УДК 004.45 + 004.7 DOI: 10.31673/2786-8362.2025.018514

Катков Ю.І., д.т.н.; **Березовська Ю.В.,** PhD;
Локойда А.О.; Лупол М.О.

ОСОБЛИВОСТІ АДМІНІСТРУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ НА ОСНОВІ WINDOWS SERVER 2022

Katkov Yu.I., Berezovska Yu.V., Lokoyda A.O., Lupol M.O. Features of administering a corporate network based on Windows Server 2022. The article is dedicated to the issue of determining the peculiarities of administering a corporate network based on Windows Server 2022. There is a problem of ensuring the security of the OS Windows Server 2022 using special vulnerability protection mechanisms during the administration of a corporate network. Solving this problem becomes extremely important for businesses and organizations. The IT infrastructure built on the basis of the OS Windows Server 2022 is becoming increasingly complex and voluminous today, requiring constant administration to timely respond to possible failures or malfunctions that may lead to interruptions in work, financial losses, or even threats to data security. Therefore, the application of special vulnerability protection mechanisms for the OS Windows Server 2022 proves to be a powerful tool for anticipating, detecting, and addressing potential issues before they affect its efficiency. The article discusses key aspects and capabilities of vulnerability protection mechanisms for software tools: Common Vulnerability Scoring System; Common Vulnerabilities and Exposures; National Vulnerability Database. It reveals the main aspects and advantages of their application.

Keywords: vulnerabilities, cybersecurity, Common Vulnerability Scoring System; Common Vulnerabilities and Exposures; National Vulnerability Database

Катков Ю.І., Березовська Ю.В., Локойда А.О., Лупол М.О. Особливості адміністрування корпоративної мережі на основі Windows Server 2022. Стаття присвячена питанню визначення особливості адміністрування корпоративної мережі на основі Windows Server 2022. IT-інфраструктура, яка побудована на основі ОС WS 2022, стає все більш складною та об'ємною, вимагаючи постійного адміністрування, щоб вчасно реагувати на можливі збої чи неполадки, які можуть призвести до перерв у роботі, фінансових втрат чи навіть загроз для безпеки даних. У зв'язку з цим, застосування спеціальних механізмів захисту від вразливостей ОС WS 2022 виявляється потужним інструментом для передбачення, виявлення та вирішення можливих проблем щодо погіршення її ефективності. В статті розглянуті ключові аспекти та можливості механізмів захисту від вразливостей для програмних засобів: Common Vulnerability Scoring System; Common Vulnerabilities and Exposures; National Vulnerability Database. Розкриті основні аспекти та переваги їх застосування.

Ключові слова: вразливості, кібербезпека, Common Vulnerability Scoring System; Common Vulnerabilities and Exposures; National Vulnerability Database

Вступ

Microsoft випустила нову флагманську операційну систему Windows Server (ОС WS) 2022 [1]. Вона побудована на ключових принципах: розширений захист, спрощена безпека, превентивний захист, та містить новітні і найважливіші функції, які доступні клієнтам Microsoft для виконання критично важливих для бізнесу робочих навантажень. Однак, під час адміністрування корпоративної мережі на основі ОС WS 2022 виникають завжди у кожному новому програмному продукті різноманітні вразливості, використання яких зловмисниками може призвести до ризиків втрати конфіденційності, цілісності, доступності.

Постановка завдання. Небезпека вразливості ОС WS 2022 у тому, що це вразливості всередині ОС, які дозволяють кіберзловмисникам завдати шкоди будь-якому обладнанню, на якому встановлена ОС. Якщо розглядати ОС WS 2022, то вже визначено з моменту її впровадження більше 1117 вразливостей та перелік їх постійно зростає [2]. Тому виникає проблема забезпечення безпеки ОС WS 2022 за допомогою спеціальних механізмів захисту від вразливостей під час адміністрування корпоративної мережі. Вирішення цієї проблеми стає надзвичайно важливою для бізнесу та організацій. IT-інфраструктура, яка побудована на основі ОС WS 2022, стає все більш складною та об'ємною, вимагаючи постійного адміністрування, щоб передбачати та реагувати на можливі неполадки, які можуть призвести

до перерв у роботі, фінансових втрат чи навіть загроз для безпеки даних. У зв'язку з цим, застосування спеціальних механізмів захисту від вразливостей ОС WS 2022 виявляється потужним інструментом для передбачення, виявлення та вирішення можливих проблем до погіршення її ефективності. У цьому контексті розуміння способів використання спеціальних механізмів захисту від вразливостей ОС WS 2022 під час адміністрування корпоративної мережі набуває особливого значення, тому що ці механізми можуть надати швидкі, точні та прогнозовані рішення щодо забезпечення безпеки ОС WS 2022. Вирішення цієї проблеми є актуальним та своєчасним.

