УДК 004.455.2;004.451:005.5
DOI https://doi.org/10.32689/maup.it.2022.4.1

Віктор БОЙКО
кандидат технічних наук, доцент, доцент кафедри кібербезпеки, Національний університет «Одеська юридична академія», вул. Рішельєвська, 28, Одеса, Україна, індекс 65011 (boyko-work@ukr.net)
ORCID: 0000-0001-5929-657X

Микола ВАСИЛЕНКО
доктор фізико-математичних наук, доктор юридичних наук, професор, професор кафедри кібербезпеки, Національний університет «Одеська юридична академія», вул. Рішельєвська, 28, Одеса, Україна, індекс 65011 (vasylenko.it@journals.maup.kiev.ua)
ORCID: 0000-0002-8555-5712

Валерія СЛАТВІНСЬКА
асистент кафедри кібербезпеки, Національний університет «Одеська юридична академія», вул. Рішельєвська, 28, Одеса, Україна, індекс 65011 (slatvinskaya_valeriya@ukr.net)
ORCID: 0000-0002-6082-981X

Viktor BOYKO
Candidate of Technical Sciences, Associate Professor, Associate Professor at the Department of Cybersecurity, National University "Odesa Law Academy", 28 Richelevska str., Odesa, Ukraine, postal code 65011 (boyko-work@ukr.net)

Nikolai VASILENKO
Doctor of Physical and Mathematical Sciences, Doctor of Law, Professor, Professor at the Department of Cybersecurity, National University "Odessa Law Academy", 28 Richelevskaya str., Odessa, Ukraine, postal code 65011 (vasylenko.it@journals.maup.kiev.ua)

Valeriia SLATVINSKA
Assistant Professor at the Department of Cybersecurity, National University "Odessa Law Academy", 28 Richelevskaya str., Odessa, Ukraine, postal code 65011 (slatvinskaya_valeriya@ukr.net)

Бібліографічний опис статті: Бойко, В., Василенко, М., Слатвінська, В. (2022). Практичні аспекти організації користувацьких процесів для робочих станцій загального доступу. *Інформаційні технології та суспільство*, 4 (6), 6–13. DOI: https://doi.org/10.32689/maup.it.2022.4.1

Bibliographic description of the article: Boyko, V., Vasilenko, M., Slatvinska, V. (2022). Praktychni aspekty orhanizatsii korystuvatskykh protsesiv dlia robochykh stantsii zahalnoho dostupu [Practical aspects of organizing user processes for public access workstations]. *Informatsiini tekhnolohii ta suspilstvo – Information technology and society*, 4 (6), 6–13. DOI: https://doi.org/10.32689/maup.it.2022.4.1

ПРАКТИЧНІ АСПЕКТИ ОРГАНІЗАЦІЇ КОРИСТУВАЦЬКИХ ПРОЦЕСІВ ДЛЯ РОБОЧИХ СТАНЦІЙ ЗАГАЛЬНОГО ДОСТУПУ

*При адмініструванні локальних мереж виокремлено особливий клас завдань, де локальна мережа, що адмініструється, має так звані робочі станції "загального доступу" (РСЗД). **Метою статті** є аналіз і вирішення практичних питань організації користувацьких процесів для робочих станцій загального доступу, робота яких дає змогу підвищити ефективність роботи інформаційних систем в цілому. Проаналізовано роботу таких станцій з позиції практичної організації користувацьких процесів. **Наукова новизна.** Проаналізовано підходи до організації РСЗД і сформовано три основні. Перший (автономного типу) надзвичайно рідко проектується "з нуля". Тут зазвичай проєктування на стадії впровадження зводиться до вибору типового апаратно-програмного рішення (конфігурація hardware, тип операційної системи), яке слугує платформою для програмного забезпечення робочого місця оператора. Другий підхід такий, коли операторам пропонується самим приносити із собою свої робочі місця в умовах обмежень, які регламентують, що саме може принести користувач. Третій – "гібридний", що поєднує в собі перший і другий підходи. Проаналізовано проблеми РСЗД автономного типу. Надано різні підходи до вирішення проблем РСЗД автономного типу. Користувацький підхід породжує набагато більше проблем, ніж вирішує. Флеш-драйви дуже швидко перетворюються на переносники і розповсюджувачі шкідливого ПЗ. З погляду системного адміністратора існує одразу кілька шляхів розв'язання проблеми РСЗД: використання LDAP-системи, встановлення додаткового ПЗ, що виконує функції як забезпечення безпеки, так і заборони доступу до налаштувань і ресурсів операційної системи, заміна операційної системи. Надані практич-*

*ні рекомендації для переведення РСЗДів на платформу з відкритим ПЗ. Як **висновок**, у статті наголошується на необхідності переведення РСЗДів на платформу з відкритим ПЗ з огляду на серйозні проблеми з конфіденційністю, проблеми "розбитих вікон".*

