УДК 004.49
DOI: 10.31673/2409-7292.2023.010002

Скибун О. Ж.

РОЛЬ АНТИВІРУСНОГО ЗАХИСТУ У ФОРМУВАННІ ЕКОСИСТЕМИ ТА ІМУННОЇ СИСТЕМИ КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

У статті розглянуто необхідність формування екосистеми, інформаційної корпоративної системи із сильною імунною системою, яка разом із антивірусним захистом забезпечує достатній рівень кіберзахисту усієї системи для можливості сталого та стійкого функціонування великих корпоративних інформаційних систем. Також відзначено необхідність врахування того, що сучасні корпоративні інформаційні системи формуються на базі нейронних систем, штучного інтелекту та Інтернету речей. Вказане обумовлює необхідність комплексного підходу до вибору антивірусного програмного продукту, який повинен гармонійно інтегровуватися у загальну архітектуру інформаційної системи для забезпечення високого рівня антивірусного захисту. Аналіз наявних антивірусних програмних продуктів показав, що їх переважна більшість є ефективною для домашнього використання. Для корпоративних інформаційних систем необхідно вибирати антивірусний продукт за рекомендацією та технічною підтримкою компанії-вендора, яка є відповідальною за увесь програмний продукт, що використовується в системі, що будується.

Ключові слова: інформаційні системи, нейронна система, кіберпростір, кібербезпека, кіберзахист, антивірусний програмний продукт, імунна система кіберзахисту, екосистема кіберзахисту.

Вступ

Сучасний етап розвитку суспільства характеризується широким впровадженням у комерційне користування результатів цифрової та промислової революцій, коли технології, техніка та процеси постійно ускладнюються. В першу чергу, вказане впливає на інформаційні та комунікативні процеси, адже розвиток міжнародних електронних комунікацій та глобальної мережі передачі даних разом із здешевленням кінцевого обладнання для споживачів і вартості підключення до електронних комунікаційних мереж дають можливість для включення у глобальні комунікаційні процеси значної кількості населення.

На сьогодні важливими показниками, які впливають на інформаційні процеси (отримання, передавання, оброблення, зберігання та захист інформації) є швидкість передачі даних та ємність для зберігання інформації. Лавиноподібне збільшення обсягів інформації, які щорічно збільшуються у геометричній пропорції вимагають, окрім потужних систем зберігання, відповідних систем та мереж для роботи (збору, обробки, зберігання, захисту) з інформацією, величезними масивами даних, з якими все важче справлятися людині, оскільки її фізичних можливостей стає недостатньо, «інформаційні технології потребують необхідності включення в них елементів генетичної інженерії, яка стосується декодування та можливого перепрограмування кодів інформації, що містяться в живому» [11]. А тому все частіше починають використовуватися можливості штучного інтелекту, Інтернету речей, робототехніки, надпотужних обчислювальних машин для побудови штучних нейронних мереж та систем («принципово нові інформаційні технології та системи, що можуть опрацьовувати інформацію у великих об’ємах, а застосування паралельних обчислень значно скорочує час на отримання інформації нової якості» [5, с.3]). Саме цьому «нейроні мережі можна розглядати як сучасні обчислювальні системи, що перетворять інформацію з образа процесів, що відбуваються в мозку людини» при цьому «оброблювана інформація має числовий характер, що дозволяє використовувати нейрону мережа, наприклад, як модель об'єкта з зовсім невідомими характеристиками», а «інші типові додатки нейронних мереж охоплюють задачі розпізнавання, класифікації, аналізу і стиску образів» [5, с.2].

Таким чином, такі нейронні системи все більше потребують відповідної імунної системи для захисту та відповідної екосистеми для ефективного функціонування, адже сучасні інформаційні системи функціонують як окремий складний організм. А тому «основною перевагою застосування штучних нейронних мереж є можливість розв’язувати різні неформалізовані задачі», коли «використання таких мереж для аналізу даних доцільне, оскільки ці мережі здатні до апроксимації функцій, до навчання та вдосконалення власної

структури, забезпечують низьку ймовірність помилки за умов коректного початкового налаштування параметрів мережі, а також можливості аналізу навіть за наявності неповних і зашумлених даних», що дає змогу «досить просто моделювати ситуації, подаючи на вхід мережі дані та оцінюючи результат, який вона видає» оскільки «вказаний вище алгоритм розв'язання поставленого завдання достатньо повно описує процес виконання необхідного аналізу. [5, с.18-19].

Аналіз останніх публікацій показав, що дослідженнями побудови сучасних корпоративних інформаційних систем на основі нейронних мереж, а також формуванням відповідної екосистеми та імунної системи для сталого та стійкого функціонування в умовах впливу шкідливого програмного забезпечення займалися як зарубіжні, так і вітчизняні науковці, серед яких можна відзначити: Г. Гайдур, С. Гахов, О. Винявський, М. Кастельс, В. Коцовський, О. Куц, Д. Рагузео тощо.

Незважаючи на досить широкий спектр проведених досліджень, питання ролі антивірусного захисту у формуванні сталої та стійкої екосистеми та здорової імунні системи корпоративних інформаційних систем, **виступає частиною загальної проблеми,** котрій присвячується означена стаття.

Формулювання завдань (мети) статті. Метою статті є розгляд питань формування сучасних корпоративних систем на базі нейронних мереж разом із екосистемою та імунною системою з високим рівнем сталості та стійкості до впливу вірусів та іншого шкіливого програмного забезпечення.

Методи дослідження, використані у процесі написання статті, передбачають застосування загальнонаукових та емпіричних прийомів, що ґрунтуються на системному підході. Крім цього, у процесі роботи застосовувались такі загальні методи досліджень, як узагальнення та порівняння. В результаті проведеного аналізу дискурсу сучасних питань етики та моралі у контексті практичної філософії кібербезпеки було сформовано практичні рекомендації щодо подальшого формування професійної та корпоративної етики у сфері кіберзахисту.

