УДК 004.75

Драглюк О. В. ORCID: 0000-0001-8572-7257 (ВІТІ)
Радченко М. М. ORCID: 0000-0002-8272-0727 (ВІТІ)
Коротков М. М. ORCID: 0000-0002-1683-0661 (ВІТІ)
Павлюк Д. О. ORCID: 0000-0001-8461-3899 (ВІТІ)

ЗАСТОСУВАННЯ ТЕХНОЛОГІЙ VIRTUAL DESKTOP INFRASTRUCTURE В ІНФОРМАЦІЙНИХ ІНФРАСТРУКТУРАХ УЧАСНИКІВ СЕКТОРУ БЕЗПЕКИ ТА ОБОРОНИ

З метою виконання завдань Стратегій національної та воєнної безпеки України щодо забезпечення упровадження сучасних інформаційних технологій, автоматизації управлінських процесів і цифровізації діяльності в силах оборони України з відповідним рівнем захищеності інформації, що обробляється, проводяться заходи щодо приведення існуючої інформаційної інфраструктури до сучасних вимог.

Технічна компонента інформаційної інфраструктури органів управління учасників сектору безпеки та оборони зазвичай складається з наборів інформаційних та інформаційно-аналітичних систем, які різні за призначенням, але однакові за практичною реалізацією в технологіях "товстого" та "тонкого" клієнтів (термінального сервера) клієнт-серверних архітектур розгортання обчислювальних мереж. В статті коротко наведені їх переваги та недоліки.

З огляду на те, що роль інформаційних технологій в системах управління полягає у забезпеченні досягнення показників достатньої якості управлінських рішень службовими особами органів управління, а точніше: в розв'язанні протиріччя між зростаючими складністю, розмірністю, динамічністю задач управління – з одного боку, і зростаючими вимогами до оперативності, раціональності, обґрунтованості, результативності цих рішень з іншого – то перебудова інформаційної інфраструктури повинна ґрунтуватися на завідомо доказаними світовою практикою у своїй ефективності технологіях.

Логічним продовженням розвитку технології термінального сервера є віртуалізація робочих столів (Virtual Desktop Infrastructure – VDI). На думку авторів статті створення віртуальних робочих станцій за робочими місцями службових осіб органів управління учасників сектору безпеки та оборони – це один ізі шляхів забезпечення якісного виконання завдань службовими особами в інфраструктурі єдиного інформаційного середовища.

В статті наданий короткий огляд продуктів вендорів, які є світовими лідерами у наданні послуг з віртуалізації, функціонально-технічних можливостей VDI, обґрунтування та шляхи упровадження наведеної технології в діючу інформаційну інфраструктуру органів управління учасників сектору безпеки та оборони.

Застосування наведеної технології дозволить існуючій архітектурі набути низки переваг за наступними напрямами: підвищення ефективності централізованого управління та надання сервісів; підвищення безпеки інформації; гнучкість в роботі та реалізація масштабування; ефективне використання фінансів на підтримку і розвиток інформаційної інфраструктури; створення умов до переходу на хмарні технології.

Ключові слова: *інформаційна інфраструктура, віртуалізація робочих столів, інформаційна технологія.*

O. Draglyuk, M. Radchenko, M. Korotkov, D. Pavlyuk Application of Virtual Desktop Infrastructure technologies in special purpose information infrastructure.

In order to fulfill the tasks of the Strategies of National and Military Security of Ukraine to ensure the introduction of modern information technologies, automation of management processes and digitalization of activities in the defense forces of Ukraine with an appropriate level of information security, which is processed, measures are being taken to bring the existing information infrastructure to modern requirements.

The technical component of the information infrastructure of the security and defense sector actors usually consists of sets of information and information-analytical systems, which are different in purpose, but the same in practice in the technology of "thick" and "thin" clients (terminal server) client-server architectures deployment of computer networks. The article briefly lists their advantages and disadvantages.

Considering that the role of information technologies in management systems is to ensure the achievement of indicators of sufficient quality of management decisions by officials of management bodies, or rather: in solving the contradiction between the growing complexity, dimension, dynamism of management tasks - on the one hand, and growing requirements for efficiency, rationality, validity, effectiveness of their decisions, on the other hand, the restructuring of the information infrastructure should be based on the technology that has been obviously proven by world practice in its effectiveness.

A logical continuation of the development of terminal server technology is desktop virtualization (Virtual Desktop Infrastructure - VDI). According to the authors of the article, the creation of virtual workstations for the jobs of officials of the governing bodies of the security and defense sector is one of the ways to ensure quality performance of tasks by officials in the infrastructure of a single information environment.

The article provides a brief overview of the products of vendors who are world leaders in providing virtualization services, VDI functionality and capabilities, rationale and ways to implement this technology in the existing information infrastructure of the security and defense sector.

The application of this technology will allow the existing architecture to gain a number of advantages in the following areas: improving the efficiency of centralized management and service delivery; improving information security; flexibility in work and implementation of scaling; effective use of finances to support and develop information infrastructure; creating conditions for the transition to cloud technologies.

Keywords: *information infrastructure, desktop virtualization, information technology.*

Постановка завдання у загальному вигляді.

Реформування сфери безпеки і оборони за стандартами НАТО належить до найважливіших пріоритетів як зовнішньої, так і внутрішньої політики України. На ряду із іншими важливими заходами щодо вдосконалення систем управління, формування оборонних ресурсів та прийняття на озброєння нових зразків озброєння та військової техніки є створення сучасної інформаційної інфраструктури спеціального призначення. На законодавчому рівні підтримка цих процесів здійснюється низкою відповідних актів, в яких загострюється увага на завданнях відповідного характеру.

