УДК 005.53:004.492

# СТРУКТУРНА МОДЕЛЬ ВИБОРУ АНТИВІРУСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

***Жданюк М.С., Ільге І.Г.***

***Харківський національний автомобільно-дорожній університет, Харків***

Оскільки антивірус є складним програмним продуктом, його оцінювання і вибір неможливе без комплексного підходу та розгляду з різних технічних і функціональних позицій і визначення критеріїв.

У першу чергу зупинимося на групі критеріїв, що визначають якість базового захисту.

Насамперед, ключовим показником ефективності будь-якої антивірусної системи є її здатність своєчасно виявляти потенційно небезпечні об’єкти та успішно запобігати шкідливим діям з їхнього боку. Високий рівень детекції є основою захисту, адже саме він визначає, наскільки якісно програма реагує на широкий спектр загроз.

Другим важливим фактором виступає стан і регулярність оновлення вірусних баз. Сучасні шкідливі програми швидко модифікуються, тому антивірус повинен оперативно отримувати нові сигнатури та відомості про актуальні загрози. Недостатня актуальність баз може значно знизити рівень безпеки навіть при ефективних алгоритмах.

По-третє, у процесі роботи антивірусу часто використовуються евристичні методи для виявлення нових або модифікованих вірусів. Хоча ці алгоритми підвищують можливості захисту, вони можуть призводити до появи хибних спрацювань. Тому доцільно враховувати, чи містить продукт інструменти для коректної обробки таких ситуацій, щоб уникнути затримок у роботі системи та надмірного навантаження на користувача.

Четвертий критерій пов’язаний із вимогами антивірусного ПЗ до апаратних ресурсів комп’ютера. Швидкодія процесора, доступний обсяг оперативної пам’яті та інші характеристики безпосередньо впливають на

продуктивність програми. Особливо важливо це для навчальних закладів, де техніка може бути застарілою або мати обмежені характеристики. Перевищення вимог антивірусу щодо ресурсів може зробити його використання неможливим або неефективним.

П’ятим критерієм першої групи виступає загальна продуктивність антивірусу. Програма має працювати у фоновому режимі, не заважаючи користувачу, але при цьому забезпечувати моніторинг системи в реальному часі. Якщо алгоритми аналізу загроз є недостатньо оптимізованими або повільними, антивірус не зможе оперативно реагувати на нові атаки, що значно знижує рівень безпеки.

Друга група критеріїв стосується захисту в мережевому середовищі, оскільки саме Інтернет сьогодні є основним джерелом надходження потенційно небезпечних даних. Першим елементом протидії мережевим атакам є брандмауер. Багато сучасних антивірусних продуктів мають власні інтегровані брандмауери, часто з елементами інтелектуальних алгоритмів чи модулів, побудованих на нейронних мережах. Від їхньої ефективності залежить здатність системи контролювати вхідні та вихідні з’єднання.

Під час перегляду веб-ресурсів користувач може випадково потрапити на шкідливі сайти, що використовують вразливості браузера для прихованого встановлення небезпечного ПЗ. Це особливо актуально в навчальних умовах, коли студенти не завжди здатні самостійно оцінити безпечність інтернет-ресурсів. Тому повнота і якість веб-захисту є значущим критерієм вибору антивірусу.

Наступним критерієм у межах мережевої функціональності є наявність та якість VPN-сервісів. Захищений VPN-канал дозволяє шифрувати трафік та приховувати реальну IP-адресу користувача, що знижує ризик перехоплення даних та несанкціонованого стеження.

Ще один аспект мережевої безпеки пов'язаний із захистом веб-камери. Хакери часто намагаються отримати доступ до неї для стеження або збору конфіденційної інформації. Наявність механізмів, які повідомляють про

спроби активації камери та дозволяють блокувати їх, є важливою перевагою антивірусу.

Третя група критеріїв охоплює властивості, пов’язані зі зручністю користування. Першочергове значення має інтерфейс: він повинен бути інтуїтивно зрозумілим і не вимагати спеціальних технічних знань, особливо в умовах навчального процесу. Чим простіше користувачу орієнтуватися в налаштуваннях і функціях програми, тим ефективніше вона буде використовуватися.

Важливим є також питання адаптивності антивірусного ПЗ. Воно повинно мати кілька режимів роботи, легко перемикатися між ними та зберігати стабільність при різних рівнях навантаження системи. Не менш вагомим критерієм є доступність технічної підтримки, яка дозволяє швидко реагувати на проблеми в роботі програми.

Ще один критерій третьої групи — можливість створення резервних копій даних. Оскільки цей процес є звичною практикою, а в навчальних установах студенти можуть мати недостатній досвід у роботі з інформацією, наявність вбудованих функцій резервування та певного обсягу хмарного сховища суттєво підвищує рівень захищеності даних.

