of Dnipropetrovsk National University of Railway Transport. 2018. Vol. 3(75). S. 67–77. doi: 10.15802/stp2018/133380.
2. Атрилл П., МакЛейни Э. Финансовый менеджмент и управленческий учет для руководителей и бизнесменов; пер. с англ. Москва : Альпина Паблишер, 2012. 648 с.
3. Васильєв О. Л. Джерела фінансування інвестиційної діяльності залізниць. *Міжнародний науковий журнал «Інтернаука».* Серія : Економічні науки. 2018. № 7(15). С. 31–36.

Махницький О. В.,
старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

РИЗИКИ ВИКОРИСТАННЯ СТАРИХ ОПЕРАЦІЙНИХ СИСТЕМ НА ПРИКЛАДІ WINDOWS XP

Нещодавно операційній системі Windows XP виповнилося 20 років, і хоча підтримка цієї операційної системи припинилася в 2014 році, багато людей продовжують використовувати небезпечну версію Windows.

Windows XP була випущена 25 жовтня 2001 р. і вважається однією з найулюбленіших версій Windows завдяки простоті використання, високій продуктивності і стабільності. Сьогодні, після того, як Microsoft випустила Windows 7, 8, 10 і 11, невелика, але пристойна кількість людей все ще використовує стару операційну систему.

Таке постійне використання свідчить про його успіх, але також викликає побоювання щодо відсутності безпеки. Основна підтримка Windows XP закінчилася 14 квітня 2009 р., а розширена підтримка триватиме ще п’ять років. Це означає, що будь-хто, хто все ще працює з Windows XP, не отримував підтримки від Microsoft протягом приблизно 7,5 років, включно з майже всіма оновленнями безпеки та виправленнями вразливостей, які могли бути виявлені.

Це величезна кількість часу для технічних фахівців, і цього більше ніж достатньо, щоб перетворити операційну систему на жах безпеки з великою кількістю незахищених вразливостей. Хоча корпорація Майкрософт зробила виправлення для деяких, найбільш серйозних уразливостей у Windows XP, таких як EternalBlue і BlueKeep, є набагато більше вразливостей, якими можуть скористатися зловмисники. Це робить підключення пристрою Windows XP до Інтернету ризикованою справою, тому всі фахівці з безпеки рекомендують користувачам перейти на підтримувану версію Windows.

Чому застаріла операційна система й досі використовується?

Тим часом як Vista здавалася експериментальним випуском для бета-версії, Windows 7 була відмінним та вдосконаленим випуском, як і Windows

10. Отже, чому в деяких системах досі використовується застаріла версія XP?

Перша категорія систем, які ще використовують Windows XP, – це системи державного сектора, відомі своєю повільною швидкістю оновлення і нерішучістю у використанні нових технологій. Для багатьох державних структур бюрократія, пов'язана із затвердженням закупівель ліцензій на нові системи, оновленням обладнання та навчанням всього державного сектора, є надто складною та дорогою.

Сумісність спеціально створених 32-бітних програмних інструментів – ще одна важлива причина того, що XP все ще зустрічається у багатьох місцях, таких як промислові підприємства, лікарні тощо. Переважно нових версій цих критично важливих інструментів немає або компаніям доводиться платити великі гроші за їх перенесення на нові системи. Потім є категорія людей, які використовують занадто старе та слабке обладнання для правильного запуску нової версії Windows, і вони не бачать вагомих причин змінити те, що все ще (технічно) працює.

Перехід на Linux тільки для кращої підтримки та безпеки не є варіантом для більшості цих людей, тому що, простіше кажучи, Windows XP – це те, до чого вони звикли вже стільки років.

Скільки ще комп'ютерів працює під керуванням Windows XP?

Відповідно до StatCounter, відсоток користувачів Windows, які використовують версію ОС XP у вересні 2021 року, становить 0,59 %, що є великою кількістю, якщо врахувати, скільки систем Windows розгорнуто у всьому світі. Платформа NetMarketShare дає операційній системі Windows XP примітну частку ринку 0,26 % на вересень 2021 року. Якщо перевірити аналітику BleepingComputer, лише за останній місяць маємо 19 000 унікальних відвідувачів, які підключилися до сайту з системами Windows XP. Якщо взяти, наприклад Вірменію, то там Windows XP є найпопулярнішою ОС, на яку припадає 53,5 % користувачів Windows.