Виклад основного матеріалу

С. Гахов відзначає, що «корпоративну інформаційну систему необхідно розглядати як цілісну систему – окрему сутність в кіберпросторі, яка повинна виконувати функції за призначенням та проявляти властивості функціональної стійкості в умовах деструктивних кібернетичних впливів» [3, с.60]. А для нормального стабільного функціонування сучасної інформаційної системи відповідним чином повинна формуватися відповідна екосистема для врівноваження та балансу, як зовнішніх, так і внутрішніх чинників впливу на її функціонування («здоров'я організму» нейронної системи) адже «інформаційна екосистема – це система, що складається з людини, інформації, інформаційного середовища та інформаційних технологій», де «принципи екології використовуються для підкреслення взаємозалежності інформаційного середовища з усіма компонентами екосистеми» [6, с.43]. По аналогії із природою у кіберпросторі є хворобливі віруси, які також впливають на функціонування інформаційної системи («організму»), здоров'я якої (якого) залежить насамперед від наявної імунної системи. А від цього залежить і гарантованість безпеки.

Так, Г. Гайдур відзначає, що «гарантованість безпеки – міра довіри, яка може бути надана архітектурі, інфраструктурі, програмно-апаратної реалізації системи і методів управління її конфігурацією і цілісністю» при цьому «гарантованість показує, наскільки коректні механізми, що відповідають за проведення в життя політики безпеки», а тому «гарантованість є пасивним, але дуже важливим компонентом захисту, реалізованим якістю розробки, впровадження, експлуатації і супроводу інформаційної системи і закладених принципів безпеки» [2, с.18].

Відповідно до стандарту ISO 2382-1 «інформаційна система (ІС)» визначається як «система обробки інформації, що працює спільно з організаційними ресурсами, такими як

© Скибун, О. Ж. (2023). Роль антивірусного захисту у формуванні екосистеми та імунної системи корпоративних інформаційних систем. Сучасний захист інформації, 1(53), 12–23. https://doi.org/10.31673/2409-7292.2023.010002.

люди, технічні засоби та фінансові ресурси, які забезпечують і розподіляють інформацію» адже ІС визначається як «сукупність апаратно-програмних та організаційних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів», де «основним завданням ІС є забезпечення конкретних інформаційних потреб у межах певної предметної області», а оскільки «переважна більшість сучасних ІС включають до свого складу бази даних та СУБД», то «на практиці часто синонімом до терміну ІС є термін «система баз даних». [5]. При цьому інформація може класифікуватися, серед іншого, таким чином (рис. 1):

Рис. 1. Класифікація інформації [8]

Сучасною тенденцією є те, що разом із подальшою цифровізацією інформації та інформаційних процесів «все більше конфіденційної інформації зберігається і обробляється в різних інформаційних системах (ІС)» [5]. При цьому необхідно зважати, що це в свою чергу, сприяє збільшенню рівня уразливостей ІС, «які обумовлюють можливість реалізації загроз оброблюваної в ній інформації» при цьому «процес управління уразливостями включає виявлення, класифікацію, оцінку і усунення уразливостей» [5].

На сьогодні ІС величезних транснаціональних корпорацій являють собою складну архітектуру, величезний масив програмованого обладнання, програмного забезпечення та інформації, яка циркулює в цих ІС як для внутрішнього (корпоративного використання), так і у вигляді відкритих даних. При цьому «підхід до забезпечення кібербезпеки корпоративних інформаційних систем, заснований на застосуванні комплексів різноманітних, фрагментованих, точкових, відокремлено функціонуючих компонентів захисту, збільшує інфраструктуру, ускладнює роботу фахівців, не призводить до суттєвого поліпшення стану та гарантій кібербезпеки» [3, с.59] для кібербезпеки ІС. А тому все частіше провідними виробниками рішень в сфері кібербезпеки починають пропонуватися рішення з елементами «інтегрованої та інтелектуальної імунної системи безпеки» (integrated and intelligent security immune system), побудовані на основі «комплексного та цілісного підходу, заснованого на когнітивному ядрі організаційної та аналітичної безпеки, яке розуміє, пояснює і впізнає множину змінних ризику у всій екосистемі пов’язаних можливостей» [13].

Наприклад «імунна система IBM Security – це інтегрований і цілісний підхід, зосереджений навколо когнітивного ядра оркестровки й аналітики безпеки, яке розуміє, обґрунтовує та вивчає численні змінні ризику в усій екосистемі підключених можливостей» і «як тільки імунна система IBM Security залучиться до всієї вашої екосистеми, дозволяючи співпрацю між сторонніми постачальниками, постачальниками технологій і бізнес-партнерами, вона може надати вам інформацію, необхідну для розуміння існуючих загроз і адаптації до нових» [18]. Для цього все частіше використовуються різні види нейронних мереж, які в свою чергу потребують власної екосистеми та сильної імунної системи для

сталості та стійкості функціонування ІС в умовах зростаючого рівня кіберзагроз та уразливостей як зовнішнього, так і внутрішнього характеру.

Як відзначає D. Raguseo «IBM розглядає кіберзахист як імунну систему безпеки, яка залежить не від одного рішення, а від інтегрованого набору додаткових елементів керування для захисту даних» [16] в ІС, а у загальному вигляді структура імунної системи IBM Security представлена на рис. 2.

