УДК 004.75

Кірпічніков Ю. А., к.т.н.;
Кондратенко Ю. В.;
Головченко А. В.;
Петрушен М. В.;
Берестов Д. С.

Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Шляхи створення захищеної ІТ-інфраструктури Збройних Сил України

Резюме. У статті розглянуто шляхи щодо створення захищеної ІТ-інфраструктури Збройних Сил України на основі центру обробки даних. Описуються проблемні питання щодо можливих вузьких місць в майбутній архітектурі, які необхідно врахувати при виділенні апаратних ресурсів.

Ключові слова: центр обробки даних, інформаційний сервіс, міграція даних, резервне копіювання даних, реплікація даних, ідентифікація, аутентифікація.

Постановка проблеми. Останні політичні та воєнні події змусили Україну жити в новій реальності і приймати блискавичні рішення у відповідь на актуальні виклики XXI століття. В умовах воєнно-політичної кризи та інформаційної війни Україні, її державним інститутам, зокрема Збройним Силам Україні, належить виробити і застосувати нові сучасні підходи до розвитку власного інформаційного простору, забезпечення його стійкості та безпеки.

Як визначено у Концепції Національної програми інформатизації [1] – інформатизація Збройних Сил України є складовою частиною інформатизації держави і включає процес створення, впровадження і застосування у різних сферах їх діяльності у мирний та воєнний час сучасних методів, систем і засобів одержання, оброблення, зберігання, передавання та використання інформації.

Поширеною є думка, що незважаючи на значне розширення ринку інформаційних послуг і продуктів, а також певний розвиток законодавчої бази щодо інформатизації, інформаційне забезпечення в Збройних Силах України залишається на низькому рівні.

Основними проблемами вважаються застарілість або неефективне використання апаратного та програмного забезпечення, відсутність швидкісних захищених мереж передачі даних та централізованих сховищ даних, складність організації доступу до існуючих баз даних, відсутність обміну даними, і як наслідок – неоперативність та недостовірність інформації.

Одним із перспективних шляхів розвитку інформаційних технологій в Збройних Силах України є використання сучасних потужних програмно-апаратних платформ, сховищ даних, засобів віртуалізації обчислювальних та мережевих ресурсів, хмарних технологій тощо.

Ключовими стають питання оновлення обчислювальних ресурсів, розвиток мережевих технологій, забезпечення високої доступності (безперервності надання) інформаційних сервісів, безпеки інформації, централізації збереження, резервування та екстреної міграції даних.

Для вирішення цих питань у державному секторі все більшого розвитку отримує практика централізації обчислювальних ресурсів та сховищ даних у власних центрах обробки даних.

Централізація достатніх потужностей для зберігання і обробки інформації дозволить Збройним Силам України створити власну захищену ІТ-інфраструктуру, яка стане основою єдиного надійного та безпечного інформаційного простору.

Ступінь розробленості проблеми. Переваги централізованої обробки інформації відомі з часів існування обчислювальних центрів (ОЦ), що використовували декілька середніх та великих електронно-обчислювальних машин (ЕОМ), мали кваліфікований персонал для обслуговування техніки та програмного забезпечення.

На сьогоднішній день поняття ОЦ дещо трансформувалося. Існуюча інформаційно-телекомунікаційна система Збройних Сил України має “острівкову” архітектуру у вигляді великого парку розрізнених автоматизованих систем управління (АСУ), інформаційних систем (ІС) та інформаційно-аналітичних систем (ІАС). ОЦ – це частіше невеликий структурний

підрозділ вузла зв'язку що займається підтримкою деякої кількості Web-серверів, поштових та файлових серверів, невеликих баз даних, мережевого обладнання.

Сучасні високопродуктивні системи для централізованих обчислень відрізняються такими характеристиками, як підвищена продуктивність, масштабованість, мінімально допустимий час простою. Інтенсивні потоки даних, що циркулюють в таких системах, потребують особливої організації IT- інфраструктури. Вона повинна адаптуватися до мінливих вимог, забезпечувати постійне зростання продуктивності використовуваних рішень та максимальну ефективність їх експлуатації.