Аналіз останніх досліджень. На сьогодні в більшості наукових джерел та публікацій розглядаються різноманітні теми: використання нових функцій та можливостей ОС WS 2022 для підвищення продуктивності, безпеки та надійності корпоративних мереж, наприклад, [2, 5, 8]. У публікаціях [7, 8] розглянуто яким чином ОС WS 2022 можна використовувати для покращення безпеки корпоративної мережі. Окремо розглянуті питання, які стосуються адміністрування корпоративної мережі, наприклад, у [9]. Але питанню розгляду спеціальних механізмів захисту від вразливостей статей небагато. Звідси можна зробити висновок про те, що дослідження цього питання на сьогоднішній день є вкрай перспективним та має значний потенціал для подальшого розвитку. Важливо продовжувати дослідження в цьому напрямку для створення ефективних спеціальних механізмів захисту від вразливостей та їх практичного застосування. Тому, для подальшого розвитку необхідно розуміння, що потрібно робити. Звідси виникає наступна мета.

Метою роботи є аналіз можливостей та переваг використання спеціальних механізмів захисту від вразливостей під час адміністрування корпоративної мережі на основі ОС WS 2022 для виявлення оптимальних методів, які допоможуть удосконалити процес контролю, щоб забезпечити надійність та безпеку функціонування цифрових систем. Тому, виникає наступне завдання в даній статті: виконати аналіз сучасних спеціальних механізмів захисту від вразливостей ОС WS 2022 для визначення їх практичного застосування.

Виклад основного матеріалу дослідження

Адміністрування ОС WS 2022 – це керування комп'ютерними системами та мережами, що використовують ОС WS 2022. Це область роботи, в якій хтось керує однією або декількома системами, будь то програмне забезпечення, обладнання, сервери або робочі станції. Мета системного адміністрування – забезпечити ефективну та дієву роботу систем. Тому, системне адміністрування передбачає визначення системних потреб компанії, встановлення обладнання та програмне забезпечення, необхідного для задоволення цих потреб, а також забезпечення безпеки мереж організацій.

Відомо, що ОС WS 2022, створена для забезпечення підвищеної стабільності та продуктивності для малого та середнього бізнесу, є ідеальним вибором для компаній, які бажають оновити свою інфраструктуру, щоб зробити її більш надійною та ефективною. ОС WS 2022 заснована на ОС Windows Server 2019 та має 10-річний цикл підтримки. Windows Server 2022 включає безліч різних функцій, покликаних зробити бізнес-операції швидшими та продуктивнішими. Деякі з нових функцій включають: процесори AMD тепер підтримують вкладену віртуалізацію; Microsoft Edge як веб-браузер за умовчанням; покращені функції безпеки для підвищення захисту від шкідливого програмного забезпечення, конфіденційності та мережевих атак; поліпшення продуктивності UDP/TCP; гібридні можливості в Azure тощо. Багато нових функцій та можливостей Windows Server 2022 дозволяють клієнтам підвищити безпеку та можливості гібридної хмари на новий рівень [1].

Однак, під час адміністрування корпоративної мережі на основі ОС WS 2022 виникають різноманітні вразливості, використання яких зловмисниками може призвести до ризиків втрати конфіденційності; цілісності; доступності. Небезпека від вразливості ОС WS 2022 у тому, що дані вразливості виникають всередині ОС, які дозволяють кіберзловмисникам завдати шкоди будь-якому пристрою, на якому встановлена ОС. Наприклад, відомі такі основні вразливості ОС WS 2022:

- підвищення рівня вразливості драйвера файлової системи загального журналу Windows (CVE-2022-37969 – коли у модулі mod_proxy_ajp httpd було виявлено помилку: з'єднання не закривається за наявності неприпустимого заголовка Transfer-Encoding, що дозволяє зловмиснику переправляти запити на сервер AJP, щоб він перенаправляв запити від себе);
- розширення протоколу обміну ключами в Інтернеті (IKE) Windows, вразливість віддаленого виконання коду (CVE-2022-34722 – коли зловмисник, який не пройшов автентифікацію, може відправити спеціально створений IP-пакет на цільовий комп'ютер під керуванням Windows і з увімкненим IPSec, що може уможливити віддалене виконання коду, ця вразливість стосується всіх серверів Windows, оскільки вони приймають IP-пакети);
- уразливість служби подій Windows COM+, що пов'язано з несанкціонованим підвищенням привілеїв (EoP) (CVE-2022-41033 – це вразливість у службі системи подій Windows COM+, може бути використана шляхом запуску спеціально створеної програми для виконання довільного коду з вищими привілеями) та інші.

Для попередження вразливості використовують спеціальні механізми захисту від вразливостей під час адміністрування корпоративної мережі на основі ОС WS 2022. З цих прикладів бачимо, що для розуміння спеціальних механізмів захисту від вразливостей по-перше необхідно розуміти та визначитися з основними поняттями.

У кібербезпеці існують важливі відмінності між вразливістю, експлойтами, ризиком та загрозами.

Вразливості (Vulnerabilities) – недоліки, які послаблюють загальну безпеку пристрою/системи. Математичне моделювання вразливостей (vulnerabilities) для Windows Server 2022 може здійснюватися через різні підходи: стохастичні моделі, моделі на основі теорії графів, теорії ймовірностей, а також моделі оцінки ризиків. Один з підходів – створення математичної моделі уразливості як функції часу, імовірності експлуатації та критичності системи [3]. Диференціальне рівняння для кількості вразливостей має вигляд (1):

$$\frac{dV(t)}{dt} = \lambda - \mu V(t). \quad (1)$$

Розв'язком буде (2):

$$V(t) = \frac{\lambda}{\mu}(1 - e^{-\mu t}), \quad (2)$$

де $V(t)$ – рівень вразливості Windows Server 2022 у момент часу t;

λ – швидкість появи нових вразливостей;

μ – швидкість усунення вразливостей (патчі, оновлення);

Ризик (Risk) – можливість значного впливу внаслідок використання вразливості. Але необхідно розуміти, що, існують вразливості без ризику, тобто коли не має значного впливу Модель ризику експлуатації має вигляд (3).

$$\mathrm{R(t)} = V(t) * \rho_e * S_c, \quad (3)$$

де: $\mathrm{R(t)}$ – поточний ризик для Windows Server 2022;

ρ_e – ймовірність експлуатації знайденої вразливості, можна взяти з даних CVSS (наприклад, для вразливостей з рейтингом 9.8 – близько 0.9);

S_c – критичність сервера (від 0 до 1), залежить від ролі сервера (наприклад, для контролера домену = 1, для внутрішнього файлового сервера = 0.6).

Імовірнісна оцінка атаки за період ($P_a(t)$) – показник оцінки імовірності того, що система буде скомпрометована в період $\mathrm{T}[0, t]$, використовуємо (4):

$$P_a(t) = 1 - e^{-R_{ср}T}, \quad (4)$$

де $R_{ср}$ – середній ризик у проміжку $[0, t]$.

Вікно вразливості (Vulnerability window) – час з моменту, коли дірка в безпеці була виявлена або виявлена в розгорнутому програмному забезпеченні, до моменту, коли доступ був закритий, виправлення безпеки було доступне/розгорнуте або зловмисник був відключений. Звідси можна розглядати вразливість різних рівнів: ніякий, низький, середній, високий, критичний (рис. 1) [3].

На рисунку 1 показано вікно вразливості, як період між моментом виявлення вразливості та моментом випуску патчу. Зона між ними є критичним періодом, коли система піддається

ризику, бо вразливість вже відома, але ще не виправлена.