***Ключові слова:** користувач, доступ, локальна мережа, користувацький режим, конфіденційність, адміністратор системи.*

PRACTICAL ASPECTS OF ORGANIZING USER PROCESSES FOR PUBLIC ACCESS WORKSTATIONS

*When administering local area networks, a special class of tasks is distinguished, where the administered local network has the so-called "public access" workstations (PAWS). **The purpose** of the article is to analyze and solve practical issues of organizing user processes for public access workstations, the work of which allows to increase the efficiency of information systems in general. The work of such stations is analyzed from the point of view of practical organization of user processes. **Scientific novelty.** Approaches to the organization of PAWS are analyzed and three main ones are formed. The first (autonomous type) is extremely rarely designed from scratch. Here, usually, the design at the implementation stage is reduced to the choice of a typical hardware and software solution (hardware configuration, type of operating system), which serves as a platform for the operator's workstation software. The second approach is when operators are encouraged to bring their own workstations with them, subject to restrictions that regulate what the user can bring. The third is a "hybrid" approach that combines the first and second approaches. The problems of autonomous type PAWSare analyzed. Different approaches to solving the problems of autonomous type PAWS are presented. The custom approach generates much more problems than it solves. Flash drives very quickly turn into carriers and distributors of malicious software. From the point of view of a system administrator, there are several ways to solve the problem of PAWS: using an LDAP system, installing additional software that performs the functions of both ensuring security and denying access to the settings and resources of the operating system, replacing the operating system. Practical recommendations are given for the transfer of flash drives to the platform with open software. As a **conclusion**, the article emphasizes the necessity of transferring the PCSD to the platform with open software, given the serious problems with confidentiality, the problem of "broken windows".*

***Key words:** user, access, local network, user mode, confidentiality, system administrator.*

Актуальність проблеми. У загальному адмініструванні локальних мереж можна виокремити особливий клас завдань, за якого локальна мережа, що адмініструється, має так звані робочі станції "загального доступу" (РСЗД), роботу на яких можуть здійснювати різні користувачі в різний час, оскільки утримувати окреме робоче місце для кожного оператора заздалегідь збитково, або принципово неможливо. Незважаючи на те, що корпоративні мережі зазвичай використовують безліч операційних систем, особливо на серверах, на більшості робочих станцій, призначених для користувача, зазвичай установлена одна із версій Windows. Немає жодних сумнівів у тому, що адміністрування серверів та сотень тисяч робочих станцій Windows являє собою вкрай масштабну задачу. Так, операційні системи Windows містять різні інструменти, які адміністратори мереж можуть застосовувати для полегшення процесів установлення, керування й обслуговування операційних систем великої кількості серверів і робочих станцій. На початку розвитку інформаційно-комунікаційних систем організація таких локальних мереж із "точками загального доступу" мала на меті насамперед забезпечити робочим місцем безліч користувачів, які або не мають домашніх робочих місць, або мають такі, але недостатньо "обчислювально озброєні". Найчастіше РСЗД використовували в інтернет-кафе, комп'ютерних класах у навчальних закладах, як робочі станції в місцях колективних систем автоматизованого проєктування тощо [1]. Нині парадигма використання РСЗД змінилася. На це вплинуло два фактори.

Перший з них представляє собою зростання "обчислювальної озброєності" окремого користувача. Зараз складно уявити людину, яка не має пристрою, під'єднаного до мережі, і не має доступу до обчислювальних систем узагалі. При цьому питома вартість пристроїв у перерахунку на доступні обчислювальні потужності сильно знизилася настільки, що більш-менш потужний пристрій може дозволити собі більшість користувачів (або їх може бути забезпечено ними за рахунок наймача).

Другий обумовлений пандемією коронавірусу, яка призвела до розвитку і збільшення доступності технологій дистанційної роботи та збільшення частки працівників, які працюють дистанційно.

Усе це зумовлює актуальність питань проектування, організації та безпечної експлуатації РСЗД.

Аналіз останніх досліджень і публікацій. Організація користувацьких процесів для робочих станцій загального доступу все ще залишається проблемою, яка заслуговує вирішення в практичній площині. Так, більшість експертів сходиться в тому, що робочий процес у нових умовах хоча й зазнає зсуву в бік "домашнього офісу", але дистанційна робота не зможе зайняти нішу повністю в осяжний час. Однак систематизованих робіт, присвячених різним практичним питання цієї проблеми через "розмитість" небагато. Так, у дослідженнях [2] та [3] наголошується, що роль офісної роботи та "гібридного режиму"(часткової роботи, де робота з офісу поєднується з роботою з дому) не стільки зменшується, скільки змінюється. Існує великий сегмент завдань, які не можуть бути перерозподілені "додому", оскільки подібний підхід може так чи інакше зачіпати інтереси стейкхолдера.