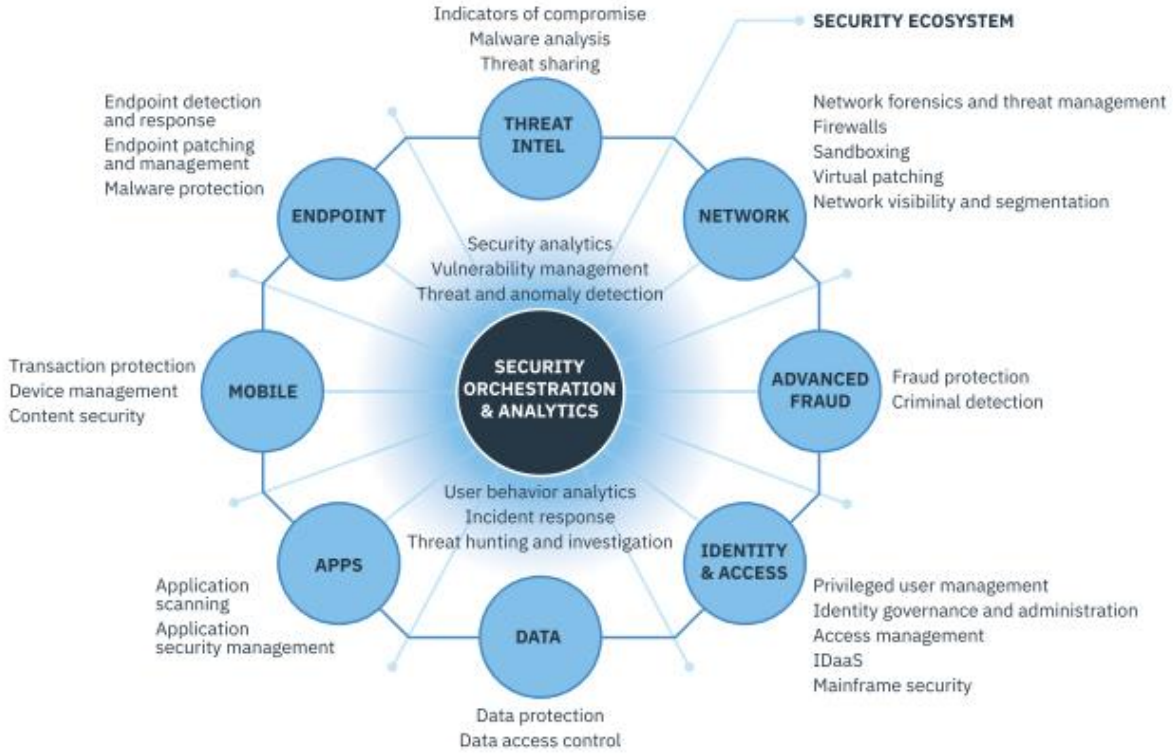

Рис. 2. Імунна система IBM Security [16]

В свою чергу С. Гахов наголошує на тому, що «при вирішенні проблеми забезпечення кібербезпеки на передній план виходять не цілі забезпечення прояву властивостей інформації, яка захищається, а цілі забезпечення безпеки процесів функціонування інформаційних систем», а тому «необхідно забезпечувати функціонування корпоративної інформаційної системи в умовах кібернетичних впливів таким чином, щоб у ній виникали тільки ті процеси (функціональні системи), які відповідають цілям створення даної системи» [3, с.60]. Це можливо лише за умови побудови стабільної екосистеми ІС та сформованої потужної імунної системи для ІС (в цілому та окремих її складових). При цьому «ефективна імунна система безпеки має бути плавною, гнучкою та раціональною», а найголовніше вона повинна «мати можливість розвиватися у відповідь на зміни у все більш нестабільному ландшафті загроз» [16].

Таким чином, «сучасні підходи до забезпечення кібернетичної безпеки корпоративних інформаційних систем базуються на функціональних системах, які виникають у середовищі «людина – SIEM-система – компоненти та процеси інформаційної системи», де «в основі механізму інтелектуальної обробки даних сучасних SIEM-систем лежить контекстна, поведінкова і часова аналітика» [3, с.60]. При цьому необхідно враховувати забезпечення «гарантованості» безперебійного сталого функціонування ІС та високої стійкості до кіберзагроз. А цього, за словами Г. Гайдур, можна досягти за умови наявності відповідної «концепції гарантованості» для ІС, де «концепція гарантованості є центральною при оцінці ступеня захисту, з якою інформаційну систему можна вважати надійною», коли «надійність

© Скибун, О. Ж. (2023). Роль антивірусного захисту у формуванні екосистеми та імунної системи корпоративних інформаційних систем. Сучасний захист інформації, 1(53), 12–23. https://doi.org/10.31673/2409-7292.2023.010002.

забезпечується всією сукупністю захисних механізмів системи в цілому і надійністю обчислювальної бази (ядра системи), що відповідають за проведення в життя політики безпеки», а сама «надійність обчислювальної бази визначається її реалізацією і коректністю вихідних даних, що вводяться адміністративним та операційним персоналом», при цьому слід враховувати, що «компоненти обчислювальної бази не можуть бути абсолютно надійними, однак це не повинно впливати на безпеку системи в цілому» [2, с.19-20]. Отже, тільки комплексний підхід до побудови ефективної системи кіберзахисту дасть позитивний ефект. При цьому чим складніша ІС (з елементами штучного інтелекту та нейронних мереж), тим більшою стає потреба у створенні кібернетичної екосистеми із сильною імунною системою. Нижче на рис. 3 наведено структуру екосистеми інформаційної та кібернетичної безпеки [4].