Вирішення цієї проблеми полягає у концентрації обчислювальних ресурсів у центрах обробки даних (ЦОД) – спеціалізованих будівлях (приміщеннях), що мають необхідне обчислювальне та технологічне обладнання, а також кваліфікований персонал.

Процес впровадження ЦОД набув широкого розповсюдження та відносно швидких темпів у всьому світі. Свої варіанти підходів до організації ЦОД пропонують майже всі відомі виробники комп'ютерного та комутаційного обладнання, а також програмного забезпечення. Як правило, в цих рішеннях використовуються останні розробки компаній. Слід зазначити, що дані підходи стосуються цивільного сектору. Досвід зарубіжних армій світу щодо побудови власної захищеної IT-інфраструктури на основі ЦОД зустрічається в загальному вигляді або на рівні концепції.

Актуальність статті пов'язана із необхідністю пошуку шляхів створення захищеної IT-інфраструктури Збройних Сил України, яка задовольняє необхідні вимоги щодо захищеності, стійкості до будь-яких факторів впливу, економічності у використанні, інтегрованості функціонування розрізнених АСУ, ІС та ІАС. Це дозволить на етапі проектування захищеної IT-інфраструктури зменшити значні витрати за рахунок визначення необхідних програмно-апаратних та інженерних ресурсів, засобів захисту та охорони, а також досягти максимальної ефективності у забезпеченні керівництва Збройних Сил України своєчасною та достовірною інформацією на етапі імплементації.

Метою статті є визначення стратегії забезпечення централізації всіх існуючих в Збройних Силах України інформаційних та інформаційно-аналітичних систем, програмних комплексів та баз даних у єдину захищену, відмовостійку та катастрофостійку IT-інфраструктуру, удосконалення існуючої та створення високотехнологічної основи для принципово нових систем з управління підпорядкованими структурами та забезпечення діяльності Міністерства оборони України і Генерального штабу за рахунок реалізації наявних та створення принципово нових, інформаційних та інформаційно-аналітичних систем, сервісів, програмних комплексів, баз даних і впровадження на їх базі потужного, єдиного програмно-технічного комплексу.

Виклад основного матеріалу. Процес технологічного розвитку в світі вимагає постійного оновлення застарілих технологій для реалізації світових стандартів та вимог сьогодення до інформаційних технологій як у технічній так і у інформаційній сферах.

Принципи створення

Основними принципами створення захищеної IT-інфраструктури в Збройних Силах України є:

створення системи автоматичної ідентифікації та аутентифікації посадових осіб – користувачів автоматизованих систем;

створення правил доступу і обміну даними для IT-інфраструктури з метою забезпечення безпеки інформації;

інтеграція в органи військового управління різного рівня Міністерства оборони України та Генерального штабу існуючих та перспективних автоматизованих систем управління, інформаційних та інформаційно-аналітичних систем, програмних комплексів та баз даних;

забезпечення високошвидкісного та захищеного доступу до інформаційних та інформаційно-аналітичних систем і сервісів;

забезпечення безперебійної роботи автоматизованих систем управління та систем підтримки прийняття рішень керівним складом;

створення IT-інфраструктури для впровадження надсучасних інформаційних технологій.

Одним із варіантів вирішення проблеми може бути створення окремих інформаційно-телекомунікаційних систем для роботи інформаційних та інформаційно-аналітичних систем Збройних Сил України. Але даний варіант потребуватиме великих фінансових затрат на утримання і обслуговування інформаційних та інформаційно-аналітичних систем, та з часом призведе до накопичення великої кількості інформаційно-телекомунікаційних систем, що створює неприйнятно складний рівень IT-інфраструктури з унеможливленням її керованості та виникненням нових проблем, які необхідно буде вирішувати.

Тому, найбільш раціональним варіантом вирішення проблеми має стати створення єдиної захищеної, відмовостійкої та катастрофостійкої ІТ-інфраструктури, головним елементом якої доцільно визначити центр обробки даних з централізованими сервісами доступу, збереження, обробки і обміну даними та засобами транспорту інформації, між окремими системами і віддаленими користувачами, на основі віртуалізації та "хмарних" технологій.