Насамперед це зростання уваги до питань особистої та корпоративної конфіденційності та приватності. У багатьох випадках, робота з чутливою інформацією "вдома" або в хмарах може створювати неприйнятні ризики. При цьому, зазначимо, що часто цим ризикам не приділяється належної уваги (див. роботу [4]). Ще один характерний приклад являє собою, великий сегмент, що представляє собою промислові системи управління (Industrial control system – ICS). Сюди можна включити і робочі місця різних операторів (наприклад, управління дорожнім трафіком), але вони принципово не допускають роботи з дому.

При цьому, як і у випадку з системами з конфіденційною інформацією, під час проєктування та експлуатації ICS до останнього часу не приділяли достатньо уваги питанням роботи з конфіденційною інформацією. Наприклад, під час аналізу безпеки таких систем нерідко з'ясовується, що розробники за інерцією схильні переоцінювати захист організованих у такий спосіб систем і покладаються на захист спільного роутера або шлюзу, що обмежує локальну мережу від зовнішнього світу, або на так званий "air gap" – "повітряний зазор", який ізолює мережу від глобальних інформаційно-комунікаційних систем. На їхню думку, керуюча система, не під'єднана до інтернету, не може піддатися атаці. Що спростовується практикою – один із найперших прикладів атаки – вірус Stuxnet, якраз був побудований на подоланні "повітряного зазору" ([5]). Таким чином ризику і небезпеки піддаються навіть системи, які не підключені до інтернету безпосередньо.

Таким чином, необхідність у РСЗД не стільки знижується, скільки змінюється в загальному тренді – з одного боку, скорочується загальна кількість таких систем, оскільки дедалі більше роботи перемикається на аутсорс або на дистанційну роботу, з іншого боку, ті системи РСЗД, що вводяться в експлуатацію, призначені для роботи із дедалі ціннішою та чутливішою інформацією, а відтак потребують більшої уваги, якої до останнього часу їм не приділяли.

Метою статті є аналіз і вирішення практичних питань організації користувацьких процесів для робочих станцій загального доступу, робота яких дає змогу підвищити ефективність роботи інформаційних систем в цілому.

Виклад основного матеріалу.

Основні підходи до організації РСЗД

У різних організаціях ця проблема може вирішуватися по-різному. Можна виділити кілька найпоширеніших підходів до організації РСЗД.

Перший – "автономний". Такий підхід передбачає проєктування й оснащення РСЗД апаратно-програмними рішеннями "з нуля". Для цього методу характерне таке – робочі станції та автоматизовані робочі місця рідко проєктуються "з нуля". Це пов'язано з тим, що такий процес досить витратний, вимагає безперервного контролю за оновленнями робочих конфігурацій і профілів. Тому, на практиці, якщо робота оператора не вимагає специфічного апаратно-програмного комплексу (наприклад, системи управління технологічним процесом), прагнуть дійти до здешевленого з точки зору витрат коштів і часу типового рішення. Зазвичай обирають або проектують необхідну апаратну конфігурацію десктопа або ноутбука, на нього встановлюють типову операційну систему, далі на неї встановлюють і конфігурують необхідне для забезпечення робочого процесу програмне забезпечення. Ми повернемося до розгляду автономного РСЗД нижче.

Другий – описується абревіатурою BYOD – bring your own device [6]. Операторам пропонується самим приносити із собою свої робочі місця (ноутбуки, планшети, смартфони тощо), при цьому можуть існувати обмежувальні або розпорядчі корпоративні політики, які регламентують, що саме може принести користувач. У роботі [7] наводяться характерні патерни впровадження та використання подібних політик в австралійських лікарнях. Зокрема описано всі вразливі моменти та недоліки, з якими політика BYOD може зіткнутися на практиці: втрата або крадіжка робочого пристрою, ризики для приватності та конфіденційності інформації тощо. Так само в цій роботі наведено розгорнуту характеристику робочого процесу – які саме пристрої та операційні системи використовуються для організації робочого місця, яка частина персоналу проходить тренінги, пов'язані з питаннями кібербезпеки тощо.

Третій – "гібридний", що поєднує в собі перший і другий підходи.

Розглянуті нами підходи не зачіпають ширший спектр проблем. Наприклад, схожий спектр проблем існує під час використання РСЗД у так званому "режимі одного застосунку" (single-app mode) або "режимі кіоску" (kiosk mode). У цих режимах, як випливає з назви, користувач під час роботи в РСЗД обмежений одним, спеціально спроєктованим застосунком, обслуговування такого РСЗД, як правило, здійснюється дистанційно та має свою специфіку [8], [9].