Для прикладу, відповідно до Указу Президента України "Про рішення Ради національної безпеки і оборони України "Про Стратегію національної безпеки України" [1] (далі – Стратегія) одним із основних напрямків зовнішньополітичної та внутрішньополітичної діяльності держави для забезпечення її національних інтересів і безпеки є здійснення цифрової трансформації, забезпечення надання адміністративних послуг через безпечне "єдине вікно" з використанням сучасних інформаційних технологій, поширення цифрової грамотності, а також визначено основним завданням системи кібербезпеки – гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури в умовах цифрової трансформації.

В Стратегії наведені напрями та завдання реформування й розвитку сектору безпеки і оборони. У зв'язку з цим зазначено, що зміцнення бойового потенціалу ЗС України, інших складових сил оборони можливо здійснити такими сприятливими для розвитку інформаційно-телекомунікаційних технологій (далі – ІТ-технологій) шляхами, як:

удосконалення та розвиток на основі сучасних технологій систем управління, телекомунікацій, розвідки, логістики;

посилення взаємодії органів сектору безпеки й оборони у виконанні спільних завдань;

створення системи ефективного управління та координації діяльності органів сектору безпеки і оборони, удосконалення її архітектури;

завершення створення та формування сучасних спроможностей національної системи кібербезпеки, зміцнення системи суб'єктів забезпечення кібербезпеки та координації кібероборони.

В Стратегії воєнної безпеки України [2] – наступному документі розвитку воєнної складової безпеки країни – визначена мета забезпечення реалізації державної політики у сфері оборони та пріоритетні шляхи її реалізації у сфері оборони та військового будівництва. Досягнення цілей реалізації державної політики у воєнній сфері передбачається здійснити шляхом виконання завдань за пріоритетом – запровадження об'єднаного керівництва з підготовки та ведення всеохоплюючої оборони України, зокрема:

упровадження сучасних інформаційних та космічних технологій, автоматизація управлінських процесів і цифровізація діяльності в силах оборони України з відповідним рівнем захищеності інформації, що обробляється.

Вирішення наведених завдань потребує здійснення цілеспрямованих, скоординованих за термінами, обсягами ресурсного забезпечення заходів щодо приведення існуючої інформаційної інфраструктури до сучасних потреб.

Аналіз останніх досліджень і публікацій.

Публікацій на тему перебудови інформаційної інфраструктури складових сил оборони з огляду на важливість питання існує достатня кількість. Нижче наведемо деякі з них.

Згідно з [3] реакція органів управління оборонного відомства України на зростаючі вимоги щодо оперативності надання інформації для прогнозування розвитку ситуацій і забезпечення оперативного управління характеризується інтенсивним впровадженням та використанням електронних систем, баз даних, реєстрів, архівів, аналітичних систем, систем моніторингу. В цьому процесі враховуються тенденції розвитку та використання інформаційних технологій в

державному секторі. Автори [3], виходячи із фінансової доцільності та технологічної можливості, зазначають необхідність створення єдиної захищеної ІТ-структури оборонного відомства, яка забезпечить централізацію всіх існуючих в МО та ЗС України інформаційних та інформаційно-аналітичних систем, програмних комплексів та баз даних на базі єдиної захищеної та катастрофостійкої технологічної платформи, основним елементом (ядром) в якій пропонується використання центру обробки даних (далі – ЦОД), що забезпечуватиме роботу єдиної масштабованої, високонадійної автоматизованої відомчої системи (рис. 1).

Автори [3] відмічають, що наявність такої платформи значно полегшить створення будь-яких проєктів у сфері інформатизації та оптимізує витрати на комплексну систему захисту інформації (далі – КСЗІ).

У статті [4] на прикладі оборонного відомства показано, що протягом тривалого часу в інформаційних інфраструктурах спеціального призначення створювались та розвивались окремі автоматизовані, інформаційні, інформаційно-аналітичні та інші програмні системи, які забезпечували інформаційну підтримку лише окремих функціональних процесів управління, що сформувало такі характеристики територіально розподіленої інформаційної інфраструктури оборонного відомства країни, як відокремленість та ізольованість її складових.

Рис. 1. Компоненти єдиної захищеної відомчої ІТ-структури

Тому побудова інформаційної системи, яка функціонує у вигляді єдиної платформи та забезпечує прозоре управління функціональними процесами, гнучко адаптується під будь-які зміни, – є одним із пріоритетних завдань вдосконалення інформаційної інфраструктури не тільки ЗС України, але й складових сил оборони у цілому.

Оскільки роль інформаційних технологій в системах управління полягає у забезпеченні досягнення показників достатньої якості управлінських рішень службовими особами органів управління, а точніше: в розв'язанні протиріччя між зростаючими складністю, розмірністю, динамічністю задач управління – з одного боку, і зростаючими вимогами до оперативності, раціональності, обґрунтованості, результативності їх рішень – з іншого, то цілісна інформаційна інфраструктура має будуватися на досвіді впровадження передових інформаційних технологій, які показали свою ефективність.

Сфера застосування ІТ повинна охоплювати практично всі етапи і складові управлінської діяльності на макрорівні корпоративно-центричної моделі управління складових сил оборони та на мікрорівні – застосування зброї чи засобів ураження і є системоутворюючим фактором сучасних процесів прийняття рішення, що дозволить досягнути якісно нового етапу розвитку воєнного мистецтва – переходу від управління військами в ході конфлікту до управління конфліктом у цілому [5].