Четверта група критеріїв охоплює економічні аспекти вибору антивірусу, що є особливо важливим у сучасних умовах обмеженого фінансування навчальних закладів. Одним з ключових моментів є доступність безкоштовної або ознайомчої (trial) версії. Вона дозволяє оцінити можливості продукту без додаткових витрат і забезпечити мінімально необхідний рівень захисту.

Ще одним фінансовим показником є вартість річної підписки. Вона може суттєво відрізнятися залежно від виробника, тому цей параметр варто ретельно порівнювати, особливо при закупівлі програмного забезпечення для великої кількості комп’ютерів.

На завершення до економічних критеріїв доцільно віднести політику повернення коштів. Наявність гарантії відшкодування вартості у випадку,

коли антивірус не відповідає потребам користувача, забезпечує додаткову гнучкість при виборі програмного продукту.

П’ята група критеріїв: інтеграційні та технологічні можливості антивірусного ПЗ.

Ця група охоплює властивості антивірусу, що визначають його здатність працювати в сучасній інфраструктурі та адаптуватися до нових технологій.

По-перше, важлива сумісність із різними ОС та платформами - Windows, Linux, macOS, а також мобільними системами. Чим ширша підтримка, тим простіше забезпечити єдиний рівень захисту в різнорідному середовищі.

Другий критерій - інтеграція з іншими системами безпеки й централізованими інструментами керування (Active Directory, MDM, брандмауери), що дозволяє керувати політиками та налаштуваннями з єдиного центру.

Третій критерій - використання хмарних технологій для швидкої реакції на нові загрози. Тут важливо враховувати й рівень захисту даних, що передаються у хмару.

Четверте - розширюваність продукту, можливість підключення додаткових модулів (антиспам, контроль пристроїв, аналізатор вразливостей тощо), що дозволяє гнучко адаптувати ПЗ під потреби користувачів.

П’ятим критерієм є застосування алгоритмів ШІ та машинного навчання, які підвищують ефективність виявлення складних і нових загроз.

Шостий критерій - регулярність і тривалість підтримки: своєчасні оновлення баз і компонентів визначають довгострокову надійність продукту.

І нарешті, потрібно враховувати стабільність роботи антивірусу та рівень його втручання в систему, щоб уникнути конфліктів із програмами та збоїв.

Зазначена група критеріїв дозволяє комплексно оцінити технологічну зрілість антивірусного ПЗ та його придатність до використання в умовах сучасної інфраструктури, де важливі не лише базові механізми захисту, а й можливість гнучкої інтеграції та масштабування.

Таким чином, можна побудувати ієрархічну модель вибору антивірусного програмного забезпечення у вигляді нумерованого переліку.

1. Мета - вибір оптимального антивірусного програмного забезпечення.

2. Групи критеріїв.

2.1. Критерії базового захисту.

2.2. Критерії мережевої безпеки.

2.3. Користувацькі критерії.

2.4. Вартісні критерії.

2.5. Інтеграційні та технологічні критерії.

3. Критерії всередині кожної групи.

3.1. Критерії базового захисту.

3.1.1. Рівень виявлення та нейтралізації загроз.

3.1.2. Актуальність і частота оновлення вірусних баз.

3.1.3. Стійкість евристичного аналізу та обробка хибних спрацювань.

3.1.4. Вимоги до ресурсів ПК.

3.1.5. Продуктивність у режимі реального часу.

3.2. Критерії мережевої безпеки.

3.2.1. Якість та функціональність брандмауера.

3.2.2. Захист від небезпечних веб-сайтів.

3.2.3. Наявність та якість VPN.

3.2.4. Захист веб-камери.

3.3. Користувацькі критерії.

3.3.1. Зручність інтерфейсу і простота використання.

3.3.2. Адаптивність до різних режимів роботи.

3.3.3. Наявність технічної підтримки.

3.3.4. Функції резервного копіювання та доступний простір зберігання.

3.4. Вартісні критерії.

3.4.1. Наявність безкоштовної або trial-версії.

3.4.2. Вартість річної підписки.

3.4.3. Гарантія повернення коштів.

3.5. Інтеграційні та технологічні критерії.

3.5.1. Сумісність із різними ОС та платформами.

3.5.2. Інтеграція з іншими системами безпеки.

3.5.3. Використання хмарних технологій.

3.5.4. Розширюваність та додаткові модулі.

3.5.5. Застосування AI/ML для аналізу загроз.

3.5.6. Регулярність оновлення та тривалість підтримки.

3.5.7. Стабільність роботи та мінімізація втручання в систему.

4. Альтернативи.

Розроблена структурна ієрархічна модель вибору антивірусного програмного забезпечення після визначення користувачем актуальних альтернатив може бути безпосередньо використана для побудови матриць попарних порівнянь і подальшої реалізації класичної процедури методу аналізу ієрархій [1].

Список літератури:

1. Saaty T. L. The Analytic Hierarchy Process: what is it and how it is used // Mathematical Modeling. – 1987. – Vol. 9.