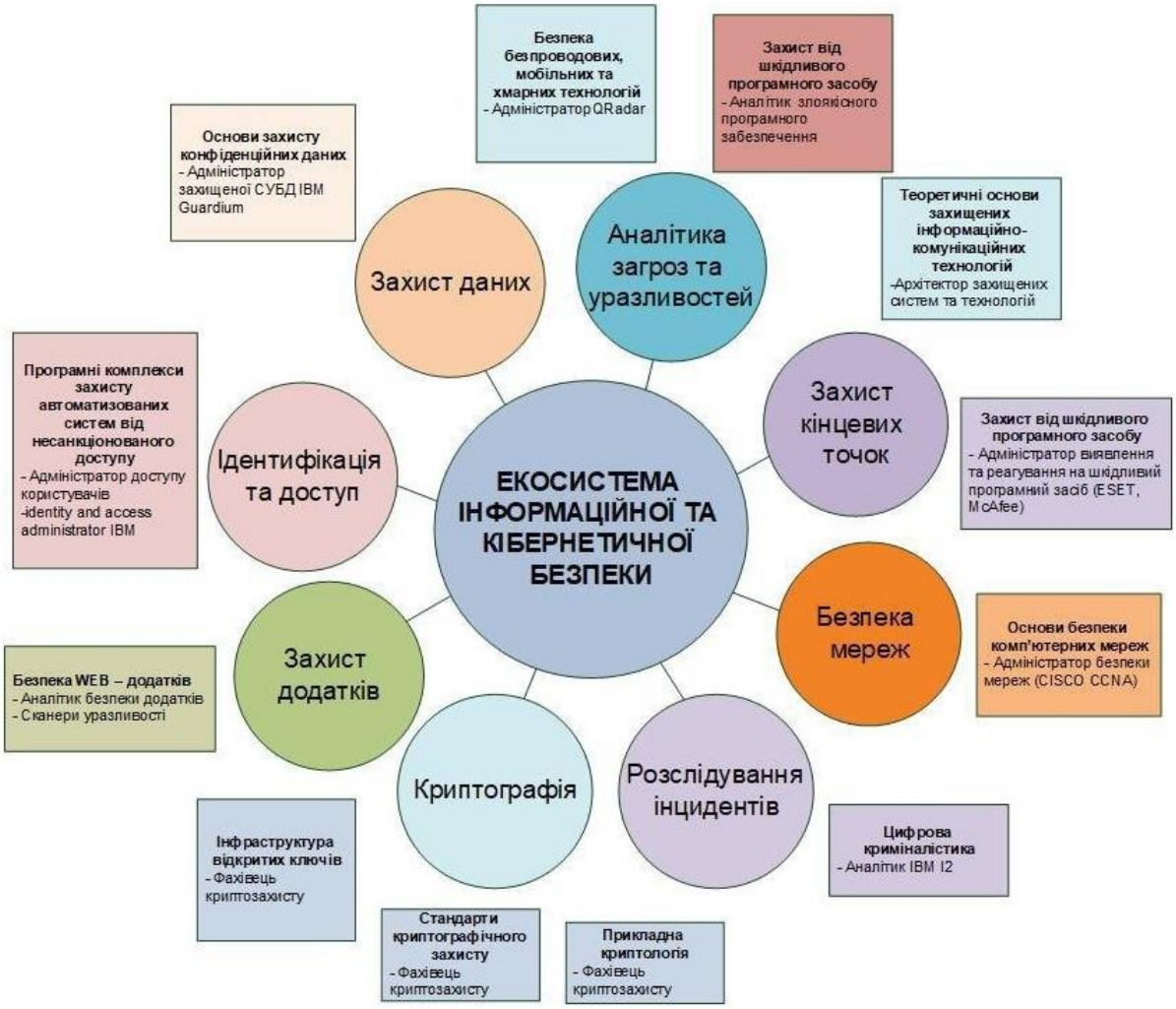

Рис. 3. Екосистема інформаційної та кібернетичної безпеки [4].

При цьому необхідно розуміти, що «мережна безпека – це еволюційний процес» бо «немає жодного продукту, здатного надати корпорації повну безпеку» оскільки «надійний захист мережі досягається поєднанням продуктів і послуг, а також грамотною політикою безпеки і її дотриманням усіма співробітниками від верху до низу», тому наявність правильної «політики безпеки навіть без ресурсів, які виділяються на захисту без наявної політики та системності дій, … дає кращі результати, ніж засоби захисту без політики безпеки» [5].

Це пов’язане з тим, що сучасні ІС вимагають комплексного підходу до формування високорівневої адаптивної системи кіберзахисту. Адже питання визначення ризиків від загроз є актуальним для приватного та державного секторів. Для обрахунку ризиків положеннями

© Скибун, О. Ж. (2023). Роль антивірусного захисту у формуванні екосистеми та імунної системи корпоративних інформаційних систем. Сучасний захист інформації, 1(53), 12–23. https://doi.org/10.31673/2409-7292.2023.010002.

стандарту ISO / IEC 27005 запропоновано наступну формулу розрахунку ризику, універсальною «для всіх типів об'єктів захисту, до яких можуть належати інформаційні активи, програмне забезпечення, технічні засоби тощо», коли «на рівні ІС відбувається ідентифікація інформаційних активів, уразливостей і загроз», а також «засобів і заходів захисту, що застосовуються і коли «цієї інформації достатньо для визначення ймовірності виникнення збитків» [5]

$$R = \sum_{j=1}^{n} P_r^j \cdot I^j,$$

де P_r^j – ймовірність реалізації j-й загрози,

I^j – значення збитку від реалізації j-й загрози,

n – число загроз.