Для другого підходу (BYOD), характерно, що фахівці з кібербезпеки часто розшифровують абревіатуру BYOD ("Bring Your Own Device" – "приносьте своє робоче місце з собою"), як "Bring Your Own Danger" ("приносьте свою потенційну загрозу з собою"), маючи на увазі, що разом зі своїм пристроєм

користувач носить ризики і загрози. Ці ризики та загрози можуть бути пов'язані як з особливостями апаратно-програмного забезпечення, так і з компетентністю самого користувача. Цей підхід для гарантування безпеки та купірування ризиків вимагає широкого спектра заходів, частина з яких розглянута в роботах [10], [11], [12]. Обмежимося загальним зауваженням, що захист конфіденційності інформації та інші заходи безпеки як за підходу BYOD, так і в разі гібридного підходу, найчастіше зводяться до обмежувальних корпоративних політик, коли апаратно-програмне забезпечення суворо регламентують або згідно з "чорним списком" (не використовувати апаратно-програмні засоби з переліку), або згідно з "білим списком" (не використовувати нічого, крім списку дозволених систем). Розгляд цього підходу також виходить за рамки цієї роботи.

Проблеми РСЗД автономного типу

Як було описано вище, РСЗД автономного типу надзвичайно рідко проектується "з нуля". Зазвичай проєктування на стадії впровадження зводиться до вибору типового апаратно-програмного рішення (конфігурація hardware, тип операційної системи), яке слугує платформою для програмного забезпечення робочого місця оператора. При цьому найчастіше все обслуговування робочого місця: конфігурація операційної системи, налаштування призначеного для користувача програмного забезпечення, файерволи тощо залишається на розсуд системного адміністратора, а іноді й самих користувачів, які використовують РСЗД.

Такий підхід несе в собі серйозні ризики: однорідність РСЗД-ів за їхньої великої кількості створює велику і дуже вразливу "поверхню атаки". При цьому, оскільки компетентність і кваліфікація операторів може сильно відрізнятися від людини до людини, що створює систему "слабкої ланки", за якої ризики досить великі.

Крім того, існують особливості, пов'язані з використанням різних сімейств операційних систем. Найчастіше для організації РСЗД використовують операційну систему сімейства Microsoft Windows, використання якої пов'язане з деякими специфічними труднощами. Насамперед система роботи з користувачами і правами являє собою досить заплутану і незручну процедуру – при цьому Microsoft не робить жодних кроків для виправлення ситуації [13], [14] оскільки зараз основна стратегія корпорації полягає у переведенні операційної системи зі статусу десктопної у статус SaaS-платформи, де робота тісно зав'язана на використання онлайнового облікового запису – і можливість отримання регулярних платежів за користування цим обліковим записом.

У результаті серед домашніх користувачів цієї системи широко поширився "квазі-однокористувацький режим". У такому режимі, не дивлячись на наявність в операційної системи засобів для організації багатокористувацької роботи, користувач прагне виконувати всю ключову роботу під одним налаштованим під час установлення користувачем, водночас найчастіше цей користувач є (або має права) адміністратора системи. Крім потенційних проблем, які викликають такий режим роботи під час роботи на домашньому (або робочому комп'ютері) [15], [16], його використання в системах РСЗД посилює основні проблеми безпеки.

Робота у квазі-однокористувацькому режимі є доволі поширеною практикою від самого початку використання операційних систем цього сімейства, і вона через інерцію користувачів поширилася і на комп'ютерні класи більшості навчальних закладів та робочі станції інтернет-кафе, а нині і на серйозніші РСЗД, описані вище. Такий РСЗД використовується в режимі "одна роль операційної системи для всіх працюючих за комп'ютером користувачів". При цьому, оскільки механізми поділу користувачів не задіюються, їхні файли, системні налаштування і установки неминуче змішуються. Це призводить відразу до кількох негативних явищ.

Перше – це серйозна проблема з конфіденційністю. За такого режиму кожен з користувачів має вільний доступ до чужих робочих файлів, що є великою проблемою з погляду безпеки, особливо для РСЗД, які використовуються для роботи з чутливими даними. Крім того, користувач може самостійно встановити на РСЗД програмне забезпечення (ПЗ), яке стежить, і таким чином зібрати інформацію про інших користувачів і про їхні дії на РСЗД.

Друге – "ефект розбитих вікон". Згідно з "теорією розбитих вікон" (англ. broken windows theory), дрібні порушення правил у суспільно-доступній системі (розбите вікно в будівлі) провокують дедалі більше таких порушень (що характеризуються місткою фразою "іншим можна, а мені не можна?") і внаслідок цього система позбавляється більшої частини свого ресурсу (у будівлі не залишається жодного цілого вікна) [17]. Цю теорію спочатку використовували для пояснення механізмів і динаміки криміногенної обстановки в межах міста [18] і в цій ролі часто критикували, однак її положення цілком можна поширити на використання операційної системи без поділу на користувацькі ролі.