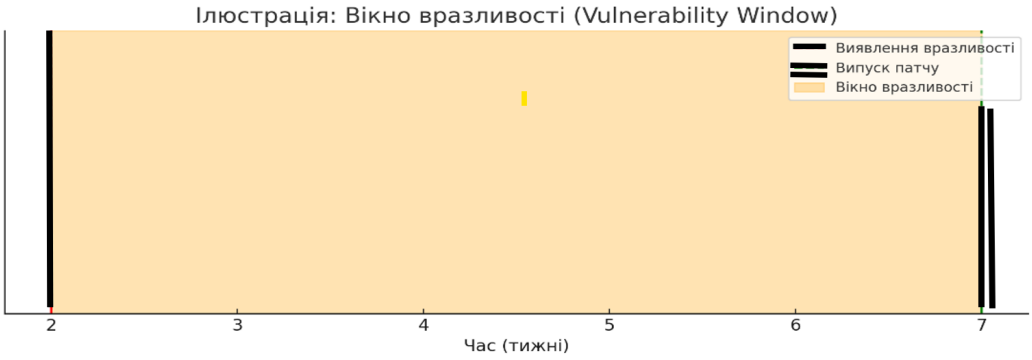

Рис. 1. Вікно вразливості для Windows Server 2022

Експлойт (Exploit) – комп'ютерна програма, фрагмент програмного коду або послідовність команд, що використовують вразливості в програмному забезпеченні та призначені для проведення атаки на обчислювальну систему. Метою атаки може бути як захоплення контролю над системою (підвищення привілеїв), так і порушення її функціонування (DoS-атака). Атака експлойта може бути націлена на різні компоненти обчислювальної системи – серверні програми, клієнтські програми або модулі операційної системи. Експлойти, фактично, призначені для виконання сторонніх дій у вразливій системі й можуть бути розділені між собою таким чином: для операційних систем; для прикладного програмного забезпечення (музичні програвачі, офісні пакети та інші); для браузерів (Internet Explorer, Mozilla Firefox, Opera та інші); для інтернет-продуктів (IPB, WordPress, VBulletin, phpBB); для сайтів (facebook, hi5, livejournal) [4].

Загроза (Threat) – це можлива небезпечна подія, яка не відбулася, але може завдати шкоди, якщо станеться [3].

Таким чином, експлойти – це те, як загрози стають атаками, а вразливості – це те, як експлойти отримують доступ до цільових систем.

Основні типи вразливостей в інформаційній безпеці: мережеві вразливості, вразливості операційної системи, процесні (або процедурні) вразливості та людські вразливості.

Мережеві вразливості – це слабкі місця в апаратній або програмній інфраструктурі організації, які дозволяють кіберзловмисникам отримати доступ і завдати шкоди.

Вразливості операційної системи (ОС) – це вразливості всередині ОС, які дозволяють кіберзловмисникам завдати шкоди будь-якому обладнанню чи пристрою, на якому встановлена ОС.

Вразливості процесів виникають, коли процедури, які мають діяти як заходи безпеки, недостатньо. Однією з найпоширеніших вразливостей процесу є слабкість аутентифікації, коли користувачі й навіть IT-адміністратори використовують слабкі паролі.

Людські вразливості створюються помилками користувачів, які можуть зробити мережі, обладнання та конфіденційні дані доступними для зловмисників. Прикладами людської вразливості в системі безпеки є відкриття вкладення електронної пошти, зараженого шкідливим програмним забезпеченням.

Управління вразливістю за допомогою спеціальних механізмів – практичні дії, які відрізняються в теорії, але містять загальні процеси, що включають: виявлення всіх активів, визначення пріоритетності активів, оцінку або виконання повного сканування вразливостей, звіт про результати, усунення вразливостей, перевірку виправлення – повторення. Ці практичні дії зазвичай відносяться до вразливостей програмного забезпечення у обчислювальних системах. Гнучке управління вразливістю передбачає запобігання атак від загроз шляхом максимально швидкого виявлення всіх шкідливостей (ступень загрози). Використання поняття «вразливості» з тим самим значенням поняття «ризику» може призвести до плутанини. Тому необхідно запам'ятати: вразливість – це слабке місце, передбачена можлива небезпека. Загроза – це реальна небезпека. Ризик – можливість

небажаної події, втрати, недосягнення очікуваних результатів діяльності агенту або відхилень від них.

Механізми захисту від вразливостей. Сьогодні існують такі механізми захисту від вразливостей для програмних засобів: загальна система оцінки вразливостей (CVSS – Common Vulnerability Scoring System); поширені вразливості та ризики (CVE – Common Vulnerabilities and Exposures); Національна база даних вразливостей (NVD – National Vulnerability Database) [6, 11, 12].