Як відзначають фахівці з кібербезпеки IBM, «коли справа доходить до загроз кібербезпеці, ніхто не застрахований, а традиційна стратегія захисту, яка полягає в тому, щоб додати ще один інструмент або технологію точкового продукту до вже фрагментованого та роз'єднаного IT-середовища не дає необхідного ефекту, виникає запит на новий продукт, який би вирішував питання кіберзахисту комплексно, систематично, автоматично та умів налаштовуватися та адаптовуватися до змін» [18]. Зважаючи на сказане, IBM розробила «інтегровану інтелектуальну імунну систему безпеки, філософія якої полягає у застосуванні кібернетичної високоадаптивної імунної системи кіберзахисту, яка дозволяє миттєво розпізнати загарбника (кіберзагрозу) та вжити заходів, щоб заблокувати його вхід до ІС або знищити його» при цьому «імунна система IBM Security розглядає портфоліо безпеки організовано – як інтегровану структуру можливостей безпеки, яка передає та отримує життєво важливі дані безпеки, щоб допомогти отримати видимість, зрозуміти та визначити пріоритети загроз, а також координувати кілька рівнів захисту» бо «за своєю суттю система використовує оркестрування безпеки й аналітику для автоматизації політик і блокування загроз – так само, як імунна система людини може оцінити й ідентифікувати вірус, наприклад, і викликати імунну відповідь» [18]. У свою чергу D. Raguseo пропонує нашій увазі певні рекомендації щодо практичного спрямування теоретичних напрацювань, які можна сформулювати таким чином»:

– Якщо резервне копіювання даних створюється, потреба платити за їх безпечне повернення зменшується у випадку атаки програм-вимагачів, наприклад WannaCry. Те саме стосується уразливостей – хоча дуже важливо застосувати патч якомога швидше, він не завжди доступний одразу, а резервне копіювання систем і даних є єдиним способом захисту від викупу та простоїв, які можуть бути пов'язані з невиправленими недоліками.

– Запобігання та виявлення інцидентів безпеки є важливими заходами, але ефективність наявної програми безпеки залежить від можливостей реагування на інциденти, а зусилля з відновлення мають бути потужними та відповідати всім чинним нормам.

– Хоча вони зазвичай не класифікуються як такі, фізичні події або події, що спостерігаються за допомогою неструктурованих даних, іноді можуть сповіщати адміністраторів про інцидент безпеки.

– Адміністратори керування мобільними пристроями рідко бувають сильними експертами з безпеки і чим більше даних про загрози матимуть у своєму розпорядженні ці професіонали, тим ефективніше вони зможуть усувати потенційні вразливості.

– Дуже важливо застосувати елементи керування безпекою до всіх даних, інтегрованих у рішення безпеки та управління подіями (SIEM) бо таким чином аналітики можуть придушити загрози в зародку, перш ніж вони пошкодять мережу» [16].

© Скибун, О. Ж. (2023). Роль антивірусного захисту у формуванні екосистеми та імунної системи корпоративних інформаційних систем. Сучасний захист інформації, 1(53), 12–23. https://doi.org/10.31673/2409-7292.2023.010002.

Вказані практичні рекомендації є слушними і заслуговують на увагу, особливо в сучасних умовах подальшого збільшення ролі корпоративних ІС в умовах соціального та/або комерційного застосування, обсягів відкритих даних та можливостей доступу до них і подальшого використання. Але разом з цим зростає і кількість та якість кіберзагроз, коли різноманітні віруси (шкідливе програмне забезпечення) знаходить уразливі місця імунної системи кіберзахисту ІС та впливає на функціонування самої ІС, цілісність інформації та даних, що циркулюють в цій ІС. Як і в природі/людському організмі на допомогу приходять антивіруси, які допомагають імунній системі ІС боротися із вірусами, адже «антивірусна програма призначена для захисту персональних комп'ютерів від різних шкідливих програм, здатних красти і пошкоджувати інформацію, яка розміщена на жорстких дисках» [7]. При цьому «основою будь-якого антивірусного продукту є певний метод розпізнавання шкідливого програмного забезпечення, наприклад, сканування, моніторинг тощо» [7].

Слід відзначити, що «робота антивірусної програми ґрунтується на двох складових – проактивного захисту і сигнатурного захисту», коли «проактивний захист відстежує програми, файли і процеси» і «якщо виявлено, що будь-яка програма або файл поводиться підозріло, користувачеві буде запропоновано заблокувати процес, який нестандартно працює», а «робота ж сигнатурного захисту полягає в скануванні даних і порівнянні їх з існуючими в антивірусних базах сигнатурами (зразками вірусів)» [7]. Так, попит на антивірусні програмні продукти зростає разом із збільшенням рівня комп’ютеризації, цифровізації та віртуалізації суспільства в цілому та переорієнтації бізнесу на е-сектор. На сьогодні на ринку представлено значну кількість антивірусного програмного забезпечення, а тому виникає потреба у виборі оптимального варіанту. У зв’язку з цим було взято п’ять продуктів різних виробників та зведено у порівняльну таблицю 1 їх можливості для можливості проведення аналізу та вибір оптимального варіанту.

Таблиця 1

Порівняння можливостей антивірусних програм [9, 10, 12, 14].

Avast Free Antivirus, версія 22.2.6003	ESET Internet Security	ESET Endpoint Protection	Avira Free Antivirus, версія 15.0.2201.2134	Comodo Internet Security, версія 12.2.4.8032 Final
1	2	3	4	5
Блокування вірусів та іншого шкідливого ПЗ: Виявлення вірусів, програм-вимагачів та інших загроз у реальному часі.	Антивірусний захист, Антишпигун, Антифішинг	Захист робочих станцій	Блокування шкідливого ПЗ та уражених сайтів	Антивірус: відслідковує та знищує любий наявний малвер, який схований в ПК
Пошук слабких місць у захисті мережі Wi-Fi: Пошук втручань у мережу й слабких місць у системі її захисту.	Захист від програм-вимагачів	Повнодискове шифрування	Генерація унікальних та надійних паролів	Anti-spyware: виявляє та знижує програми-шпигуни
Додатковий рівень захисту від програм-вимагачів: Захист особистих фотографій і файлів від шифрування зловмисниками.	Розширене машинне навчання	Захист файлових серверів	Сканування домашньої мережі на наявність уразливостей	Anti-rootkit: сканує, знаходить та знищує руткіти в комп’ютері
Уникнення підроблених сайтів для безпечніших покупок в Інтернеті: Захист від намагань злочинців перехопити ваші паролі та банківські дані.	Захист від атак на основі скриптів	Сервіси з виявлення та реагування	Настройка 200 параметрів конфіденційності	Bot-protection: знищує шкідливі програми, перетворюють ПК в зомбі