Рідко виходить так, що всі користувачі РСЗД суворо дотримуються писаних і неписаних правил використання файлового простору, налаштування призначеного для користувача ПЗ і конфігурації

операційної системи. Порушення правил одним користувачем провокує на порушення правил іншими користувачами. Це поступово призводить до того, що поведінка користувачів одного комп'ютера стає дедалі менш щадною і шанобливою по відношенню один до одного. Іноді таке ставлення може провокувати ворожість між користувачами. При цьому дрібні порушення можуть перерости в цілеспрямований вандалізм. Це відбувається рідко, хоча автору кілька разів доводилося спостерігати розвиток конфліктів, які починалися з установки заставок на робочих столах провокуючого змісту і закінчувалися використанням шкідливого ПЗ та викраденням особистих даних з кешу браузера (або просто з незакритої через забудькуватість сесії роботи).

При цьому, можливості навести лад у таких системах досить обмежені. У разі вандалізму в РСЗД, яким користується досить велика кількість користувачів, рідко можна визначити конкретного порушника без складного і витратного за часом і ресурсами дослідження системних журналів, навести лад у файлах теж складно, оскільки кожен користувач вважає свої файли цінними та активно чинить опір їхньому упорядкуванню.

За всієї зовнішньої незначності, такий режим роботи і створює атмосферу безладу і хаосу і – згідно з тією ж "теорією розбитих вікон" – впливає на якість робочого процесу.

Різні підходи до вирішення проблем РСЗД автономного типу

Суто користувацький підхід у розв'язанні проблеми конфіденційності під час користування РСЗД полягає у відмові від постійного зберігання файлів на робочому місці та переходу на використання сторонніх носіїв (найчастіше usb флеш-драйвів або хмарних сервісів). При цьому файли копіюються на робоче місце, з ними відбувається робота. Далі вони зберігаються назад на флеш-драйв (або в хмару), після чого файли, що залишилися на робочому місці, видаляються. Це вирішує проблему тільки частково – використання файлів так чи інакше залишає слід. Крім того, як зазначалося вище, на комп'ютер може бути встановлено різне ПЗ, що стежить.

Такий підхід породжує набагато більше проблем, ніж вирішує. Флеш-драйви дуже швидко перетворюються на переносники і розповсюджувачі шкідливого ПЗ. Крім того, копіювання файлів займає час і забирає енергію, "від'їдаючи" її в робочого процесу і працюючи таким чином як своєрідне "тертя". Найчастіше використання таких заходів швидко сходить нанівець, і комп'ютер перетворюється на хаотичне нагромадження різних файлів, яке в системних адміністраторів отримало окремий термін – "файлопомийок", що часто провокує й посилює проблему "розбитих вікон".

З погляду системного адміністратора існує одразу кілька шляхів розв'язання проблеми РСЗД.

Питання ідентифікації користувача в РСЗД часто прагнуть обійти за допомогою використання LDAP-системи, яка в ідеальному випадку повинна добре справлятися з аутентифікацією користувача і в теорії може надавати йому доступ на дозволених РСЗД, але, з іншого боку, є складною в налаштуванні та вимогливою до умов експлуатації та кваліфікації персоналу (про проблеми з розгортанням LDAP див. [19]) – і теж породжує більше проблем, ніж розв'язує.

Очевидні недоліки в безпеці та незручності такого режиму використання операційної системи користувачі й адміністратори системи прагнуть компенсувати за рахунок встановлення додаткового ПЗ, що виконує функції як забезпечення безпеки, так і заборони доступу до налаштувань і ресурсів операційної системи. Плюс зазвичай встановлюють різне стороннє ПЗ, що обмежує функціональність і саме собою є проблемою.

Таке "блокуюче ПЗ" не тільки має сумнівну ліцензійну чистоту і потенційно несе в собі додаткові загрози безпеці, а й насамперед значно ускладнює навчальний процес, оскільки для встановлення та оновлення необхідного програмного забезпечення (а також відкриття прав і доступу, які це ПЗ вимагає) доводиться звертатися до системного адміністратора. При цьому хоча "блокуюче ПЗ" створює хибну ілюзію відносної безпеки, його механізми захисту і блокування розраховані на некваліфікованого користувача і досить просто обходяться, а крім того, створюють мінімальну перешкоду (або не створюють її зовсім) для різного шкідливого ПЗ. Таке ПЗ не може перешкодити поширенню вірусів, троянів, хробаків і так далі.

