УДК 65.011.56

Соколов К. О.[1];
Гудима О. П., к.т.н., снс[1];
Ткаченко В. А. к.військ.н.[2];
Шиятий О. Б.[1]

[1] - Управління інформаційних технологій Міністерства оборони України, Київ;
[2] - Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Основні напрями створення ІТ-інфраструктури Міністерства оборони України

Резюме. У статті розглядається проблема розвитку інформаційних технологій у Міністерстві оборони України, яка впливає на ефективність керування військами, діяльністю Міністерства оборони України та Збройних Сил України. На сьогоднішній день впровадження інформаційних технологій несе несистематизований характер, що призвело до неспроможності реалізації більшості інформаційних та інформаційно-аналітичних систем, а ті, що реалізовані, не в повному обсязі використовують свої можливості. Одним із шляхів вирішення проблеми є побудова єдиного ядра інформаційної інфраструктури для Міністерства оборони України та Збройних Сил України.

Ключові слова: інформаційні технології; ІТ-інфраструктура; комплексна система захисту інформації; інформаційні системи; інформаційно-аналітичні системи.

Постановка проблеми. Враховуючи тенденції розвитку та використання інформаційних технологій (ІТ-технологій) в діяльності органів державної влади розвинутих країн світу, зростаючі вимоги щодо оперативності надання інформації для прогнозування розвитку ситуацій і забезпечення оперативного управління, в Міністерстві оборони України інтенсивно впроваджуються та використовуються електронні системи, бази даних, реєстри, архіви, аналітичні системи, системи моніторингу.

Протягом цього року в Україні прийнята ціла низка законодавчих актів, які сприяють розвитку та впровадженню інформаційних систем у сфері національної безпеки і оборони України, розвитку інформаційної інфраструктури для реалізації отримання та обміну інформацією і підвищення функціональності органів державної влади.

Указ Президента України № 555/2015 від 24 вересня 2015 року Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України" [1].

Основними завданнями, які сприяють створенню інформаційної інфраструктури є:

створення єдиної системи видової розвідки з відповідною інфраструктурою отримання та обробки інформації в режимі часу, наближеного до реального;

створення цілісного сектору безпеки і оборони держави як головного елементу системи забезпечення воєнної безпеки, інтеграція спроможностей його складових для своєчасного і ефективного реагування на наявні та потенційні загрози;

забезпечення матеріально-технічної бази системи управління сектором безпеки і оборони України за допомогою Головного ситуаційного центру України, мережі відомчих ситуаційних центрів;

здійснення координації відповідно діяльності всіх органів державної влади, органів місцевого самоврядування і громадян в інтересах ліквідації воєнного конфлікту і відсічі збройній агресії;

забезпечення інформаційної складової воєнної безпеки шляхом запровадження ефективної системи заходів стратегічних комунікацій у діяльність органів сектору безпеки.

Указ Президента України № 287/2015 від 26 травня 2015 року Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України" [2].

Основними завданнями, які сприяють створенню інформаційної інфраструктури є:

забезпечення централізованого управління сектором безпеки і оборони та міжвідомчої координації і взаємодії у мирний час, у кризових

ситуаціях, що загрожують національній безпеці та в особливий період;

удосконалення державної системи стратегічного планування, створення єдиної системи моніторингу, аналізу, прогнозування та прийняття рішень у сфері національної безпеки і оборони, забезпечення ефективної координації та функціонування єдиної системи ситуаційних центрів профільних органів державної влади сектору безпеки і оборони;

посилення координації розвідувальних органів та їх взаємодії між собою, зокрема для підготовки узгоджених розвідувальних оцінок;

забезпечення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

здійснення протидії інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації;

виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

забезпечення кібербезпеки і безпеки інформаційних ресурсів;

забезпечення безпеки критичної інфраструктури;

забезпечення обміну інформацією між державними органами, приватним сектором і населенням стосовно загроз критичній інфраструктурі та захисту інформації у цій сфері.

Указ Президента України № 5/2015 від 12 січня 2015 "Про Стратегію сталого розвитку "України-2020" [3].

Основним завданням, яке сприяє створенню зазначеної інфраструктури, є створення ефективної державної системи кризового реагування (мережі ситуаційних центрів центральних органів виконавчої влади) за провідної ролі Ради національної безпеки і оборони України.

Необхідно відзначити, що у Міністерстві оборони України та Збройних Силах України єдина інформаційна структура відсутня, а наявні розрізнені інформаційні та інформаційно-телекомунікаційні системи не дозволяють реалізувати виконання поставлених завдань у повному обсязі.