Рівень заробітної плати за три з половиною роки зріс на майже 40 %, але все одно перебуває в межах рівня мінімальної оплати праці по країні. Це є одним з головних стримуючих факторів щодо створення привабливого іміджу організації для потенційних майбутніх наукових працівників. Причому ця проблема не має очевидного вирішення у найближчій перспективі через вплив низки як внутрішніх, так і зовнішніх факторів.

До внутрішніх варто віднести відсутність нагальної потреби в залученні молоді до виконання науково-дослідних робіт через майже відсутність нових замовлень та перспективних ринків як всередині, так і поза межами України. Відповідно наявний обсяг робіт цілком спроможні виконати наявні штатні працівники ДП «НДТІ». Також останніми роками спостерігається чітка тенденція до зменшення кількості випускників технічних вузів, які здатні замінити працюючих в науковій установі співробітників пенсійного віку. І йдеться не стільки про низький рівень заробітної плати, скільки про фізичну відсутність молодих фахівців як таких.

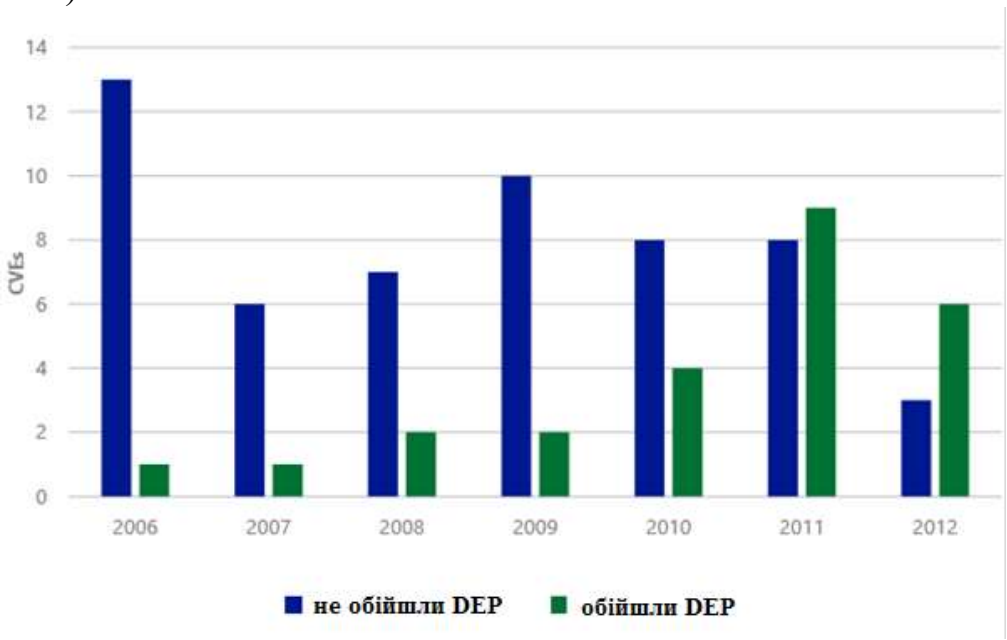
Половина всіх комп'ютерів у Вірменії працює під керуванням Windows XP.

Хоча ринкова частка Windows XP відносно невелика, надто багато організацій та користувачів все ще використовують цю застарілу версію Windows.

Оскільки кібератаки і програми-вимагачі є загрозою, що постійно розвивається, використання застарілих і непідтримуваних систем – занадто великий ризик для організацій, особливо якщо ці пристрої живлять критично важливі системи.