Не дивлячись на перераховані недоліки, описані вище підходи є доволі прийнятними (з різним ступенем придатності залежно від необхідності та серйозності поставлених проблем), однак, на наш погляд, найрадикальнішим способом розв'язання проблеми є заміна операційної системи, у тих випадках, коли це є можливим. Під час вибору зміни операційної системи слід враховувати, що загалом, серед розробників і професіоналів в IT-галузі склався стійкий тренд до збільшення і розширення використання засобів відкритого ПЗ. Наприклад, згідно з опитуванням Forrester Research від 2014-го року [1] 84% розробників (зокрема, з компаній із пропрієтарним ПЗ) використовують програмне забезпечення з відкритим вихідним кодом. При цьому більша частина розробників використовує ПЗ з огляду на його продуктивність і надійність, у більшості випадків вартість відіграє для них останню чергу.

Це, зокрема, остільки, оскільки пропрієтарні, закриті вихідні коди, протоколи взаємодії та формати даних, не дивлячись на свою привабливість – "вирішимо всі ваші проблеми" (розробник бере на себе поставку і розгортання системи "під ключ", а також забезпечує подальшу технічну підтримку), на практиці породжують безліч проблем.

Серед них: "vendor lock-in" – прагнення постачальників послуг замкнути клієнта на себе, монополізувавши надання послуги, можлива наявність "чорних ходів" ("backdoors"), невиправдане роздмухування обсягів ПЗ і підвищення вимог до парку апаратного забезпечення, який використовується, тощо. Крім того, під час використання закритого програмного забезпечення, виникає ризик втрати можливості обслуговування системи в тому разі, якщо її розробник збанкрутує, піде з ринку або його компанія буде поглинена іншим розробником.

Усе це слугує суттєвим аргументом на користь використання відкритого ПЗ під час проєктування автономних РСЗДів. Більшість POSIX-сумісних систем мають спільного предка – систему UNIX, яку від самого початку проєктували як багатокористувацьку систему зі зручним керуванням користувачами, користувацькими профілями та налаштуваннями, а її "ідеологічні спадкоємці" містять оптимально організовані засоби керування поділом користувачів між собою.

Досвід переведення робочих процесів на відкрите ПЗ дав змогу виробити такі практичні рекомендації.

Переведення РСЗДів на платформу з відкритим ПЗ

Основним принципом при переході на відкрите ПЗ має бути поступовість і посильність процесу переходу. Будь-яка зміна ПЗ неминуче пов'язана зі зміною робочих процесів, а отже, з "дитячими хворобами", з добором нових інструментів і – що особливо важливо – зі зміною звичок і організації робочих процесів, оскільки людський чинник складає істотну частину. Найгіршою є ситуація "потрібно було вчора".

Для забезпечення поступовості впровадження слід дотримуватися таких рекомендацій.

– проаналізуйте, які Open Source засоби та відкриті формати даних ви можете використовувати вже зараз – під поточною операційною системою

Суттєва частина відкритого ПЗ є кросплатформеною – тобто існує в різних версіях для різних операційних систем та архітектур. Тому процес впровадження, навчання та використання відкритого ПЗ можна починати навіть не змінюючи платформу, а поступово змінюючи користувацьке ПЗ. Наприклад, змінити поштовий клієнт на Mozilla Thunderbird, як офісний пакет використовувати Libre Office тощо.

– вивчіть відмінності платформи на яку збираєтеся перейти

У різних операційних систем часто набагато більше спільного, ніж різного, оскільки існує своєрідний аналог біологічної конвергенції для комп'ютерних систем. Однак, деякі існуючі відмінності можуть збивати з пантелику, ускладнюючи перехід. До цього слід бути готовим.

– почніть перехід з використання відкритого ПЗ, відкритих форматів даних і вибудовування робочих процесів на поточній робочій платформі

Як було сказано вище, це цілком здійснено в більшості випадків.

– проведіть поступовий перехід, зберігаючи можливість повернення до платформи

З нашого досвіду, найоптимальніша схема – це впровадження пілотного проєкту, для поступового переведення користувачів на нову систему. Як було сказано вище, слід бути готовим до "дитячих хвороб" впровадження – і схема з пілотним проєктом дає змогу розв'язати ці проблеми "малою кров'ю" без істотних втрат, пов'язаних із несподіваними труднощами впровадження.

Зазвичай впровадження починається з кількох РСЗДів, які слугують полігоном для виявлення всіх помилок і проблем впровадження. У міру освоєння системи "поверхня впровадження" розширюється, займаючи дедалі більше РСЗДів. При цьому на кожному етапі зберігається можливість повернення на попередній етап, якщо в цьому виникне необхідність.

– відмовтеся від перфекціонізму

Іноді в проєктах може вимагатися наявність старих систем. У цьому разі розумно буде залишити кілька старих ділянок доти, доки подальше зростання освоєння нових систем не дасть змоги замінити їх або перейти на використання віртуальних оточень – словом, якимось чином розв'язати проблему.

– продовжуйте вивчати нові засоби нової платформи

Вибір схожого ПЗ і схем роботи полегшує зміну систем і перехідний період, однак, часто (і це характерно для відкритого ПЗ) можна значно підвищити ефективність використання ПЗ, якщо задіяти сильні та унікальні сторони наявних систем.