Таким чином, робота щодо пошуку ефективних шляхів впровадження нових інформаційних технологій, які практикуються світовими ІТ-спільнотами, триває, тому автори цієї статті вважають актуальним дослідження прикладних застосувань технологій Virtual Desktop Infrastructure (далі – VDI) в інформаційних інфраструктурах складових сектору безпеки та оборони.

Метою роботи є аналіз функціонально-технологічних можливостей технології VDI та обґрунтування пропозицій щодо її застосування в інформаційних інфраструктурах складових сектору безпеки та оборони.

Виклад основного матеріалу.

Виконання завдань, які забезпечуються локальними обчислювальними мережами органів управління (далі – ОУ) учасників сектору безпеки та оборони, визначаються функціональними повноваженнями службових осіб, які, як наведено в [5] на прикладі оборонного відомства, виражаються у здійсненні:

процесів оперативного планування на етапі підготовки операцій (бойових дій) щодо розподілу особового складу органу військового управління по пунктах управління та розмежування доступу службових осіб до даних, які використовуються;

формування деталізованого переліку заходів (завдань), що виконуються службовими особами структурних підрозділів штабу на етапі підготовки операцій (бойових дій);

доведення запланованих завдань до службових осіб штабу та контроль їх виконання;

формування проєктів електронних документів щодо організації роботи штабу при плануванні операцій (бойових дій);

ведення спеціалізованого військового діловодства в ОУ – автоматизована розробка, пошук і відпрацювання бойових (оперативних) документів за напрямками всебічного забезпечення і логістики;

проведення оперативно-тактичних розрахунків та інформаційно-аналітичної підтримки прийняття рішень, де передують оцінки фізико-географічних умов регіону проведення операцій (бойових дій), противника, розрахунки переміщення сил та засобів, визначення маршрутів прольоту армійської авіації тощо;

інформаційного обміну між користувачами та постачальниками інформації як в середині ОУ, так і ззовні (відповідно до категорій терміновості та прав доступу до них службових осіб, автоматизоване ведення адресних книг, журналів і формування звітної документації), реалізація вимог керівних документів щодо організації обміну інформацією;

геоінформаційного забезпечення службових осіб шляхом надійного доступу до просторових даних із поданням їх в наочній формі (електронної картографічної інформації про місцевість, автоматизація процесів створення, оновлення та підготовки до друку топографічних карт усього масштабного ряду, формування електронних карт різних масштабів, доведення до ОУ та військ (сил) електронної картографічної інформації про місцевість, об'єкти на ній, цифрових даних обстановки та ін.).

Очевидно, що робота службових осіб (далі – користувачів) в ОУ відбувається в умовах високої багатоаспектності та складності задач управління. Тому критично важливим стає забезпечення розроблення, впровадження і використання сучасних ІТ, починаючи з постановки завдань, визначення джерел отримання інформації, застосування математичних засобів інформаційно-аналітичної підтримки до створення цілісної інформаційної інфраструктури складових сектору безпеки та оборони.

Відповідно, під кожен напрямок діяльності створювались свої підсистеми автоматизованого управління, основою яких є клієнт-серверна архітектура розгортання. Як наведено в [3; 5], технічна компонента інформаційної інфраструктури ОУ може складатися із таких

наборів інформаційних та інформаційно-аналітичних систем, які різні за призначенням, але однакові за принципами побудови технологічних платформ, як: підсистема організації роботи штабу, підсистема електронного документообігу, інформаційно-довідкова підсистема, інформаційно-розрахункова підсистема, підсистема інформаційного обміну, геоінформаційні системи, інформаційно-аналітична система автоматизованого обліку особового складу, інформаційно-аналітична система обліку майна (житла) та ін.

Коротко кажучи, традиційні клієнт-серверні архітектури розгортання обчислювальних мереж, в яких є сервери – вузли-постачальники деяких специфічних функцій (сервісів) і клієнти – споживачі цих функцій, в практичній реалізації набуті технологіями "товстого" та "тонкого" клієнтів.

Кожна з них визначає власні або використовує наявні правила взаємодії між клієнтом і сервером (протоколами взаємодії). Переваги і недоліки наведених технологій розглянемо нижче.

1. Архітектура розгортання "товстий клієнт" (рис. 2).

Рис. 2. "Товстий клієнт" – робоча станція або ПК, що працює під управлінням власної дискової ОС і має необхідний набір ПЗ

"Товстий клієнт" в архітектурі "клієнт-сервер" являє собою клієнтський мережевий додаток, запущений під керуванням локальної (дискової) операційної системи (далі – ОС), що забезпечує (на противагу тонкому клієнтові) повну функціональність і незалежність від центрального сервера. При цьому можливе забезпечення роботи багатьом користувачам навіть при обривах зв'язку із сервером. Такий додаток поєднує компонент подання даних (графічний користувальницький інтерфейс ОС) і прикладний компонент (обчислювальні потужності комп'ютера клієнта). Часто сервер у цьому випадку є лише сховищем даних, а вся робота по обробці та поданню даних переноситься на персональний комп'ютер (далі – ПК) користувача. До мережевих серверів "товсті клієнти" звертаються в основному за додатковими послугами (наприклад, доступ до web-серверу чи до відомчої бази даних).

Переваги:

наділений широкою функціональністю на відміну від тонкого клієнта;

можливість автономної роботи навіть при обривах зв'язку із сервером;

висока швидкодія (залежить від технічних характеристик робочої станції користувача).