CVSS – система, яка широко використовується в програмах керування вразливістю. CVSS вказує на серйозність уразливості інформаційної безпеки та є невід'ємним компонентом багатьох інструментів сканування вразливостей. Вона дозволяє виявити основні характеристики вразливості та отримати числову оцінку, що відображає її серйозність [9, 10]. CVSS намагається привласнити вразливість ступінь серйозності, дозволяючи службам реагування розставляти пріоритети відповідей та ресурсів відповідно до загрози. CVSS зараз має версії v.1, v.2.0, v.3.1, v4.0. Оцінка CVSS вимірює три проблемні області:

1. Базові метрики якостей, які належать вразливості;

2. Тимчасові метрики якостей, які належать характеристикам вразливості, що змінюються протягом терміну;

3. Метрики якостей конкретної реалізації, які належать характеристикам вразливості та залежать від конкретної реалізації або дій.

Величина оцінки розраховується на основі формули, що залежить від декількох показників, які визначають простоту і вплив експлойту. Оцінка CVSS поєднує безліч факторів, що дозволяють отримати оцінку. Цими факторами є: вектор атаки; складність атаки; необхідні привілеї; взаємодія з користувачем; обсяг; конфіденційність; чесність; доступність.

Вектор атаки показує звідки зловмисник може отримати доступ до системи. Має 4 різні значення, які йому можна привласнити: мережевий, сусідній, місцевий або фізичний.

Складність атаки зводиться до того, як складно використовувати вразливість. Для цього існують два можливі значення: низький або високий. Низька складність атаки дозволить здобути найвищий бал.

Необхідні привілеї описують, які привілеї повинен мати зловмисник перед використанням вразливості. Можливі значення: ніякий, низький або високий. "Ніякий" – відсутність доступу до будь-яких параметрів або файлів у системі. "Низький" – базові можливості користувача. "Високий" – потрібні привілеї адміністративного рівня.

Взаємодія з користувачем визначає, як користувач повинен якимось чином залучитися до роботи, щоб успішно скористатися вразливістю. Можливі варіанти: не потрібний або необхідний. Коли користувач "не потрібний", вплив на оцінку CVSS є найвищим.

Обсяг трохи складніший для розуміння підкомпонент. За його допомогою намагаються визначити масштаб вразливості вплинути на об'єкти системи, що знаходяться за межами повноважень безпеки порушеного компонента. Орган безпеки – це те, що контролює доступ до об'єктів, які знаходяться під його контролем. Прикладами об'єктів системи для органу безпеки можуть бути додаток (керує тим, як усе працює всередині програми), операційна система (керує тим, як усе працює в середовищі). Значення тут такі: без змін або змінений. Зміна масштабу має найбільший вплив.

Конфіденційність – це можливість несанкціонованого доступу до конфіденційної інформації. Можливі значення: високий, низький або ніякій. Найбільший вплив має високе значення або повна втрата конфіденційності.

Чесність вимірює ймовірність несанкціонованої зміни, витоку чи видалення даних. Потенційні значення: високий, низький або ніякій. Високий – найважчий.

Доступність намагається виміряти можливість відмови у доступі авторизованим користувачам. Це може бути відмова у доступі до сервісу або циклів процесора. Можливі значення доступності: високий, низький або ніякій. Високий – найважчий.

Також існують часові оцінки CVSS для оцінки навколишнього середовища, які враховують наявність заходів щодо пом'якшення наслідків та ступінь поширеності вразливих

систем в організації відповідно. Для розрахунку цих показників в Інтернеті є безліч калькуляторів, наприклад, [6].

CVE – база даних загальновідомих вразливостей інформаційної безпеки, що підтримується некомерційною організацією MITRE. Кожній вразливості присвоюється ідентифікаційний номер виду (CVE-рік-номер). Для цього номеру є опис і ряд загальнодоступних посилань з описом. Підтримкою CVE займається організація MITRE. Фінансуванням проекту CVE займається US-CERT. Список CVE є "словником", в якому створено загальну стандартизовану угоду про імена для системних, мережевих та програмних вразливостей, що дозволяє організаціям обмінюватися інформацією про нові ризики та створювати базові показники для оцінки ефективності інструментів та послуг кібербезпеки. Прикладами недоліків програмного забезпечення, які можуть призвести до появи вразливостей, є: переповнення буфера; оцінка та використання коду; маніпуляції із звичайними спеціальними елементами; різноманітні помилки, а саме: каналу; оброблювача; інтерфейсу користувача; автентифікації [9 – 10].