Призначенням центру обробки даних, як основного елементу єдиної захищеної, відмовостійкої та катастрофостійкої ІТ-інфраструктури є забезпечення єдиним масштабованим, високонадійним та катастрофостійким обчислювальним ресурсом автоматизованих систем Збройних Сил України.

Центр обробки даних повинен мати наступні функції:

технічне забезпечення обробки і зберігання відкритих та категорованих даних відповідно до вимог з безпеки інформації;

технічне та програмне забезпечення розгортання і роботи сервісів, програмних комплексів, інформаційних та інформаційно-аналітичних систем на основі віртуалізації та "хмарних" технологій, з наданням можливості опрацювання відкритої та категорованої інформації відповідно до вимог з безпеки інформації;

інфраструктурне забезпечення безперебійної роботи технічного та інформаційного обладнання;

інфраструктурний захист технічного та інформаційного обладнання від впливу зовнішніх негативних факторів та порушень захисту інформації;

моніторинг параметрів та стану елементів інфраструктури, технічного та інформаційного обладнання;

технічне забезпечення з транспортування даних між інформаційними та інформаційно-аналітичними системами і віддаленими користувачами.

Основними задачами центру обробки даних є:

забезпечення фізичного розміщення обчислювального обладнання (серверного, комутаційного обладнання, систем зберігання даних, тощо);

забезпечення технологічних умов для роботи обчислювального обладнання;

забезпечення безперебійного надання інформаційних послуг протягом заданого інтервалу часу у разі впливу зовнішніх і внутрішніх негативних факторів;

забезпечення можливості моніторингу основних параметрів та стану компонентів технологічної інфраструктури;

забезпечення технічного захисту інформації, у тому числі забезпечення захисту обладнання та інформації від зовнішніх електромагнітних випромінювань і перешкод;

забезпечення фізичного захисту інформації за рахунок резервного копіювання (міграції) даних на віддалені ресурси.

Структура ІТ-інфраструктури

Єдина захищена, відмовостійка та катастрофостійка ІТ-інфраструктура Збройних Сил України для забезпечення відмовостійкості повинна мати фізично географічно рознесену структуру та бути реалізованою на основному, резервному і мобільному елементах, які пов'язані між собою захищеною швидкісною мережею передачі даних.

Кожен з елементів повинен складатися з інтегрованих програмних та апаратних компонентів, інженерних систем, а також організаційних процедур, засобів управління обчислювальними ресурсами та забезпечення безпеки інформації.

Основний елемент (основний центр обробки даних) має представляти об'єкт з достатньою кількістю технологічних приміщень, що відповідають вимогам нормативних документів до створення центрів обробки даних, та дозволяють розмістити ІТ-обладнання загальною потужністю до 1 МВт, з урахуванням можливості подальшого розширення.

Резервний елемент (резервний центр обробки даних) повинен створюватися з урахуванням повної відповідності функціям основного елементу (основного центру обробки даних) і вимогам нормативних документів щодо його створення, із забезпеченням сумісної роботи у режимі "гарячого резерву". Головною вимогою до резервного елементу (резервного центру обробки даних) є гарантія безперервності надання інформаційних сервісів у разі часткового або повного виходу з ладу основного елементу (основного центру обробки даних).

Основний та резервний елемент (основний та резервний центр обробки даних) повинні бути територіально рознесеними.

Мобільний елемент (мобільний центр обробки даних) має бути створеним у вигляді контейнерів стандартного формфактору. Вибір місця його розгортання залежить від завдань, які на нього покладаються. Основними завданнями мобільного елементу (мобільного центру обробки даних) є резервування роботи основного елементу (основного центру обробки даних) та виконання функцій допоміжного

елементу в управлінні військами у зоні проведення військових дій.

Зазначені комплекси мають представляти собою повністю закінчені технологічні рішення, що взаємопов'язані за метою та є повністю незалежними (автономними) за можливістю виконання своїх функцій.