Недоліки:

ускладнене адміністрування прикладних функцій через відсутність централізації;

великий розмір дистрибутива;

проблеми з віддаленим доступом до даних, що виражаються у складності відновлення даних, узгодження їх з іншими клієнтами і пов'язаної з цим не актуальністю даних;

ресурсозатратне обслуговування робочих місць (установка, налаштування і супроводження життєвого циклу, необхідність оновлення ліцензійного програмного забезпечення (далі – ПЗ) та відповідного апаратного забезпечення, кібернетичного захисту на кожному робочому місці);

ускладнений і ресурсозатратний контроль виконання політики безпеки або збільшення її вартості при територіальному розосередженні підрозділів;

висока вартість виконання вимог КСЗІ при мобільному виконанні робочого місця чи здійсненні масштабування.

2. Архітектура термінальний сервер ("тонкий клієнт") (рис. 3).

Суть полягає в розміщенні додатків на одному сервері відразу для двох і більшої кількості користувачів. Користувачі отримують "хмарний" доступ до певних додатків і спеціалізованих програм. Клієнт лише виводить віддалений користувацький інтерфейс, що фізично розміщений на сервері.

В термінальному доступі всі співробітники отримують доступ до однієї ОС і одному набору додатків на всіх через відомчу мережу або Інтернет. (Наприклад, так працюють з програмою 1С-Підприємство).

Серверні обчислення із тонким клієнтом (SBC) або служба віддаленого робочого столу (RDS) дозволяють користувачу віддалено підключатися до програми, яка працює на серверній інфраструктурі, яка розміщена у ЦОД. Далі доставка додатків здійснюється шляхом їх встановлення та запуску на самому сервері. У цьому випадку використовують багатокористувацьку версію програми, яка затребувана для створення окремих сеансів роботи користувачів. Кожен користувач підключається до власного окремого, та захищеного сеансу цієї програми через свій термінал.

При термінальному доступі створюються окремі облікові записи всіх користувачів, які надають доступ до одночасної роботи в єдиній ОС таким чином, щоб користувачі не створювали завад один одному. На клієнтські комп'ютери встановлюються спеціальні додатки, які дають користувачам можливість працювати з окремими сесіями на термінальному сервері. При цьому слід пам'ятати, що у зв'язку з тим, що не всі виробники випускають програмні продукти, які здатні працювати в термінальному режимі, то в такому випадку, нема можливості запускати будь-який додаток.

Основна функціональна можливість, яку надає термінальний сервер – це віддалений доступ до додатків ОС, які встановлені на сервері. У користувача на пристрої повинна бути встановлена програма-клієнт, яка здійснює підключення терміналу до термінального сервера. Найпростіший приклад – програма "Підключення до віддаленого робочого столу", яка вбудована в будь-яку ОС Windows. Доступ може бути надано або до всього робочого столу, або до певного додатку, який відкривається у так званому безшовному вікні. У першому випадку на екрані користувача запуститься термінальна сесія, яка і "закриє" собою поточний робочий стіл. У другому випадку для користувача не буде навіть помітно, що програма, яка запущена в окремому вікні, не з його ПК, а на сервері.

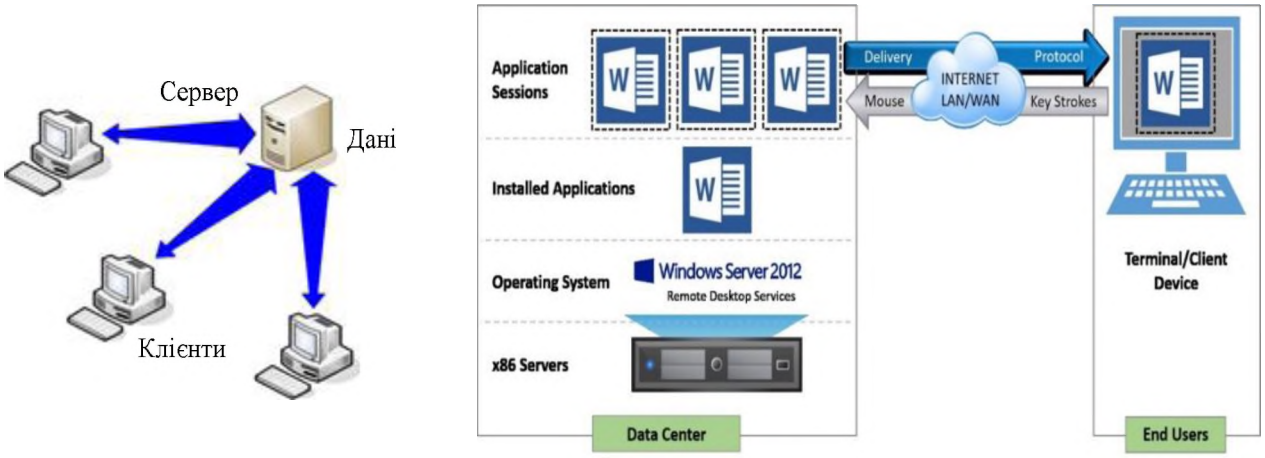

Рис. 3. Робота "тонкого клієнту" в сесії застосунку Word ОС Windows

Переваги:

централізоване управління;

просте адміністрування, дешевше розгортання;

масштабованість;

безпека, захищеність файлів (дані зберігаються на сервері);

зменшення витрат на модернізацію обладнання (клієнтські термінали потребують менших витрат на утримання за рахунок збільшеного терміну роботи);

економія трафіку у WAN-мережах, і як наслідок, зменшення затребуваної пропускної спроможності і вартості трафіку, що орендується. У випадку з термінальним доступом трафік, який раніше проходив між клієнтськими станціями і серверами, замінюється на трафік передачі зображення на віддалений екран користувача.

Недоліки:

непрацездатність сервера може зробити непрацездатною всю обчислювальну мережу;

не можна створити повністю ізольоване середовище з окремим набором прав і програм.