CVE-ідентифікатори. При перевірці вразливостей орган нумерації CVE (CNA) надає номер. Ідентифікатор CVE має формат *CVE-{год}-{ID}*. CNA надає свої повноваження MITRE, який також може безпосередньо надавати номери CVE. Інформація про вразливість надається CNA через дослідників, постачальників чи користувачів [10].

Відмінності між CVSS та CVE. CVSS – має загальний бал, що присвоюється вразливості. CVE – це просто список усіх публічно розкритих вразливостей, що включає ідентифікатор CVE, опис, дати та коментарі. Оцінка CVSS не вказана у списку CVE. Під час використання CVE необхідно використовувати NVD, щоб знайти призначені оцінки CVSS.

NVD – Національна база даних вразливостей – це база даних, що підтримується NIST, повністю синхронізована зі списком MITRE CVE. Ці дані дозволяють автоматизувати управління вразливістю, вимірювання безпеки та дотримання вимог. База складається з різних фід (feed). Існують різні види фід. Фіди "рік", які оновлюються один раз на день, а фіди "останні" та "змінені" оновлюються кожні дві години [6].

Відмінності між CVE та NVD. Список CVE передається в NVD, тому обидва вони постійно синхронізуються. NVD надає розширену інформацію, окрім тієї, що міститься у списку CVE, включаючи наявність виправлень та оцінки серйозності. NVD також надає простіший механізм пошуку по широкому діапазону змінних. CVE і NVD спонсоруються федеральним урядом США та доступні для безкоштовного використання будь-ким.

Результати моделювання. Для прикладу розглянемо результати моделювання вразливостей і ризику для Windows Server 2022 для параметрів, що наведені у таблиці 1.

Таблиця 1

Значення параметрів для моделювання

Параметр	Значення
λ	0.2 вразливостей/тиждень
μ	0.1 (патчі повільні)
ρ_e	0.85
S_c	0.9

На рисунку 2 наведено графік залежності вразливості та ризику для Windows Server 2022, який побудовано за допомогою мови програмування Python з використанням бібліотеки Matplotlib.

На графіку показано:

пряма лінія ($V(t)$) – зростання кількості вразливостей з часом. Вона наближається до стабільного значення (максимуму), коли темп патчів дорівнює темпу появи нових вразливостей;

пунктирна лінія ($\mathrm{R(t)}$) – ризик компрометації сервера. Він стабілізується, але зростає швидше через множення на ймовірність експлуатації та критичність.

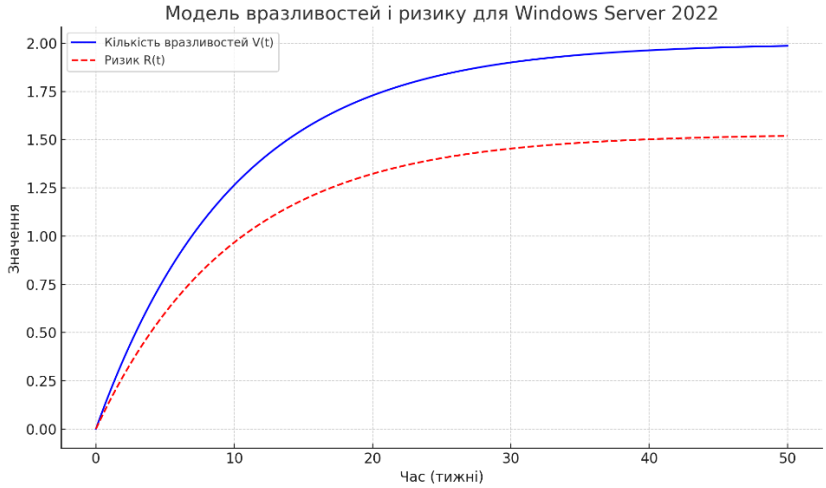

Рис. 2. Графік залежності вразливості та ризику для Windows Server 2022

Цей графік допомагає оцінити, як важливо регулярно оновлювати Windows Server 2022, щоб зменшити рівень ризику.

