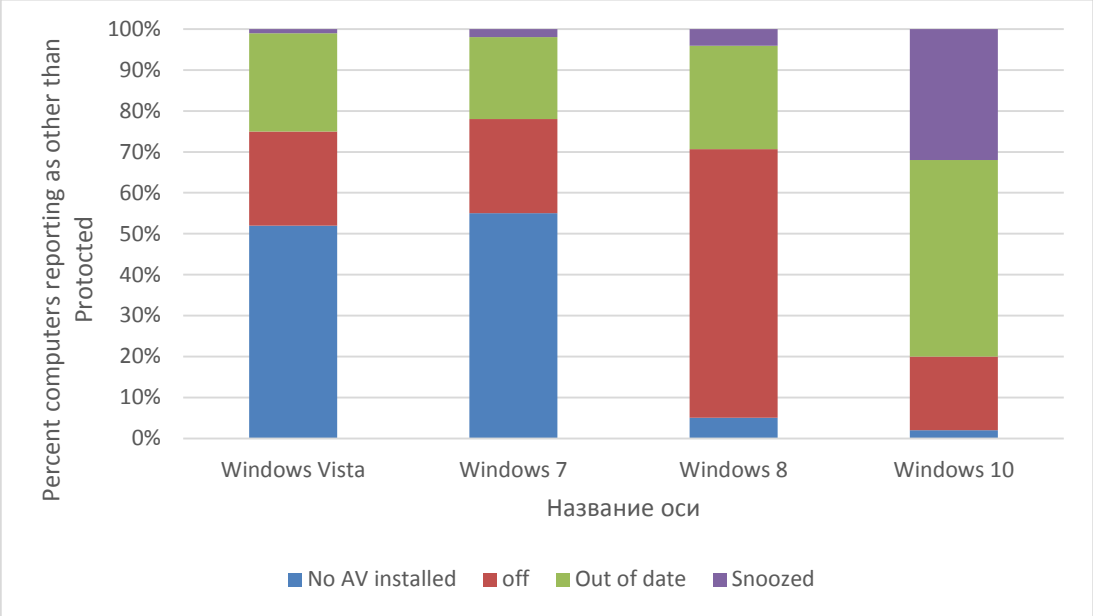

Рис. 1. Результат дослідження Microsoft Security щодо використання та активації антивірусного ПЗ

Fig. 1. The result of Microsoft Security study on the use and activation of anti-virus software

Таблиця 1

Найбільш поширені антивірусні програми

Table 1

Most advanced anti-virus programs

Антивірус	Безкоштовна версія	Ціна	Демо-доступ	Кількість пристроїв	Вбудований фаєрвол	Мультиплатформенність
Kaspersky	існує	665 ₴	30 днів	до 5	існує	існує
McAfee	немає	655 ₴	30 днів	до 10	існує	існує
Захисник Windows	існує	—	—	1	існує	немає
ESET NOD32	існує	365 ₴	30 днів	1	існує	окремі підписки на інші ОС
Bitdefender	існує	530 ₴	немає	до 5	існує	існує
Sucuri	існує	199 $	немає	1	немає	лише веб
Dr. Web	існує	400 ₴	1–3 міся-ці	1	існує	окремі підписки на інші ОС
Avast	існує	440 ₴	—	1	існує	немає
Norton Security	немає	930 ₴	30 днів	до 10	існує	існує
Avira	існує	860 ₴	немає	до 5	існує	існує

doi: https://doi.org/10.15802/stp2021/253290

Контент-аналіз публікацій щодо антивірусного програмного забезпечення доводить численність досліджуваних аспектів, зокрема щодо спроможності такого програмного забезпечення не тільки розпізнавати загрозу, але й бути здатним знищити її. Для виконання цього завдання антивірус повинен мати такі функції: регулярне (або в режимі реального часу) сканування системних файлів і програм; сканування вмісту месенджерів та електронної пошти; повне сканування комп'ютера за командою користувача; моніторинг вхідного та вихідного мережевого трафіка; усунення наслідків роботи шкідливого ПЗ. Крім того, порівняльний аналіз найбільш популярного антивірусного ПЗ дає можливість виявити недоліки та переваги кожного з них.

Наукова новизна та практична значимість

Набув подальшого розвитку системний та узагальнювальний аналіз наявного та найбільш поширеного антивірусного програмного забезпечення, що надає можливість звичайним користувачам усвідомлено роботи вибір щодо встановлення таких програмних пакетів.