Ізоляція відбувається на рівні сесії, і якщо додаток одного з користувачів викликає збій на рівні ОС, то разом із винуватцем, який викликав збій, будуть змушені перезавантажувати свої додатки й інші користувачі, які працюють на цьому ж сервері.

Деякі виробники не підтримують програмні продукти в термінальному середовищі, наприклад, Autodesk AutoCAD, а для деякого ПЗ необхідні права адміністратора.

Разом із тим загально-світові тенденції розвитку ІТ-технологій [6] дають змогу констатувати факт еволюції статичних комп'ютерних систем до віртуальних за рівнями, які наведені на рис. 4.

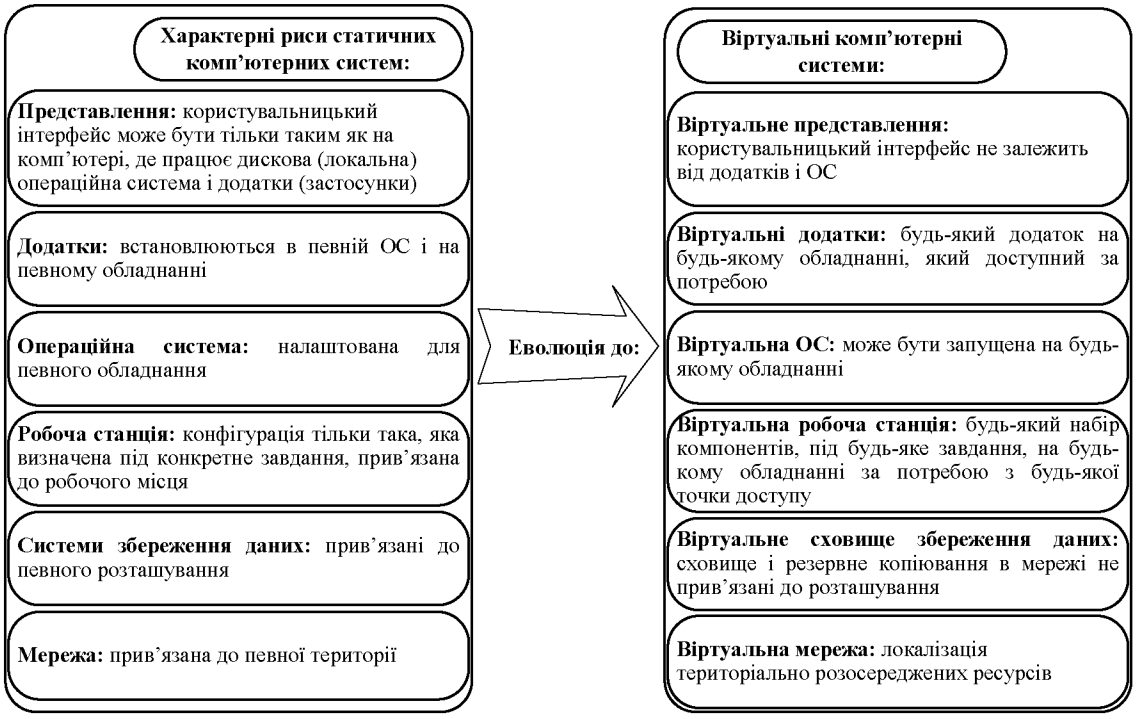

Рис. 4. Еволюція системного підходу побудови ІТ-інфраструктури

Говорячи про технології віртуалізації, які стали невід'ємною частиною сучасних ІТ-інфраструктур державних секторів, необхідно зазначити, що на перше місце виходять питання побудови високопродуктивної, масштабованої, ефективно керованої та безпечної інфраструктури.

У різних країнах із різною швидкістю відбувалося впровадження нових систем, а також оптимізація витрат на підтримку існуючих. Україна не є виключенням і фактично на теперішній час триває перший етап практичного застосування засобів віртуалізації, який можна охарактеризувати як "застосування віртуалізації в умовах існуючої ІТ-інфраструктури". Наступним етапом буде зміна компонентів самої інфраструктури з урахуванням можливостей віртуалізації, як нинішніх, так і перспективних.

Логічним продовженням розвитку технології термінального сервера стала віртуалізація робочих столів (VDI) – створення віртуальних робочих станцій за робочими місцями користувачів, що і пропонується авторами дійсної статті як один із шляхів забезпечення якісного виконання завдань службовими особами ОУ.

Розглянемо детальніше особливості VDI.

3. "Тонкий клієнт" в технології VDI.

VDI – це концепція, в якій дані з ПК користувача зберігаються централізовано на сервері в ЦОД, а у кожного користувача ПК – віртуальний. Розгортається особлива інфраструктура для віддаленої роботи, при якій на основі одного фізичного сервера створюється кілька віртуальних, що дозволяє запускати дві і більше ОС у віддаленому режимі. З архітектурної точки зору, адміністратор сервера для паралельної роботи кожного користувача створює віртуальний повноцінний робочий стіл з окремим набором додатків, програм, документів і доступів.

Операційна система, профіль користувача, політики настільних ПК та програми обробляються як окремі компоненти, які абстрагуються від базової машини, а потім передаються разом з метою створення робочих столів користувачам. Підключення і вся робота користувачів йде через "прошарок" – "тонкий клієнт" (рис. 5).

Замість того, щоб підключатися до відокремленого, захищеного індивідуального сеансу програми, користувач тепер підключається до відокремленого, захищеного, індивідуального примірника ОС сервера, в якому містяться затребувані застосунки.