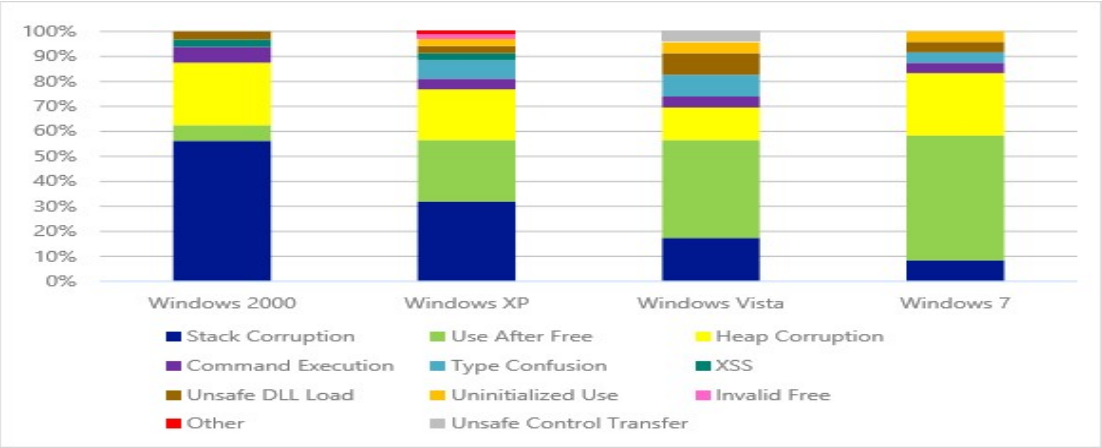
У чому ризик роботи у застарілій операційній системі?

З часом корисність старих захисних механізмів знижується, але не тому, що вони стають менш ефективними власними силами. Справа в тому, що зловмисники навчаються обходити їх, адаптуючись до умов, у яких ці механізми працюють. Хорошим прикладом цієї тези є DEP (Data Execution Prevention).



На діаграмі вище синім кольором позначені вразливості, для яких були випущені експлойти, чия дія звелася б нанівець включеним DEP. Зеленим кольором позначені вразливості, експлуатації яких DEP перешкодити не зміг. Ці дані Microsoft показують, що починаючи з 2009 року все більше і більше вразливостей експлуатується в обхід DEP. Компанія також спостерігає схожий тренд з механізмом ASLR, який обходиться за рахунок атак на ресурси, що не сховалися під парасолькою. Останні 12 місяців у нових клієнтських операційних системах Microsoft було закрито значно менше вразливостей, ніж у попередніх. Звичайно, нові ОС менше поширені, а тому не мають такого гострого інтересу для зловмисників. Однак Microsoft напевно посилює захист, беручи до уваги напрямки атак на свої продукти, що ускладнює експлуатацію вад у безпеці.

Компанія класифікує вразливості за типом експлуатації, і на діаграмі нижче наведено розподіл цих класів у клієнтських ОС, для яких були випущені експлойти з 2006 до 2016 року.



Тут добре видно, що увага зловмисників зміщується у бік експлуатації уразливостей двох класів:

Use after free. Вразливість експлуатується, коли до об’єкта відбувається звернення після звільнення. Зловмисники використовують такі вразливості, щоб змусити програми використовувати свої значення, домагатися падіння програм чи віддаленого виконання коду. Саме цей клас найчастіше експлуатується в атаках Internet Explorer. У Windows 8 на боротьбу з цим відряджена технологія Virtual Table Guard.

Heap Corruption. Вразливість експлуатується шляхом пошкодження стану даних додатків, які зберігаються у його купі (heap). Нерідко це досягається шляхом переповнення буфера купи, що дозволяє взяти під контроль роботу програми. У Windows 8 для протидії таким атакам передбачено механізм Heap Hardening.

Цілком очевидно, що нові захисні заходи є наслідком перегонів озброєнь між виробниками програмного забезпечення та зловмисниками.

Підтвердження цієї тези ви побачите далі. Порівняємо захисні

механізми Windows XP та Windows 8 (див. табл. 1)

Дуже часто один бюлетень стосується всіх продуктів лінійки, випущених у різні роки (наприклад, від Windows XP до Windows 8). Зрозуміло, що підготовка виправлення та його тестування на різних продуктах можуть займати різний час, але бюлетені та латки виходять лише в один день. Тим самим Microsoft нівелює ефект від зворотної розробки виправлень, яка неминуче починається після їх виходу у світ.