Рівень надійності елементів ІТ-інфраструктури (центрів обробки даних) повинен відповідати рівню не меншому за Tier 3 у відповідності до стандарту TIA/EIA-942.

Нормативно-правове забезпечення

Створення єдиної захищеної, відмовостійкої та катастрофостійкої ІТ-інфраструктури Збройних Сил України на етапах проектування та побудови повинне здійснюватися відповідно до стандартів та вимог нормативних документів в сфері створення і функціонування центрів обробки даних та телекомунікаційних мереж органів державної влади, а також у сфері захисту інформації.

Реалізація

Створення єдиної захищеної, відмовостійкої та катастрофостійкої ІТ-інфраструктури Збройних Сил України здійснюватиметься у три етапи.

На першому етапі: загальне проектування всієї інфраструктури та побудова у Збройних Силах України захищеної, відмовостійкої та катастрофостійкої ІТ-інфраструктури основного центру обробки даних.

На другому етапі: побудова у Збройних Силах України захищеної, відмовостійкої та катастрофостійкої ІТ-інфраструктури резервного центру обробки даних.

На третьому етапі: побудова у Збройних Силах України захищеної, відмовостійкої та катастрофостійкої ІТ-інфраструктури мобільного центру обробки даних.

Фінансове забезпечення реалізації

Реалізація впровадження центрів обробки даних здійснюватиметься за рахунок коштів державного бюджету, залучення інвестицій та інших джерел, не заборонених законом.

Визначення обсягів фінансового ресурсу, необхідного для створення єдиної захищеної, відмовостійкої та катастрофостійкої ІТ-інфраструктури сектору безпеки і оборони України, буде здійснено за результатами проведення проектування.

Висновки. У результаті побудови єдиної захищеної, відмовостійкої та катастрофостійкої ІТ-інфраструктури сектору безпеки і оборони України на основі центру обробки даних, на відміну від створення та підтримки окремих (розрізнених) обчислювальних систем для кожної окремої задачі інформатизації буде здійснено інтеграцію обчислювальних ресурсів у єдиний, потужний програмно-технічний комплекс з централізованим забезпеченням їх функціонування та обслуговування мінімальною кількістю кваліфікованого персоналу, вирішено питання своєчасної модернізації та ремонту, що загалом значно зменшить витрати на утримання.

На базі обчислювальних потужностей центру обробки даних з застосуванням віртуалізації та "хмарних" технологій будуть розгорнуті сучасні програмно-апаратні комплекси зв'язку та автоматизовані системи, різні за призначенням аналітичні системи, бази даних, системи електронного документообігу, віддалені робочі місця посадових осіб, що дозволить провести міграцію (перенесення) на нове обладнання парку існуючих програмних систем, поштових систем, файлових серверів, поступово вивести з експлуатації застаріле обладнання та вирішити проблеми з ліцензуванням програмного забезпечення.

Єдина захищена, відмовостійка та катастрофостійка ІТ-інфраструктура надасть змогу розгорнути Ситуаційний центр Міністерства оборони України, а у перспективі і розгортання ситуаційних центрів інших органів сектору безпеки і оборони України.

Потужності елементів єдиної захищеної, відмовостійкої та катастрофостійкої ІТ-інфраструктури можуть бути використані для розгортання компонентів Єдиної автоматизованої системи управління Збройними Силами України, таких як автоматизовані системи оперативного (бойового) управління військами та зброєю, системи формування єдиного віртуального бойового простору, системи космічної розвідки тощо.

Елементи єдиної, гнучкої, високонадійної, захищеної, відмовостійкої, катастрофостійкої та легко масштабованої ІТ-інфраструктури стануть ядром, навколо якого можливо швидко розпочати формування перспективної системи управління Збройними Силами України.