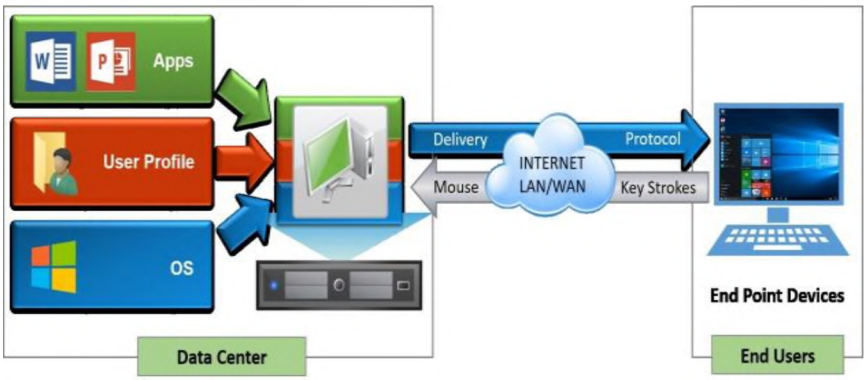

Рис. 5. Набір компонентів віртуального робочого столу для "тонкого клієнта"

Існує два типи інфраструктури VDI: зі збереженням стану і без збереження стану. У випадку зі збереженням стану користувачеві надається певний віртуальний робочий стіл, до якого він може постійно підключатися і котрий він може налаштувати відповідно до своїх потреб, оскільки зміни зберігаються після скидання підключення. Іншими словами, віртуальний робочий стіл у VDI зі збереженням стану працює аналогічно фізичному комп'ютеру. Інфраструктура VDI без збереження стану, в якій користувачам надаються стандартні віртуальні робочі столи і зміни не зберігаються, є більш простим і дешевшим варіантом, оскільки немає необхідності зберігати налаштування віртуальних робочих столів після завершення сеансу. Цей спосіб VDI часто використовується в організаціях із великою кількістю співробітників, що виконують стандартні завдання або при вирішенні обмеженої кількості завдань, що повторюються, для яких не потрібно налаштовувати віртуальні робочі місця.

Відповідно до [7], 80 % світових організацій вже включили технологію VDI у стратегії розвитку інформаційно-телекомунікаційних інфраструктур і які очікують прогнозоване зменшення адміністративних витрат на 70 %, на електроенергію – 97 %, а дозвіл працювати своїм 70 % співробітникам з мобільних пристроїв з будь-якого місця і в будь-який час – дасть на 98 % збільшення продуктивності їх роботи.

Впровадження VDI в роботу службових осіб в ОУ учасників сектору безпеки та оборони із врахуванням обмежень державного регулятора із захисту інформації теж може бути доцільним і обґрунтованим за нижче наведеними напрямками.

Централізація ІТ-сервісів. Перехід до "хмарної" моделі обслуговування. Оскільки зростання пропускної здатності каналів передачі даних і якості сервісів дозволяє уникнути необхідності їх розміщення в безпосередній близькості від користувачів, створюється можливість здійснення централізації ІТ-сервісів в одному чи декількох ЦОД або створення умов переходу до "хмарної" моделі обслуговування. Перехід до такої моделі можливий, оскільки обмін великого об'єму частини трафіку між користувацькими додатками здійснюється в середині серверів ЦОД, а на робоче місце користувача передаються лише дані, що змінилися.

Централізоване управління. Спрощення підтримки та оновлення робочих місць. Централізовані робочі столи на рівні із централізованим управлінням для 1-2 адміністраторів (незалежно від їх територіального розміщення у мережі) дають можливість для кожного робочого столу виконувати набагато простіше такі завдання, як: резервне копіювання, оновлення ПЗ, налаштування ОС чи встановлення нових програм. Контроль за діями користувачів, керування різнорідним парком апаратного забезпечення відбувається з однієї точки мережі. Технологія VDI

дозволяє створювати віртуальні робочі столи з єдиного образу, що підтримується та оновлюється централізовано, а також надає гнучкості при переході на нові версії ОС, оскільки не вимагає негайної відмови від існуючої ОС або заміни клієнтського пристрою.

Організація віддаленої роботи. Гнучкість в роботі та масштабованість. За допомогою VDI можливе забезпечення доступу до будь-якої програми, навіть якщо користувачі знаходяться за межами контрольованої зони відомчої мережі та не мають доступу до своїх робочих місць. На відміну від термінального доступу, VDI дозволяє запустити більш широкий спектр додатків завдяки використанню клієнтських версій ОС. За рахунок ізоляції робочих середовищ користувачів на рівні віртуальних машин (далі – ВМ), для кожної ОС і користувача можуть бути виконані індивідуальні налаштування, що не перемежовуються з іншими користувачами, наприклад, деяким з них можуть надаватися права локальних адміністраторів. Технологія VDI дозволяє гнучко змінювати апаратну конфігурацію ВМ, швидко створювати або повторно розгортати віртуальні робочі столи, що доречно у разі територіально-розподіленої роботи окремих підрозділів, наприклад, у випадку коли немає можливості оперативно доставити користувачу нову робочу станцію або за відсутності у філіальному підрозділі підмінного фонду комп'ютерів і комплектуючих.

Заощадження операційних витрат. Впровадження середовища віртуального робочого столу разом із найкращими практиками щодо управління зображеннями, виправленнями та профілями за допомогою централізованого розгортання додатків призведе до економії операційних витрат порівняно з традиційним управлінням робочих столів. Капітальні витрати на початку проєкту VDI будуть вищими у міру розгортання інфраструктури, проте зниження операційних витрат будуть пов'язані із: закупівлею ліцензій на ПЗ (завдяки встановленню набору користувацьких додатків не на кожен ПК, а на один сервер); зменшеними затратами на електроенергію (завдяки зниженню електроспоживання клієнтських пристроїв до рівня 7–15 Вт); модернізацією парку обчислювальної техніки (завдяки витратам тільки на серверну частину, більш тривалого терміну експлуатації тонких або нульових клієнтів); зменшенням штату технічної підтримки; обслуговуванням і ремонтом системи у цілому.