На основі отриманих результатів можна коригувати власні дії щодо безпечної роботи в інтернет-мережі. Також наведена інформація допоможе зробити вибір щодо використання антивірусного ПЗ, виходячи з конкретних задач, які ставить користувач.

Висновки

Незважаючи на значне поширення антивірусних програм віруси продовжують «плодитися». Щоб впоратися з ними, необхідно створювати більш універсальні та якісно нові антивірусні програми, які міститимуть усі позитивні якості своїх попередників. На жаль, у наш час немає такої антивірусної програми, яка б гарантувала захист від усіх різновидів вірусів на 100 %. Проблема протистояння «меча і щита» це постійний процес, який із кожним роком тільки набирає обертів. Як і в будь-якій сутичці, у кожної зі сторін бувають успіхи та невдачі, проте чим більшим і небезпечним стає меч, тим більшим і міцнішим стає щит. Розвиток шкідливого ПЗ тільки стимулює розвиток антивірусного ПЗ, і навпаки.

Чутки про марність антивірусного ПЗ у світі явно перебільшені. Ефективність антивірусного ПЗ залежить від безлічі факторів, багато з яких є непередбачуваними, тому навіть найкращі антивіруси іноді не можуть заблокувати нову загрозу.

Найслабшою ланкою в ланцюжку захисту комп'ютера від шкідливого ПЗ, як і в будь-якому процесі, так чи інакше пов'язаному з автоматизацією, є людина. Навіть найбільш кваліфікований фахівець рано чи пізно робить помилки, тому наявність антивірусного програмного забезпечення на комп'ютері не є панацеєю, проте дозволяє суттєво знизити ризики.

У подальшому плануємо більш детальний огляд та порівняльний аналіз алгоритмів, на базі яких створено антивірусне програмне забезпечення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Белоус А. И., Солодуха В. А. *Кибероружие и кибербезопасность. О сложных вещах простыми словами.* Москва, Вологда : Инфра-Инженерия, 2020. 692 с.
2. Кардава Н. В. Киберпространство как новая политическая реальность : вызовы и ответы. *История и современность*. 2018. № 2. С. 152–166. DOI: https://doi.org/10.30884/iis/2018.02.03
3. Кузнецов Е., Сауров А. Аппаратные трояны. Часть 1 : новые угрозы кибербезопасности. *Наноиндустрия*. 2021. С. 16–25. DOI: https://doi.org/10.22184/1993-8578.2016.69.7.16.25
4. *Проблемы информационной безопасности в международных военно-политических отношениях* / под ред. А. В. Загорского, Н. П. Ромашкиной. Москва : ИМЕМО РАНР, 2016. 183 с. DOI: https://doi.org/10.20542/978-5-9535-0477-5
5. Сухомлин В. А., Белякова О. С., Климина А. С., Полянская М. С., Русанов А. А. *Модель цифровых навыков кибербезопасности*. Фонд Лига интернет-медиа, 2021. 294 с.

doi: https://doi.org/10.15802/stp2021/253290

6. *Antivirus software (antivirus program)*. URL: https://www.techtarget.com/searchsecurity/definition/antivirus-software
7. *Best Antivirus Software for PC in 2021*. URL: https://www.wizcase.com/best-antivirus-for-pc/gr/
8. *Data Breach Investigations Report*. 2020. Verizon. URL: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf
9. Kostogryzov A. *Probabilistic Modeling in System Engineering.* London : IntechOpen, 2018. 290 p. DOI: https://doi.org/10.5772/intechopen.71396
10. Trifonov R., Yoshinov R., Pavlova G., Tsochev G. Artificial neural network intelligent method for prediction. *AIP Conference Proceedings*. 2017. Vol. 1872. P. 1–7. DOI: https://doi.org/10.1063/1.4996678

D. S. ASTAKHOV[1*], N. O. LYSENKO[2*], V. B. MAZURENKO[3*], A. I. FEDOROVYCH[4*]

[1*]Dep. «Radio-Electronic Automation», Oles Honchar Dnipro National University, Haharina Av., 72, Dnipro, Ukraine, 49000, tel. +38 (056) 374 98 22, e-mail astakhov.ds@gmail.com, ORCID 0000-0002-8636-1776
[2*]Dep. «Radio-Electronic Automation», Oles Honchar Dnipro National University, Haharina Av., 72, Dnipro, Ukraine, 49000, tel. +38 (056) 374 98 22, e-mail LysenkoNA@ukr.net, ORCID 0000-0001-6865-6207
[3*]Dep. «Radio-Electronic Automation», Oles Honchar Dnipro National University, Haharina Av., 72, Dnipro, Ukraine, 49000, tel. +38 (056) 374 98 22, e-mail mazurenko_v@yahoo.com, ORCID 0000-0001-8340-012X
[4*]Dep. «Radio-Electronic Automation», Oles Honchar Dnipro National University, Haharina Av., 72, Dnipro, Ukraine, 49000, tel. +38 (056) 374 98 22, e-mail sonya.soolovskaya@gmail.com, ORCID 0000-0003-0752-7190