1	2	3	4	5
Безпечний запуск підозрілих програм: Можливість помістити будь-яку програму в пісочницю перед запуском на комп'ютері, щоб переконатись у її безпечності.	Сканер UEFI	Розширений аналіз в хмарі. Розгортання та модернізація	Автоматичне оновлення ПЗ та драйверів	Технологія Defense+: захищає самі важливі системні файли та блокує віруси до того, як вони зробили спробу інсталяції
Захист від зловмисників за допомогою вдосконаленого брандмауера: Захист від проникнення зловмисників у систему ПК та викрадення даних.	Захист від експлойтів	Захист хмарних додатків	Оповіщення про наявність уразливих учотних записів Інтернет-служб	Технологія Auto Sandbox: відкриває незнайомі файли в ізольованому просторі, в якому вони не можуть спричинити шкоди
Захист від стеження через вебкамеру: Блокування спроб сторонніх осіб стежити за вами через вебкамеру.	Мульти-платформений захист	Захист поштових серверів	Блокування атак програм-вимагачів останніх версій	Memory Firewall: передова технологія захисту проти дрібних атак у буфері
Остаточне видалення конфіденційних файлів: Безпечне видалення файлів без можливості відновлення.	Захист під час роботи в Інтернеті	Преміум-підтримка	Служба підтримки в пакеті	Anti-malware: знищує малвер та інші шкідливі процеси, перш ніж вони нанесуть шкоду системі
Автоматичне оновлення програм: Зменшення ризиків для безпеки завдяки автоматичному встановленню найновіших версій усіх програм.	Захист паролів та даних	Інструменти для офіцера кібербезпеки	Оптимізація швидкодії системи за допомогою 30 інструментів настройки класу преміум	
Встановлення на всіх ваших пристроях: Удосконалений захист до 10 пристроїв (ПК, Mac, Android і iOS).	Інспектор мережі		Анонімний та безпечний перегляд веб-сторінок з необмеженим доступом через VPN	
Містить Avast Cleanup Premium: Видалення непотрібних прихованих файлів, звільнення місця на диску й прискорення роботи комп'ютера.			Захист для 5 пристроїв	
Містить Avast SecureLine VPN: Шифрування підключення для безпеки та конфіденційності в Інтернеті.			Додатки класу преміум для Android и iOS в пакеті	
Містить Avast AntiTrack: Маскування цифрового відбитка для уникнення персоналізованої реклами.				

Аналіз інформації розміщеної на офіційних сайтах виробників антивірусного програмного забезпечення показав, що на сьогодні вказаний сегмент ринку пропозицій програмного забезпечення для широкого кола користувачів (споживачів) є досить широким і пропонує як безкоштовні варіанти, так і платні [9, 10, 12, 14]. Але при цьому необхідно враховувати, що увесь спектр інструментів (можливостей) конкретного антивірусу в залежності від потреб користувача (споживача) розподілено на окремі пакети послуг. При

© Скибун, О. Ж. (2023). Роль антивірусного захисту у формуванні екосистеми та імунної системи корпоративних інформаційних систем. Сучасний захист інформації, 1(53), 12–23. https://doi.org/10.31673/2409-7292.2023.010002.

цьому максимально повний перелік інструментів (можливостей) знаходиться у преміум сегменті.

Водночас необхідно зважати, що переважна більшість представленого антивірусного програмного продукту стосується приватних користувачів (для пристроїв, що знаходяться у домашньому користуванні та/або у малому бізнесі), а отже, не зовсім підходять для корпоративних ІС побудованих на сучасних платформах зі сформованою екосистемою та імунною системою протидії вірусам.

Прикладом такого підходу з боку компаній-розробників антивірусного програмного забезпечення є пакет «ESET Endpoint Protection» в рамках якого окрім базових інструментів захисту пропонуються додаткові: «сучасний захист робочих станцій з потужним машинним навчанням та легким керуванням; ведучий захист робочих станцій від програм-вимагачів та «0-денних» загроз, а також безпека даних; розширене виявлення та реагування на інциденти (XDR) з можливостями огляду корпоративної мережі; багаторівневий захист IT-середовища, управління ризиками та допомога провідних фахівців ESET» [14]. Досить цікавим є надання додаткової розширеної допомоги в частині підвищення рівня кіберзахисту через «Додаткові інструменти для офіцера кібербезпеки» [14].

Крім того, необхідно зауважити, що для просування на ринку надання послуг для секторів безпеки, оборони та державного сектора є сертифікація Державною службою спеціального зв'язку та захисту інформації України продуктів, експертні висновки якої підтверджують відповідність продуктової лінійки ESET нормативним документам, які регламентують вимоги до засобів технічного захисту інформації, встановлених законодавством України», а тому «рішення ESET можуть бути використані у всіх державних, фінансових, міжнародних та інших організаціях» [14]. Вказане є доречним і для приватного сектору, який співпрацює із вказаними організаціями.