Інакше кажучи, якщо випускати, наприклад, виправлення для Windows 7 через місяць після латок для Windows 8, то на цей момент експлойт для вразливостей Windows 7 з XI = 1 вже буде давно готовий.

Таблиця 1

Порівняльний аналіз захисних механізмів Windows XP та Windows 8

	Windows XP SP3 Internet Explorer 8	Windows 8 Internet Explorer 10
SEHOP	No	Yes
Protected Mode	No	Yes
Enhanced Protected Mode (EPM)	No	Yes
Virtual Table Guard	No	Yes
ASLR	Limited	Extensive
Stack randomization	No	Yes
Heap randomization	No	Yes
Image randomization	No	Yes
Force image randomization	No	Yes
Bottom-up randomization	No	Yes
Top-down randomization	No	Yes
High entropy randomization	No	Yes
PEB/TEB randomization	Yes	Yes
Heap hardening	Limited	Extensive
Header encoding	No	Yes
Terminate on corruption	No	Yes
Guard pages	No	Yes
Allocation randomization	No	Yes
Safe unlinking	Yes	Yes
Header checksums	Yes	Yes
/GS	Yes	Yes
Enhanced /GS	No	Yes
SafeSEH	Yes	Yes

На закінчення повторимо деякі тези цієї статті:

– зловмисники навчилися обходити старі захисні механізми;

– до багатьох уразливостей експлойти виходять протягом місяця після випуску виправлень, чому сприяє їхня зворотна розробка;

– нові експлойти для XP обов’язково включатимуться до наборів для атаки;

– захищати стару систему потрібно не безкоштовним антивірусом, а як мінімум, комплексним захисним рішенням (ще краще – SRP чи EMET).

У нових ОС закривається менше вразливостей, тому що їх захисні механізми удосконалюються з урахуванням напрямків атак. Слід завжди користуюся найновішими програмними продуктами Microsoft, у тому числі й тому, що це є безпечнішою практикою. Однак будь-яку ОС та все популярне

ПЗ необхідно оновлювати максимально швидко. Можна рекомендувати включити автоматичне оновлення Windows, а Java та Adobe Reader не встановлювати, щоб зменшити поверхню атаки.

Бібліографічні посилання

1. Microsoft: Software Vulnerabilities Exploitation Trends (PDF).
2. Microsoft Security Intelligence Report: Exploitation Trends.
3. Kaspersky Security Bulletin 2016. Основна статистика за 2016 рік.

Мироненко М. А.,
учений секретар ДП «НДТІ»,
кандидат технічних наук, доцент

Король Р. М.,
директор ДП «НДТІ»,
кандидат технічних наук

АНАЛІЗ ДЕЯКИХ ПОКАЗНИКІВ КАДРОВОГО ТА ФІНАНСОВОГО СТАНУ НАУКОВО-ДОСЛІДНОЇ УСТАНОВИ ДЕРЖАВНОЇ ФОРМИ ВЛАСНОСТІ У 2018 – ІІ кв. 2021 РОКІВ

Державне підприємство «Науково-дослідний та конструкторсько-технологічний інститут трубної промисловості ім. Я. Ю. Осади» (ДП «НДТІ») є розробником технологій виробництва усіх видів труб та балонів, що впроваджені на заводах колишнього СРСР та деяких інших країн.

До складу інституту входять: адміністративно-управлінські підрозділи; 3 науково-дослідних підрозділи; міжрегіональний науково-інженерний центр обґрунтування вимог до якості труб, балонів, іншої металопродукції та забезпечення їх нормативною документацією; науково-інженерний центр з випробування труб, балонів, іншої продукції і матеріалів; центр технічного забезпечення євроінтеграції в металургійній та енергетичній галузях України ENtoUA-VNITI; сектор технології і виробництва виробів спеціального призначення.

У табл. 1 наведено деякі показники кадрового та фінансового стану ДП «НДТІ» за період 2018 – І півріччя 2021 років.

Як випливає із наведеної у табл. 1 інформації, за проаналізований період в інституті відбулося скорочення кількості працівників на 12,5 %. Водночас кількість працівників пенсійного віку збільшилась майже на 30 %, а тих, хто має повну вищу освіту, скоротилась на 5 %.