Analysis of Modern Anti-Virus Software in Cyber Security Tasks

Purpose. The research is aimed at gaining general knowledge about modern anti-virus software. Because it is one aspect of cybersecurity, and is subject to ongoing discussions about its appropriateness. **Methodology**. To obtain data, the authors conducted a review of world literature on the topic of work using full-text and abstract databases. Signature and heuristic methods of antivirus software operation are considered. As well as the conditional division of these products into programs-detectors, programs-doctors, programs-auditors, programs-filters, programs-immunizers was made. **Findings.** Content analysis of publications in the direction of anti-virus software proves the number of aspects studied. The question of the ability of such software not only to recognize the threat, but also to be able to destroy it is being studied. To perform this task, the antivirus must have the following functions: regular (or real-time) scanning of system files and programs; scanning the content of messengers and e-mail; full computer scan at the user's command; monitoring of incoming and outgoing network traffic; elimination of the malware operation consequences. In addition, a comparative analysis of the most popular anti-virus software makes it possible to identify the disadvantages and advantages of each of them. **Originality**. Systematic and generalized analysis of the existing and most common anti-virus software has been further developed, which allows ordinary users to make informed choices about installing such software packages. **Practical value.** Based on the results obtained, it is possible to adjust your own actions regarding safe work on the Internet. In addition, the article aims to dispel myths suggesting that users do not protect their computers from malware at all. These studies can also be useful in studying the discipline "Fundamentals of Software Testing", the organization of scientific and practical seminars, refresher courses and etc.

Keywords: software; information threat; antivirus; singular method; heuristic method

REFERENCES

1. Belous, A. I., & Solodukha, V. A. (2020). *Kiberoruzhie i kiberbezopasnost. O slozhnykh veshchakh prostymi slovami*. Moscow, Vologda: Infra-Inzheneriya. (in Russian)
2. Kardava, N. V. (2018). Kiberprostranstvo kak novaya politicheskaya realnost: vyzovy i otvety. *History and Present, 2*, 152-166. DOI: https://doi.org/10.30884/iis/2018.02.03 (in Russian)
3. Kuznetsov, E., & Saurov, A. (2016). Hardware Trojans. Part 1: new threats to cyber security. *Nanoindustry Russia, 7*, 16-25. DOI: https://doi.org/10.22184/1993-8578.2016.69.7.16.25 (in Russian)
4. Zagorskii, A. V., & Romashkina, N. P. (Eds.). (2016). *Informational Security Problems in Modern International Crises and Conflicts of XXI century*. Moscow: IMEMO RAN. DOI: https://doi.org/10.20542/978-5-9535-0477-5 (in Russian)

doi: https://doi.org/10.15802/stp2021/253290

5. Sukhomlin, V. A., Belyakova, O. S., Klimina, A. S., Polyanskaya, M. S., & Rusanov, A. A. *Model tsifrovykh navykov kiberbezopasnosti*. Fond Liga internet-media. (in Russian)
6. *Antivirus software (antivirus program)*. Retrieved from https://www.techtarget.com/searchsecurity/definition/antivirus-software (in English)
7. *Best Antivirus Software for PC in 2021*. Retrieved from https://www.wizcase.com/best-antivirus-for-pc/gr/ (in English)
8. *Data Breach Investigations Report.*(2020). Verizon. Retrieved from https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf (in English)
9. Kostogryzov, A. (Ed.). (2018). *Probabilistic Modeling in System Engineering.* IntechOpen. DOI: https://doi.org/10.5772/intechopen.71396 (in English)
10. Trifonov, R., Yoshinov, R., Pavlova, G., & Tsochev, G. (2017). Artificial neural network intelligent method for prediction. In *AIP Conference Proceedings* (Vol. 1872, pp. 1-7). DOI: https://doi.org/10.1063/1.4996678 (in English)

Надійшла до редколегії: 31.05.2021
Прийнята до друку: 01.10.2021

doi: https://doi.org/10.15802/stp2021/253290