Підвищення безпеки інформації. Технологія VDI задовольняє потреби, які висуває діяльність користувачів без компрометації безпеки, контролю, керованості та здійснює відповідність вимогам щодо нормативних обмежень державного регулятора із захисту інформації. При кожному підключенні користувача до свого віртуального робочого столу завжди створюється нова ВМ з налаштуваннями особистого оточення. У разі зараження шкідливим ПЗ досить просто перепідключитися до свого віртуального робочого столу, в результаті чого під користувача буде автоматично створена нова ВМ з особистими налаштуваннями оточення, груповими політиками й особистими файлами.

Завдяки централізованому зберіганню призначених для користувачів даних VDI дозволяє спростити механізми резервування й аварійного відновлення робочих столів. Технологія дозволяє реалізувати різні сценарії катастрофостійкості, наприклад, із використанням територіально-розподілених кластерів, автоматичного перемикання на резервний ЦОД або виділення користувачам двох віртуальних робочих столів у різних ЦОД.

Очевидно, що виконання вимог щодо захисту інформації повинно здійснюватися в рамках впровадження хмарних обчислень в державні інформаційні інфраструктури учасників сектору безпеки та оборони, як наведено в [8; 9].

Недоліки VDI. Основним недоліком, що перешкоджає широкому поширенню VDI, залишається висока вартість впровадження порівняно з фізичними робочими станціями або термінальним доступом [10]. Чималу частку у вартості відіграють ліцензії на ПЗ віртуалізації, ОС Windows і брокери VDI. Наприклад, на теперішній час для легального використання клієнтських ОС Windows потрібно або мати ліцензію Windows з чинним Software Assurance на кожен пристрій, з якого здійснюється підключення до віртуальних робочих столів, або щорічну передплатну підписку Windows VDA. До цього додаються витрати на серверні ОС Microsoft Windows і в ряді випадків Microsoft SQL Server, що потрібно для функціонування більшості VDI рішень, а також вимоги щодо ліцензування брокерів VDI (як правило, за кількістю користувачів або активних підключень).

Витрати на апаратне забезпечення. При реалізації у відомстві сценарію інсталяції наведеної технології не з нуля (при збільшені кількості робочих місць, при масовій модернізації) у випадку, коли вже є в наявності достатня кількість функціонуючих ПК, їх можна використати як «тонкі клієнти» після здійснення відповідних доналаштувань. Водночас, для запуску великої кількості віртуальних робочих столів (їх зберігання) потрібне здійснення достатньо затратного апаратного забезпечення, такого як: високопродуктивних серверів із багатоядерними процесорами та великим об'ємом оперативної пам'яті; виділені системи зберігання даних, які здатні надавати необхідні обсяги дискового простору і з високими характеристиками IOPS (кількість операцій введення/виводу в секунду), щоб забезпечити як типові навантаження, так і періодичні пікові; клієнтських терміналів, які необхідні для розгортання VDI.

Клієнтські пристрої («тонкі» клієнти) залишаються вельми недешевим задоволенням. За ціну брендового «тонкого» клієнта (далі – ТК) можна придбати ПК початкового рівня, достатнього для вирішення типових офісних завдань. Крім того, для роботи деяких функцій VDI (підключення сканерів, інтеграція з VOIP-клієнтами та ін.) може знадобитися придбання ТК з ОС Windows Embedded/IOT, що відрізняється більш високою вартістю.

Вимога доступу до мережі. VDI, як і переважна більшість сучасних ІТ-сервісів, вимагає наявності надійного високошвидкісного мережевого доступу до ЦОД. Незважаючи на розвиток бездротового та мобільного Інтернету, далеко не завжди швидкість і стабільність підключення задовільняють комфортну роботу.

Рівень підготовки кваліфікованих спеціалістів ІТ. Якщо для управління фізичними робочими станціями досить фахівця початкового рівня, то для організації VDI потрібно спеціально підготовлений співробітник або група, які б розбиралися у платформах віртуалізації. Огляд компаній-вендорів, які надають послуги VDI, що наведений у звіті компанії IDC Market Scape щодо проведених досліджень ринку надання послуг VDI за 2019–2020 роки [11] свідчить, що лідерами ринку є: Citrix і VMware. Решта – це учасники другого ешелону: Microsoft, Amazon, Parallels, CloudJumper, Huawei та ін.

Доцільно коротко зупинитись на продуктах Citrix і VMware. В мережі Інтернет достатньо порівнянь як відносно незалежних, так і ангажованих за одну чи іншу сторону [12–14]. Якщо говорити про кожного лідера окремо, то VMware може бути цікавим завдяки широкому набору власних продуктів і рішень, які є у складі бандла Horizon або інтегруються з ним. VMware надає найбільш повний і функціональний набір продуктів, на якому можливо побудувати закінчену VDI інфраструктуру з нуля. VMware виходить вперед завдяки реалізації в Horizon таких можливостей, які раніше були сильними сторонами Citrix – доставці додатків з термінальних серверів, а також протоколу Blast, який оптимізований для роботи через повільні, ненадійні канали.