Наприклад, LibreOffice, який зазвичай використовується в режимі "безкоштовний Microsoft Word", містить у собі такі додаткові інструменти, як зручний навігатор по документу, html/css-подібну систему задання стилів документа, складові документи (робота здійснюється через майстер-документ, що

містить у собі посилання на інші документи), систему полів, систему бібліографії, генератор змісту документа на основі стильової системи, систему текстового задання математичних формул, схожу на LaTeX тощо. Усе це, поряд із вбудованим експортом у pdf-файли, робить LibreOffice зручним і потужним інструментом, а не тільки "безкоштовним варіантом текстового процесора".

Однак, "глибоке освоєння" теж має бути поступовим і посильним. До нього слід переходити тільки після завершення переходу і виведення робочих процесів в оптимальний режим.

Висновки та перспективи подальших досліджень. Проаналізовано еволюцію розвитку організації користувацьких процесів для робочих станцій загального доступу. З погляду системного адміністратора з'ясовано, що існує одразу кілька шляхів розв'язання проблеми РСЗД: використання LDAP-системи, встановлення додаткового ПЗ, що виконує функції як забезпечення безпеки, так і заборони доступу до налаштувань і ресурсів операційної системи, заміна операційної системи. Доведена необхідність переведення РСЗДів на платформу з відкритим ПЗ з огляду на серйозні проблеми з конфіденційністю, проблеми "розбитих вікон". Перспективним для подальшого дослідження є питання адміністрування користувачів в операційній системі WINDOWS.

Список використаних джерел:

1. *Rastogi U.* Computer Network And Its Consequences – A Literature Survey. *International Journal of Health, Education & Social (IJHES).* 2019. Vol. 2, no. 11. P. 5–19.
2. *Wang Y., Liu Y., Cui W., Tang J., Zhang H., Walston D., Zhang D.* Returning to the Office During the COVID-19 Pandemic Recovery: Early Indicators from China / Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems. ACM, 2021.
3. *Parker L. D.* The COVID-19 office in transition: cost, efficiency and the social responsibility business case. *Accounting, Auditing and Accountability Journal.* Emerald, 2020. Vol. 33, no. 8. P. 1943–1967.
4. *Matisāne L., Paegle L., Akūlova L., Vanadziņš I.* Challenges for Workplace Risk Assessment in Home Offices-Results from a Qualitative Descriptive Study on Working Life during the First Wave of the COVID-19 Pandemic in Latvia. *International Journal of Environmental Research and Public Health.* 2021. Vol. 18, no. 20. P. 1–19.
5. *Barzashka I.* Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme. *The RUSI Journal. Taylor & Francis.* 2013. Vol. 158, no. 2. P. 48–56.
6. *What is BYOD? | IBM*. URL: https://www.ibm.com/topics/byod (дата звернення: 2023-01-10).
7. *Wani T. A., Mendoza A., Gray K., Smolenaers F.* Status of bring-your-own-device (BYOD) security practices in Australian hospitals A national survey. *Health Policy and Technology. Elsevier BV,* 2022. Vol. 11, no. 3. P. 100627.
8. *5 Kiosk Security Strategies That Businesses Should Know*. URL: https://blog.scalefusion.com/strategies-to-secure-your-public-facing-kiosks/ (дата звернення: 2023-01-10).
9. *Cyber attack threats to kiosks*. URL: https://www.sourcesecurity.com/insights/self-service-kiosks-target-cyber-attacks-physical-security-co-1540547340-ga.1543319929.html (дата звернення: 2023-01-10).
10. *Olalere M., Abdullah M. T., Mahmod R., Abdullah A.* A Review of Bring Your Own Device on Security Issues. SAGE Open. SAGE Publications, 2015. Vol. 5, no. 2. P. 215824401558037.
11. *Disterer G., Kleiner C.* BYOD Bring Your Own Device // Procedia Technology. Elsevier BV, 2013. Vol. 9. P. 43–53.
12. *Blizzard S.* Coming full circle: are there benefits to BYOD? *Computer Fraud and Security. Mark Allen Group,* 2015. Vol. 2015, no. 2. P. 18–20.
13. *Report: Microsoft makes it difficult to create local accounts in Windows 10*. URL: https://www.ghacks.net/2019/09/30/report-microsoft-makes-it-difficult-to-create-local-accounts-in-windows-10/ (дата звернення: 2023-01-11).
14. *How (and Why) to Create a Separate Windows Account Just for School | PCMag*. URL: https://www.pcmag.com/how-to/how-and-why-to-create-a-separate-windows-account-just-for-school (дата звернення: 2023-01-11).
15. *Both D.* Working As Root // Using and Administering Linux: Volume 1. Apress, 2019. P. 283–307.
16. *The 21 worst tech habits – and how to break them – ARN*. URL: https://www.arnnet.com.au/article/459900/21_worst_tech_habits_-_how_break_them/?fp=2&fpid=2 (дата звернення: 2023-01-11).
17. *Wilson J. Q., Kelling G. L.* "Broken Windows": Atlantic Monthly (1982). The city reader. Routledge, 2011. P. 309–319.
18. *HARCOURT B. E., LUDWIG J.* Reefer madness: broken windows policing and misdemeanor marijuana arrests in New York city, 1989–2000. Criminology and Public Policy. Wiley, 2007. Vol. 6, no. 1. P. 165–181.
19. *Ito E., Kasahara Y., Fujimura N.* Implementation and operation of the Kyushu university authentication system. Proceedings of the 41st annual ACM SIGUCCS conference on User services. ACM, 2013.