Але все рівно актуальним залишається питання вибору антивірусного програмного забезпечення. Якщо це величезна транснаціональна корпорація, то скоріш за все питання програмного забезпечення вирішується на рівні вендорів, які пропонують повний пакет, в тому числі і антивірусного програмного забезпечення. Це стосується окремих користувачів та/або малого бізнесу у яких немає значних фінансових ресурсів, то на допомогу їм приходить метод експертних оцінок, коли «для покращення ефективності оцінки передбачена можливість розподілу показників за групами, що складають індивідуальну пріоритетність за потребами». Наприклад для корпоративних ІС можна взяти такі показники: «локальне управління захистом; управління захистом на основі хмар; антивірусний захист робочих станцій; захист файлових серверів; захист поштових серверів; DLP; SIEM; Privileged Users», а розрахунок суми кількості балів для кожного продукту визначається за такою формулою:

$$S_i = \sum_{i=1}^{n} a_i \cdot M_i,$$

де S_i – сумарна кількість балів стандарту,

a_i – і оцінка параметру,

M_i – ваговий коефіцієнт i параметра системи.

Кількісні показники («з врахуванням важливості параметрів, з максимальним коефіцієнтом важливості 10») для запропонованих нами антивірусних програмних продуктів представлені у таблиці 2. Вказані дані носять елемент суб'єктивності, який базується на наявних початкових даних, які є у наявності у експерта для проведення експертного оцінки.

Для отримання чисельної аргументації, визначаємо середню оцінку кожного стандарту за формулою:

© Скибун, О. Ж. (2023). Роль антивірусного захисту у формуванні екосистеми та імунної системи корпоративних інформаційних систем. Сучасний захист інформації, 1(53), 12–23. https://doi.org/10.31673/2409-7292.2023.010002.

$$S = 10 \cdot \frac{S_I}{A},$$

де S_i – сумарна кількість балів для стандарту,

А – максимальна кількість балів.

Результати порівняння аналізу оцінок антивірусного програмного забезпечення зведені у таблицю 3.

Таблиця 2

Кількісні показники важливості параметрів для вибраних антивірусів

	Avast Free Antivirus 22.2.6003	ESET Internet Security	ESET Endpoint Protection	Avira Free Antivirus 15.0.2201.2134	Comodo Internet Security 12.2.4.8032 Final
Локальне управління захистом	10	7	10	10	9
Управління захистом на основі хмар	0	0	10	10	9
Антивірусний захист робочих станцій	10	10	10	10	10
Захист файлових серверів	9	9	10	10	10
Захист поштових серверів	9	9	10	10	10
DLP	10	0	10	10	10
SIEM	0	10	10	9	10
Privileged Users	7	8	10	7	7
Максимальна кількість балів	56	53	80	78	75

Сучасний стан і темпи розвитку шкідливого програмного забезпечення, які орієнтовані на різноманітну шкоду для споживачів та організацій, дозволяють зробити висновок про складність та необхідність проведення обґрунтованого вибору технологій захисту від вірусів, троянів та іншого шкідливого програмного забезпечення. Це обумовлено, з одного боку, зростаючими темпами атак на споживачів та постачальників. Споживачі стають більш вразливими в питаннях кібернетичної безпеки на ринку кібербезпеки та послуг, що надаються, і їх оптимального використання в своїй повсякденній та професійній діяльності.

Таблиця 3

Загальна оцінка антивірусу

Антивірус	Загальна оцінка антивірусу (S)
Avast Free Antivirus 22.2.6003	7,0
ESET Internet Security	6,62
ESET Endpoint Protection	10,0
Avira Free Antivirus 15.0.2201.2134	9,75
Comodo Internet Security 12.2.4.8032 Final	9,37

Аналіз тенденцій розвитку антивірусного захисту для корпоративного бізнесу, представлених складними ІС на основі нейронних мереж, з використанням штучного інтелекту, Інтернету речей, створенню імунної системи та власної екосистеми кіберпростору та кіберзахисту дозволяють визначити, що головними запитами з боку замовників (споживачів) є забезпечення інтеграції у імунну та екосистеми корпоративного ІС для сталого та стійкого функціонування ІС в цілому, захисту та збереження чутливої інформації (власної та клієнтської) персональних даних, можливість швидкого реагування на зовнішні та внутрішні подразники з подальшою адаптацією до змін та самонавчання.

© Скибун, О. Ж. (2023). Роль антивірусного захисту у формуванні екосистеми та імунної системи корпоративних інформаційних систем. Сучасний захист інформації, 1(53), 12–23. https://doi.org/10.31673/2409-7292.2023.010002.

Висновки

У рамках здійснення порівняння систем антивірусного захисту розглянуто сучасні тенденції щодо корпоративних інформаційних систем, які все більше ускладнюються разом із задачами, що необхідно вирішувати за допомогою ІС. Разом з цим збільшуються обсяги оброблюваної інформації (в ІС все частіше залучаються потужні обчислювальні системи так звані «суперкомп'ютери»); структура ІС стає більш відкритою для ведення бізнесу в онлайн (дистанційно). В таких умовах побудова та робота ІС відбувається на основі нейронних мереж, з використанням штучного інтелекту, побудові власної екосистеми та створення імунної системи, адже поряд із позитивним технічно-технологічним розвитком відбувається і негативний, пов'язаний із кіберзлочинами. Ось чому питання кіберзахисту та кібербезпеки набувають все більшої актуальності. І така тенденція тільки зростає. А тому запит на антивірусний програмний продукт, який би міг ефективно протистояти сучасним кіберзлочинам йде від усіх учасників кіберпростору.

У рамках даної статті розглянуто п'ять антивірусних продуктів відомих виробників програмного продукту. Так, для базового початкового рівня звичайного користувача (домашній комп'ютер та/або декілька пристроїв), коли технічні можливості використовуються для елементарних потреб (ділова переписка, Інтернет серфінг, ігри тощо), то в цілому безкоштовних версій антивірусного програмного продукту достатньо. Якщо вже користувачем (споживачем) здійснюється робота з великими масивами інформації, базами даних, відео, аудіо, дизайн, 3D графіка тощо, то можливості безкоштовних антивірусних продуктів буде недостатньо, оскільки вони забезпечуються мінімальний захист. Більш повними та спроможними у кіберзахисті є преміальні (максимальні) пакети антивірусних програмних продуктів, які є доступними тільки на платній основі.