Таким чином, математична модель вразливостей Windows Server 2022 дозволяє: кількісно оцінити рівень загрози; визначити, як часто потрібно оновлювати сервер; визначити критичні періоди для безпеки системи; прогнозувати ймовірність компрометації.

Висновки

Для вирішення проблеми забезпечення безпеки ОС WS 2022 за допомогою спеціальних механізмів захисту від вразливостей під час адміністрування корпоративної мережі необхідно їх грамотне використання, що допоможе удосконалити процес контролю, щоб забезпечити надійність та безпеку функціонування цифрових систем.

Майбутньою перспективою використання механізмів захисту від вразливостей для програмних засобів буде базуватися на механізмах: загальна система оцінки вразливостей (CVSS – Common Vulnerability Scoring System); поширені вразливості та ризики (CVE – Common Vulnerabilities and Exposures); Національна база даних вразливостей (NVD – National Vulnerability Database). Ці системи мають значний потенціал.

Список використаної літератури:

1. Microsoft Windows Server 2022 Security Vulnerabilities in 2025. stack.watch – Weekly Security Vulnerability Emails. URL: https://stack.watch/product/microsoft/windows-server-2022/

2. 10 New Things in Windows Server 2022 to Know. Geekflare. URL: https://geekflare.com/new-features-in-windows-server-2022/

3. Даник Ю.Г., Катков Ю.І., Пічугін М.Ф. Національна безпека: запобігання критичним ситуаціям : монографія. Житомир : Рута, 2006. 386 с.

4. What's new in Windows Server 2022. Microsoft Learn: Build skills that open doors in your career. URL: https://learn.microsoft.com/en-us/windows-server/get-started/whats-new-in-windows-server-2022

5. Windows Server 2022 Security Hardening best practices. Virtualization Howto. URL: https://www.virtualizationhowto.com/2021/12/windows-server-2022-security-hardening-best-practices/

6. NATIONAL VULNERABILITY DATABASE. NVD – Home. URL: https://nvd.nist.gov

7. Катков Ю. І., Локойда А. О. Захист критичної інфраструктури від кібератак і терористичних загроз. «Актуальні проблеми кібербезпеки» : матеріали Всеукр. науково-практ. конф., м. Київ, 27 жовт. 2023 р. Київ, 2023. С. 180–182.

8. Windows Server supported networking scenarios. URL: https://learn.microsoft.com/en-us/windows-server/networking/windows-server-supported-networking-scenarios

9. Common Vulnerability Scoring System v3.1: Specification Document. URL:

https://www.first.org/cvss/v3.1/specification-document

10. Common Vulnerabilities and Exposures. URL: https://www.cvedetails.com/

11. Функціональна стійкість інформаційних мереж при наявності обмеженої апріорної інформації про надійність / Ю. Березовська та ін. Зв'язок. 2020. № 6(148). С. 42–46.

12. Березовська Ю. Інформаційні системи безперервного використання з часовим резервуванням. Сучасні досягнення компанії Hewlett Packard Enterprise в галузі IT та нові можливості їх вивчення і застосування : тези доп. Міжнар. науково-практ. конф., м. Київ, 16 груд. 2020 р. Київ, 2020. С. 6–8.

Автори статті

Катков Юрій – доктор технічних наук, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0009-0007-1194-4014

Березовська Юлія – PhD, доцент, Державний університет інформаційно-комунікаційних технологій, Київ, Україна.

ORCID: 0000-0002-9973-0497

Локойда Андрій – магістр, Державний університет інформаційно-телекомунікаційних технологій, Київ, Україна.

ORCID: 0009-0000-8110-5098

Лупол Максим – студент, Державний професійно-технічний навчальний заклад "Вінницьке вище професійне училище сфери послуг", Вінниця, Україна.

ORCID: 0009-0009-2133-541X

Authors of the article

Katkov Yuriy – Doctor of Sciences (technical), Associate Professor, Professor of Computer Science Department, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0007-1194-4014

Berezovska Yuliia – PhD (technical), Associate Professor of Computer Science Department, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0000-0002-9973-0497

Lokoida Andriy – master, State University of Information and Communication Technologies, Kyiv, Ukraine.

ORCID: 0009-0000-8110-5098

Lupol Maksim – student, State Vocational Educational Institution "Vinnytsia Higher Vocational School of Service", Vinnytsia, Ukraine.

ORCID: 0009-0009-2133-541X