Водночас, завдяки здійсненню централізації (враховуючи підвищення рівня відмовостійкості та катастрофостійкості) будуть досягнуті такі результати:

підвищено рівень відмовостійкості та катастрофостійкості існуючої ІТ-інфратруктури, що зменшить вікно простою сервісів і систем та підвищить надійність і безпеку;

зменшено кількість трудозатрат на обслуговування ІТ-інфратруктури, що вивільнить людські ресурси;

збільшено щільність та продуктивність ІТ-інфратруктури, що зменшить кількість систем,

енергозатрати та трудозатрати під час її експлуатації та обслуговування;

забезпечено більш високий рівень інтеграції систем і сервісів, що підвищить швидкість обміну даними між системами та зменшить кількість інцидентів;

приведено до загального стандарту на рівні апаратних та програмних рішень;

підвищено рівень інформаційної безпеки.

Подальші дослідження доцільно присвятити обґрунтуванню основних рішень щодо створення програмно-технічної платформи, яку буде використано при побудові захищеної інфраструктури Збройних Сил України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Про Концепцію Національної програми інформатизації [Електронний ресурс]: закон України [прийнято Верхов. Радою 04 лютого 1998 р. №75/98-ВР (Зі змінами та доповненнями)]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/75/98-вр.
2. Морозов А. О. Основні проблеми інформатизації Збройних Сил України на сучасному етапі / А. О. Морозов, Г. Є. Кузьменко, А. Д. Яровий // Наука і оборона. – 2004. – № 3. – С. 16–22.
3. Артюх В. М. Современный этап разработки и строительства Единой автоматизированной системы управления Вооруженными Силами Украины / В. М. Артюх, В. К. Медведев // Оборонный вестник. – 2012. – № 1. – С. 15–24. – Режим доступу: http://defpol.org.ua/site/files/OV_1_2012_rus.pdf.
4. Главный инспектор МО Украины Валерий Фролов: «Дальнейшее промедление с внедрением Единой автоматизированной системы управления ВС Украины становится опасным для обороноспособности государства»– Режим доступа: http://ak-inzt.net/forces/641-article7674.–
5. Коммерческие ЦОД в Украине: новый этап развития [Электронный ресурс]. – Режим доступа: http://www.sib.com.ua/arhiv_2010/2010_3/statia_3_1_2010/statia_3_1_2010.htm. – Название с экрана.
6. Institute for Data Center Professionals [Electronic Resource]. – Mode of access: http://idcp.marist.edu/. – Title from the screen.
7. Uptime Institute LLC [Electronic Resource]. – Mode of access: http://uptimeinstitute.com/. – Title from the screen.
8. TIA/EIA-942. Telecommunications Infrastructure Standard for Data Centers. – SP–3-0092, 2005. Датацентр консалтинг: Denovo [Электронный ресурс]. – Режим доступа: http://www.de-novo.biz/chastnye-oblaka-i-korporativnye-tsody/datatsentr-konsalting/. – Название с экрана.

Стаття надійшла до редакції 02.04.2015

Кирпичников Ю. А. (к.т.н.); Кондратенко Ю. В.;
Головченко А. В.; Петрушен Н. В.;
Берестов Д. С.

Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, г. Киев

Пути создания защищённой ИТ-инфраструктуры Вооруженных Сил Украины

Резюме. В статье рассмотрены пути создания защищенной IT-инфраструктуры Вооруженных Сил Украины на основе центра обработки данных. Описываются проблемные вопросы относительно возможных узких мест в будущей архитектуре, которые необходимо учесть при выделении аппаратных ресурсов..

Ключевые слова: центр обработки данных, информационный сервис, миграция данных, резервное копирование данных, репликация данных, идентификация, аутентификация.

Y. Kirpichnikov; Y. Kondratenko;
A. Golovchenko; N. Petrushen;
D. Berestov

Center for Military and Strategic Studies National Defence University of Ukraine named Ivan Chernyhovskij

Towards the creation of a secure IT infrastructure of the Armed Forces of Ukraine

Resume. The article reviews some approaches to identifying key requirements for data center infrastructure projected. Describe the problem areas of possible bottlenecks in the future architecture that must be taken into account in the allocation of hardware resources.

Keywords: data center, information services, data migration, data backup, data replication, identification, authentication.