Аналіз останніх досліджень і публікацій. На сьогоднішній день в Міністерстві оборони України створюється ряд інформаційних та інформаційно-аналітичних систем у сферах медицини і логістики.

Роботи виконуються відповідно до стандартів, але зазначені системи створюються на різних технологічних платформах [4, 5].

Метою статті є надання пропозиції з вирішення питання щодо впровадження у Міністерстві оборони України та Збройних Силах України концептуальних основ зі створення єдиної інформаційної системи, з відповідною інфраструктурою отримання та обробки інформації у сфері національної безпеки і оборони України для підвищення функціональності органів військового управління.

Виклад основного матеріалу. Під час участі Збройних Сил України в антитерористичній операції на території Донецької та Луганської областей, з'ясувалось, що на фактори, які впливають на спроможність адекватно протистояти агресії противника, суттєво впливає рівень впровадження інформаційних технологій.

Найбільш помітно це у сферах матеріально-технічного, медичного та інформаційного забезпечення, розвідки.

На сьогоднішній день в Міністерстві оборони України використовуються наступні інформаційні та інформаційно-телекомунікаційні системи:

офіційний веб-портал Міністерства оборони України в мережі Інтернет;

захищена система електронного документообігу "Седо-М";

інформаційно-аналітична система планування мобілізаційного розгортання Збройних Сил України;

інформаційно-аналітична система автоматизованого обліку особового складу "Персонал";

інформаційно-аналітична система підтримки оборонного планування "Ресурс";

каталог предметів постачання Збройних Сил України "КПП";

інформаційно-аналітична система підтримки планування розвитку озброєння "Клеопатра";

інформаційно-аналітична система "Майно-Житло".

Тривають роботи щодо створення:

медичної інформаційної системи Збройних Сил України "е-Здоров'є";

системи дистанційного телемедичного консультування "Телемедицина";

функціональної підсистеми "Логістика", системи управління адміністративно-господарськими процесами;

системи автоматизації процесів обліку та планування обігу медичного майна на

медичних складах Міністерства оборони України.

Для підтримки кожної інформаційної та інформаційно-телекомунікаційної системи використовується коштовне технічне обладнання та утримується штат чергового і обслуговуючого персоналу. А найголовніше те, що експлуатація більшості зазначених систем здійснюється на окремих технічних засобах, що вимагає використання одним працівником декількох автоматизованих робочих місць (далі - АРМ).

Зазначене вимагає залучення великої кількості матеріальних затрат на впровадження, використання і підтримку інформаційних та інформаційно-аналітичної систем.

При необхідності впровадження нової інформаційної та інформаційно-аналітичної системи виникає необхідність розгортання нової технічної складової з виконанням вимог комплексної системи захисту інформації (далі - КСЗІ), що будується відповідно до вимог нормативної бази у сфері технічного захисту інформації, яка морально застаріла та не відповідає сучасним світовим стандартам, включаючи стандарти НАТО, що збільшує витрати та кількість АРМів.

Так, наприклад, для розгортання захищеної системи електронного документообігу "Седо-М" була розгорнута інформаційно-телекомунікаційна система з відповідними АРМ, головним сервером, та виконанням вимог КСЗІ на відповідну систему. Теж саме здійснювалось при розгортанні автоматизованої системи управління Збройних Сил України "Дніпро", інформаційно-довідкової системи "Інтернет", а практично це однакові за принципами побудови технологічні платформи, різні лише за завданням.

Так, рішенням проблеми є створення єдиної захищеної ІТ-інфраструктури (рис. 1).