References:

1. *Rastogi U.* (2019). Computer Network And Its Consequences – A Literature Survey. International Journal of Health, Education & Social (IJHES). Vol. 2, no. 11. 5–19. [in English].
2. *Wang Y., Liu Y., Cui W., Tang J., Zhang H., Walston D., Zhang D.* (2021). Returning to the Office During the COVID-19 Pandemic Recovery: Early Indicators from China / Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems. ACM. [in English].
3. *Parker L. D.* (2020). The COVID-19 office in transition: cost, efficiency and the social responsibility business case. Accounting, Auditing and Accountability Journal. Emerald, Vol. 33, no. 8. 1943–1967. [in English].

4. *Matisāne L., Paegle L., Akūlova L., Vanadziņš I.* (2021). Challenges for Workplace Risk Assessment in Home Offices-Results from a Qualitative Descriptive Study on Working Life during the First Wave of the COVID-19 Pandemic in Latvia. International Journal of Environmental Research and Public Health. Vol. 18, no. 20. 1–19. [in English].

5. *Barzashka I.* (2013). Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme. The RUSI Journal. Taylor & Francis, Vol. 158, no. 2. 48–56. [in English].

6. *What is BYOD? | IBM*. URL: https://www.ibm.com/topics/byod [in English].

7. *Wani T. A., Mendoza A., Gray K., Smolenaers F.* (2022). Status of bring-your-own-device (BYOD) security practices in Australian hospitals A national survey. Health Policy and Technology. Elsevier BV, Vol. 11, no. 3. 100627. [in English].

8. *5 Kiosk Security Strategies That Businesses Should Know*. Retrieved from https://blog.scalefusion.com/strategies-to-secure-your-public-facing-kiosks/ [in English].

9. *Cyber attack threats to kiosks*. Retrieved from https://www.sourcesecurity.com/insights/self-service-kiosks-target-cyber-attacks-physical-security-co-1540547340-ga.1543319929.html [in English].

10. *Olalere M., Abdullah M. T., Mahmod R., Abdullah A.* (2015). A Review of Bring Your Own Device on Security Issues // SAGE Open. – SAGE Publications, Vol. 5, no. 2. 215824401558037. [in English].

11. *Disterer G., Kleiner C.* (2013). BYOD Bring Your Own Device // Procedia Technology. – Elsevier BV, Vol. 9. 43–53. [in English].

12. *Blizzard S.* (2015). Coming full circle: are there benefits to BYOD? // Computer Fraud and Security. – Mark Allen Group, no. 2. 18–20. [in English].

13. *Report: Microsoft makes it difficult to create local accounts in Windows 10*. Retrieved from https://www.ghacks.net/2019/09/30/report-microsoft-makes-it-difficult-to-create-local-accounts-in-windows-10/ [in English].

14. *How (and Why) to Create a Separate Windows Account Just for School | PCMag*. Retrieved from https://www.pcmag.com/how-to/how-and-why-to-create-a-separate-windows-account-just-for-school [in English].

15. *Both D.* (2019). Working As Root. Using and Administering Linux: Volume 1. Apress, 283–307. [in English].

16. *The 21 worst tech habits – and how to break them – ARN*. Retrieved from https://www.arnnet.com.au/article/459900/21_worst_tech_habits_-_how_break_them/?fp=2&fpid=2 [in English].

17. *Wilson J. Q., Kelling G. L.* (2011). "Broken Windows": Atlantic Monthly (1982) // The city reader. — Routledge, 309–319. [in English].

18. *HARCOURT B. E., LUDWIG J.* (2007). Reefer madness: broken windows policing and misdemeanor marijuana arrests in New York city, 1989-2000. Criminology and Public Policy. Wiley, Vol. 6, no. 1. 165–181. [in English].

19. *Ito E., Kasahara Y., Fujimura N.* (2013). Implementation and operation of the Kyushu university authentication system. Proceedings of the 41st annual ACM SIGUCCS conference on User services. ACM. [in English].