З іншого боку, компанія Citrix зайняла частину ринку завдяки поширеності рішень з організації термінального доступу XenApp, а також пропозицій широких можливостей щодо інтеграції з різними платформами віртуалізації (власний гіпервізор Citrix XenServer, Microsoft Hyper-V, Nutanix AHV і VMware vSphere) чи із хмарними сервісами інших вендорів – Microsoft Azure і Amazon AWS. Забезпечення крос-платформеності і партнерство з іншими виробниками систем віртуалізації є сильними сторонами Citrix.

Висновки. Таким чином, наведені функціонально-технологічні можливості VDI – створення віртуальних робочих столів за робочими місцями службових осіб органів управління – учасників сектору безпеки та оборони, дозволять набути переваг існуючим інформаційним інфраструктурам за наступними напрямками: централізоване управління та надання сервісів; безпека інформації; гнучкість в роботі та реалізація масштабування; ефективне використання фінансів на підтримку і розвиток інформаційної інфраструктури; створення умов до переходу на хмарні технології.

В реаліях сьогодення впровадження засобів віртуалізації проводитиметься в умовах діючої ІТ-інфраструктури. Найдоцільнішим варіантом забезпечення міграції буде здійснення переналаштування визначеного парку ПК в тонкі клієнти, резервування серверів в ЦОД, оплати ліцензій ПЗ обраного вендора, налаштування високошвидкісних каналів передачі даних, задання відповідного алгоритму переходу на VDI водночас із паралельним процесом закінчення життєвих циклів існуючих ІТС. Переваги технології VDI, які наведені в статті, – очевидні, проте постає

питання правильної оптимальної конфігурації для різних пунктів управління, переліку функціональних сервісів, які надаватимуться відповідним службовим особам, що і буде напрямком подальших досліджень.

ЛІТЕРАТУРА

1. Про рішення Ради національної безпеки і оборони України "Про Стратегію національної безпеки України": Указ Президента України від 14.09.2020 № 392/2020 // Офіс Президента України: офіційний портал. URL: https://www.president.gov.ua/news/volodimir-zelenskij-zatverdiv-strategiyu-nacionalnoyi-bezpek-63577 (дата звернення: 02.04.2022).

2. Про рішення Ради національної безпеки і оборони України "Про Стратегію воєнної безпеки України": Указ Президента України від 25.03.2022 № 121/2022. // Офіс Президента України: офіційний портал. URL: https://www.president.gov.ua/documents/1212022-37661 (дата звернення: 02.04.2022).

3. Гудима О. П. ІТ-структура армії / О. П. Гудима, О. Б. Шиятий. *Оборонний вісник.* Київ, 2016. № 8. С. 4–7. URL: https://issuu.com/defensebulletin/docs/ov_08_2016_ukr (дата звернення: 02.04.2022).

4. Кірпічніков Ю. А. Визначення технологічних рішень щодо створення Єдиної інформаційної системи управління оборонними ресурсами / Ю. А. Кірпічніков, О. В. Андрощук, О. В. Головченко, М. В. Петрушен. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського.* Київ, 2019. № 1 (65). С. 86–91.

5. Пермяков О. Ю. Організація інформаційних систем Збройних Сил України: навч. посіб. / О. Ю. Пермяков, Н. О. Королюк, С. І. Фараон. Київ: Національний університет оборони України імені Івана Черняховського, 2019. 134 с.

6. Колесов А. Виртуализация инфраструктуры – ключевое направление в ИТ // Портал "itWeek". 31.05.2011. URL:. https://www.itweek.ru/infrastructure/article/detail.php?ID=131652 (дата звернення: 02.04.2022).

7. Бараш Л. Инфраструктура виртуального десктопа. Почему технология VDI становится популярнее в отечественном корпсекторе? // Компьютерное Обозрение. 25 червня 2019 р. URL: https://ko.com.ua/infrastruktura_virtualnogo_desktopa_pochemu_tehnologiya_vdi_stanovitsya_populyarnee_v_otechestvennom_korpsektore (дата звернення: 02.04.2022).

8. Драглюк О. В. Аналіз можливостей хмарних технологій при застосуванні в інформаційній інфраструктурі складових сил оборони / О. В. Драглюк, Є. І. Нерознак, М. М. Радченко, М. М. Коротков. *Збірник наукових праць ВІТІ.* Київ, 2022. № 1.

9. Аксенов В. Архитектура G-Cloud в облаках // Ассоциация "BISA". 21 октября 2016 р. URL: https://bis-expert.ru/articles/54528 (дата звернення: 02.04.2022).

10. Коновалов А. Немного о дизайне VDI // Blogger: блог, посвященный технологиям виртуализации и смежным с ними областям. 04.09.2017. URL: http://blog.vmpress.org/2017/09/vdi-1.html (дата звернення: 02.04.2022).

11. Звіт IDC MarketScape: Worldwide Virtual Client Computing 2019–2020 Prondor Assessment" (Doc # US45752419, січень 2020). URL: https://www.idc.com/getdoc.jsp?containerId=US45752419 (дата звернення: 02.04.2022).

12. Порівняйте віртуальні програми та настільні комп'ютери Citrix та VMware Horizon View // Портал інтернет-видання IT-Central Station Unbiazed reviews from the tech community. URL: https://www.itcentralstation.com/products/comparisons/vmware-horizon-view_vs_xendesktop (дата звернення: 02.04.2022).

13. Компанія Citrix: вебсайт. URL: https://www.citrix.ru/products/xenapp-xendesktop/ compare.html (дата звернення: 02.04.2022).

14. Компанія VMware: вебсайт. URL: https://www.vmware.com/company/why-choose-vmware/workspace-transformation.html (дата звернення: 02.04.2022).