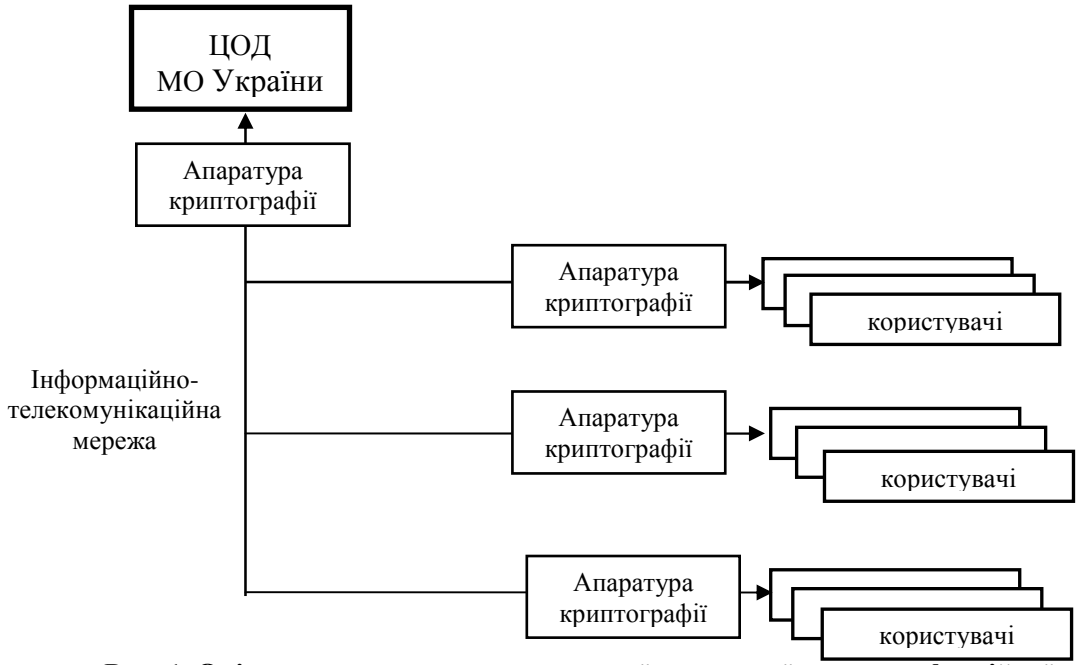

Рис. 1. Орієнтовна загальна схема єдиної захищеної, катастрофостійкої та відказостійкої ІТ-інфраструктури

Впровадження запропонованого рішення при створенні нової інформаційної, інформаційно-аналітичної системи виключає необхідність створення технічної складової, зменшує витрати на створення КСЗІ, завдяки створенню КСЗІ на єдину технологічну платформу.

Основним елементом (ядром) єдиної захищеної ІТ-інфраструктури є центр обробки даних (рис. 2).

Призначенням центру обробки даних є забезпечення єдиною масштабованою, високонадійною обчислювальною системою автоматизовані системи Міністерства оборони України та 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 Держспецзвя'зку;

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 обладнання;

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

моніторинг параметрів та стану елементів інфраструктури, технічного обладнання;

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

Основними задачами центру обробки даних є:

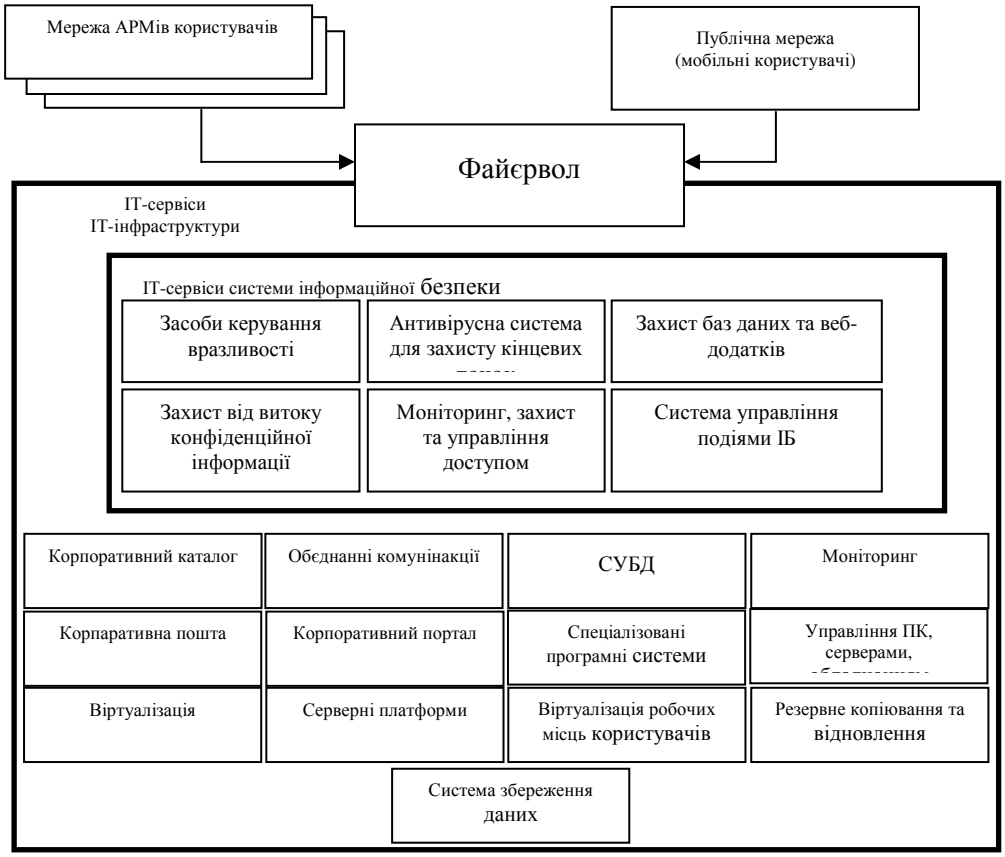

Рис. 2. Функціональні складові центра обробки даних

забезпечення фізичного розміщення телекомунікаційного 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;