Що стосується корпоративних ІС нового покоління, то не всі навіть преміальні пакети програмних антивірусних продуктів, які розглянуті в рамках цієї статті, спроможні задовольнити вимоги і потреби не тільки по захисту, а й адаптації до наявної екосистеми та спроможності сформувати стійку та сталу до вірусів та уразливостей імунну систему ІС.

Огляд запропонованих систем антивірусного захисту показав, що вказані антивірусні продукти демонструють результати вище середніх лише у версіях «premium», а тому можуть бути рекомендовані лише такі для використання. Що стосується великих корпоративних ІС, то найкращий варіант – це використовувати той антивірусний продукт, який буде рекомендований головним вендором, який відповідає за програмне забезпечення усього комплексу ІС.

Перелік посилань

1. Використання нейромережевих технологій для інформаційної підтримки етапів життєвого циклу САПР. [Електронний ресурс] – Режим доступу: https://essuir.sumdu.edu.ua/handle/123456789/26560. (дата звернення 04.12.2022) – Назва з екрана.
2. Гайдур Г.І. План-конспект лекції № 3 з дисципліни «Прикладна загальна теорія систем ІКБ» за спеціальністю 125 – Кібербезпека – Інформаційна та кібернетична безпека. 19 с.
3. Гахов С.О. Застосування положень імунології в теорії захищених інформаційних систем. Сучасний захист інформації № 2(34), 2018. С.59-64.
4. Екосистема інформаційної та кібернетичної безпеки. Інформація з екрана. [Електронний ресурс] – Режим доступу:https://www.dut.edu.ua/ua/298-zagalna-informaciya-kafedra-informaciynoi-ta-kibernetichnoi-bezpeki. (дата звернення 05.12.2022) – Назва з екрана.
5. Коцовський В. М. Інтелектуальні інформаційні системи. Конспект лекцій. Ужгородський національний університет, Ужгород. 2019. 73 с.
6. Куц О.В. Концепція інформаційної екології у дослідженні бібліотек. Матеріали XX-ї ювілейної міжнародної науково-практичної конференції, 2021 р. Київ–Ужгород. С.43-44.
7. Огляд безкоштовних і платних антивірусів: плюси і мінуси. [Електронний ресурс] – Режим доступу: https://bankchart.com.ua/finansoviy_gid/groshi_rodini/statti/oglyad_bezkoshtovnih_i_platnih_antivirusiv_plyusi_i_minusi. (дата звернення 08.12.2022) – Назва з екрана.

8. Тертичний В.О. Дослідження і обгрунтування вибору методів інформаційної безпеки IT компанії. Харківський національний університет радіоелектроніки, Харків, 2020, 81 с.

9. Avast Free Antivirus. [Електронний ресурс] – Режим доступу: https://www.avast.ua/lp-ppc-hp-v5?ppc_code=012&ppc=a&gclid=EAIaIQobChMI8J-B3Jvf-wIVxO93Ch09eAgVEAAYASAAEgJ-p_D_BwE&gclsrc=aw.ds#pc. (дата звернення 10.12.2022) – Назва з екрана.

10. Avira Free Security. [Електронний ресурс] – Режим доступу: https://www.avira.com/ru?x-clickref=1101lwnEXHkt&x-c-channel=partnerize&x-a-medium=111l748&utm_source=partnerize&utm_medium=affiliate&utm_content=0&utm_term=adgoal_eu. (дата звернення 09.12.2022) – Назва з екрана.

11. Castels M., Flecha R., Freire P., Critical Education in the New Information Age. (Критична освіта в епоху нової інформації). Rowman and Littlefield Publishers, 1999. 176 p. ISBN 0-8476-9011-3

12. Comodo Internet Security. [Електронний ресурс] – Режим доступу: https://ru.comodo.com/software/internet_security/free-internet-security.php. (дата звернення 12.12.2022) – Назва з екрана.

13. Enterprise security solutions. IBM Security provides enterprise cybersecurity solutions to help you thrive in the face of uncertainty. [Електронний ресурс] – Режим доступу: https://www.ibm.com/security. (дата звернення 11.12.2022) – Назва з екрана.

14. ESET Internet Security. Комплексная защита. Версия 2023. [Електронний ресурс] – Режим доступу: https://www.eset.com/ua-ru/. (дата звернення 05.12.2022) – Назва з екрана.

15. Ganguly Raman Digital ecosystems for data preservation (Цифрова екосистема для збереження даних). Цифрова платформа: інформаційні технології в соціокультурній сфері. 2018, № 1. С.87-96. DOI:10.31866/2617-796x.1.2018.151343. [Електронний ресурс] – Режим доступу: http://infotech-soccult.knukim.edu.ua/article/view/151343. (дата звернення 08.12.2022) – Назва з екрана.

16. Raguseo Domenico. The Power of the Security Immune System Intelligence & Analytics June 16, 2017. [Електронний ресурс] – Режим доступу:https://securityintelligence.com/the-power-of-the-security-immune-system/. (дата звернення 09.12.2022) – Назва з екрана.

17. The security immune system. An integrated approach to protecting your organization. [Електронний ресурс] – Режим доступу: https://www.midlandinfosys.com/pdf/qradar-siem-cybersecurity-ai-products.pdf. (дата звернення 09.12.2022) – Назва з екрана.

18. Vinyavsky Alexander. How to create a cyber immune system? Is it possible to make a hack-proof system? [Електронний ресурс] – Режим доступу: https://www.kaspersky.com/blog/how-to-create-cyberimmune-system/46314/. (дата звернення 03.12.2022) – Назва з екрана.

Надійшла: 21.12.2022 Рецензент: д.т.н., професор Гайдур Г.І.