забезпечення роботи, за технологією Virtual Desktop Infrastructure (VDI), користувачів сервісів, програмних комплексів, інформаційних та інформаційно-аналітичних систем.

Так, центри обробки даних функціонують в цивільних організаціях діяльність яких пов’язана з інформаційною діяльністю.

На території України основними комерційними центрами обробки даних є:

“Парковий” – комерційний центр обробки даних з наданням всебічних сервісів замовникам, на сьогодні має КСЗІ на “хмарний” сервіс;

“Мобілайн” – забезпечення роботи телекомунікаційної мережі та надання сервісних послуг замовникам;

“DENOVO” – є найпотужнішим центром обробки даних із надання сервісних послуг замовникам;

“BEMOBILE” – центр обробки даних із надання сервісних послуг замовникам.

Висновки. Побудова зазначеної інфраструктури надасть можливість швидкої реалізації будь-яких проектів у сфері інформатизації.

На сьогодні за рішенням Міністра оборони України тривають консультації з представниками корпорації "Майкрософт" в Україні та іншими компаніями і науковими установами щодо розроблення концептуального архітектурного бачення побудови ядра інформаційної інфраструктури для Міністерства оборони України у сфері інформаційних технологій з забезпеченням максимальної інформаційної безпеки.

Подальші дослідження доцільно спрямувати на вивчення сервісів, які реалізуються у зазначеній системі для Міністерства оборони України та Збройних Сил України з подальшою їх інтеграцією у єдину систему сектору безпеки та оборони України.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Указ Президента України від 24.09.2015 року № 555/2015 Про рішення Ради національної безпеки і оборони України від 2 вересня 2015 року "Про нову редакцію Воєнної доктрини України".
2. Указ Президента України від 26.05.2015 року 287/2015 Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року "Про Стратегію національної безпеки України".
3. Указ Президента України від 12.01.2015 № 5/2015 "Про Стратегію сталого розвитку "України-2020"".
4. ГОСТ 34.601-90 "Автоматизированные системы. Стадии создания".
5. Постанова Кабінету Міністрів України від 04.02.1998 року № 121 "Про затвердження переліку обов'язкових етапів робіт під час проектування, провадження та експлуатації системи і засобів автоматизованої обробки та передачі даних".

Стаття надійшла до редакції 05.11.2015

Соколов К. А.[1];
Гудима О. П., к.т.н., снс[1];
Ткаченко В. А. к.воен.н.[2];
Шиятий А. Б.[1]

[1] - Управление информационных технологий Министерства оборони Украины, Киев;

[2] - Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев

Основные направления создания ИТ-инфраструктуры Министерства обороны Украины

Резюме. В статье рассматривается проблема развития информационных технологий в МО Украины, которая влияет на эффективность управления войсками и деятельностью Министерства обороны Украины и ВС Украины. На сегодняшний день внедрение информационных технологий несет несистематизированный характер. Одним из путей решения проблемы является построение единого ядра информационной инфраструктуры для МО Украины и ВС Украины.

Ключевые слова: информационные технологии; ИТ-инфраструктура; комплексная система защиты информации; информационные системы; информационно-аналитические системы.

K.Sokolov[1];
O.Hudyma, Ph.D[1];
V.Tkachenko, Ph.D[2];
O.Shyyatyy[1]

[1] - Department of Information Technology of the Ministry of Defense of Ukraine, Kyiv;

[2] - Center for Military and Strategic Studies National Defence University of Ukraine named after Ivan Chernyhovskij, Kyiv

Main directions of creation of IT infrastructure of the Ministry of Defense of Ukraine

Resume. The problem of information technology in the MD of Ukraine, which affects the efficiency of management and operations of the troops of the MD Ukraine and the AF of Ukraine. To date, implementation of IT is unstructured nature. One way to solve the problem is to build a single core information infrastructure for the Ministry of Defense of Ukraine and the Armed Forces of Ukraine.

Keywords: information technology; IT infrastructure; system of information security; information system; information-annalistic system.