УДК 623.7

Дмитро Євгенович Заклевський *(канд. техн. наук, провідний науковий співробітник)*
Олег Васильович Юрченко *(канд. техн. наук, головний науковий співробітник)*

Військова частина А0251, Київ

ПОРІВНЯЛЬНИЙ АНАЛІЗ ПЕРЕЛІКІВ MCTL ТА DSTL США

Проаналізовано функціонування програми військових критичних технологій США МСТР. Проведено порівняльний аналіз розділу переліку військових критичних технологій MCTL та розділу переліку наукових напрямів і технологій, що розробляються, DSTL. Коротко описано структуру та зміст переліків, розглянуто їхні спільні риси та відмінності. Зосереджено увагу на паспортах технологій, які є ключовими елементами зазначених переліків. Розглянуто деякі поняття, які використовуються у сфері військових інформаційних технологій та інформаційної безпеки США. Розкрито специфічні моменти формування та підтримання переліків у актуальному стані. Запропоновано шляхи використання досвіду США для України.

Ключові слова: *перелік військових критичних технологій; перелік наукових напрямів і технологій, що розробляються; інформаційні технології; інформаційна безпека.*

Найважливішою умовою ефективної реалізації державної науково-технічної політики є концентрація наукового потенціалу, фінансових і матеріальних ресурсів на пріоритетних напрямах розвитку науки і техніки. Під пріоритетними напрямами розвитку науки і техніки розуміються основні галузі досліджень і розробок, реалізація яких повинна забезпечити значний внесок у соціальний, науково-технічний та промисловий розвиток країни і в досягнення за рахунок цього національних соціально-економічних цілей.

Як уже зазначалося у статті [1], Міністерством оборони США (МО США) терміном "критичні технології" окреслюються технології, здатні гарантувати переваги систем озброєння США. З цією метою МО США реалізує довготривалу програму військових критичних технологій (МСТР– Military Critical Technologies Program).

Результатами функціонування програми військових критичних технологій є переліки MCTL і DSTL:

а) перелік військових критичних технологій (MCTL – Military Critical Technologies List);

б) перелік наукових напрямів і технологій, що розробляються (DSTL – Developing Science and Technologies List).

MCTL – це каталог технологій і виробів, здатних забезпечити у перспективі найважливіші досягнення у розробці, виробництві і використанні військових можливостей. Він містить детальні описи технологічних областей, найважливіших з точки зору забезпечення переваги американських систем озброєння або зниження витрат на ці системи.

DSTL – це каталог науково-технологічних напрямів, які розробляються в усьому світі і здатні суттєво підвищити або знизити військові можливості США. Головна увага приділяється технологіям, які зароджуються, містить фундаментальні та прикладні дослідження.

Метою статті є порівняльний аналіз переліків MCTL та DSTL США, їх структури та змісту, розгляд деяких понять, використовуваних у сфері військових інформаційних технологій та інформаційної безпеки США, а також розроблення пропозицій щодо формування переліків військових критичних технологій в Україні.

Зазначимо, що для ідентифікації і захисту критичних технологій урядом США підтримується низка державних програм. До цих програм належать ті, що регулюють експорт товарів оборонного призначення і контролюють імпорт американських компаній, які працюють у сфері національної безпеки. До участі в цих програмах залучається низка федеральних агентств. У 2007 році Рахункова палата США віднесла ці програми до критично важливих для інтересів національної безпеки США (Рис. 1) [2].

Загалом MCTL містить більше 500 паспортів технологій. Як показано в таблиці 1, кількість паспортів технологій у кожному розділі змінюється в межах від 2 у біомедичних технологіях до 78 у лазерних, оптичних та сенсорних технологіях. DSTL включає в себе фундаментальні, прикладні дослідження та передові технологічні розробки. Після відпрацювання та/або впровадження технології переходять із переліку DSTL до MCTL [2].

Спільні риси обох переліків. Вступна частина будь-якого розділу переліку DSTL і переліку MCTL є ідентичною. Інформацію, яка міститься у вступній частині, розділено на 4 параграфи, від A до D.

У параграфі А коротко описується сутність програми МСТР, порядок її реалізації та список двадцяти розділів переліків MCTL та DSTL. Варто зазначити, що найменування розділів обох переліків є однаковими і вже розкрито авторами у попередній статті [1]. Єдині найменування розділів свідчать про глибокий зв'язок між MCTL та DSTL і полегшують перехід технологій із розроблюваних до критичних у процесі науково-технічного розвитку.

Параграф В безпосередньо розкриває процедури розроблення та ведення переліків, надає узгоджений опис технологій, які військове відомство вважає істотно необхідними для проектування, розроблення, виробництва, експлуатації, застосування і технічного обслуговування виробу або послуги, що уможливлює істотний внесок у військовий потенціал будь-якої країни, в тому числі і США.

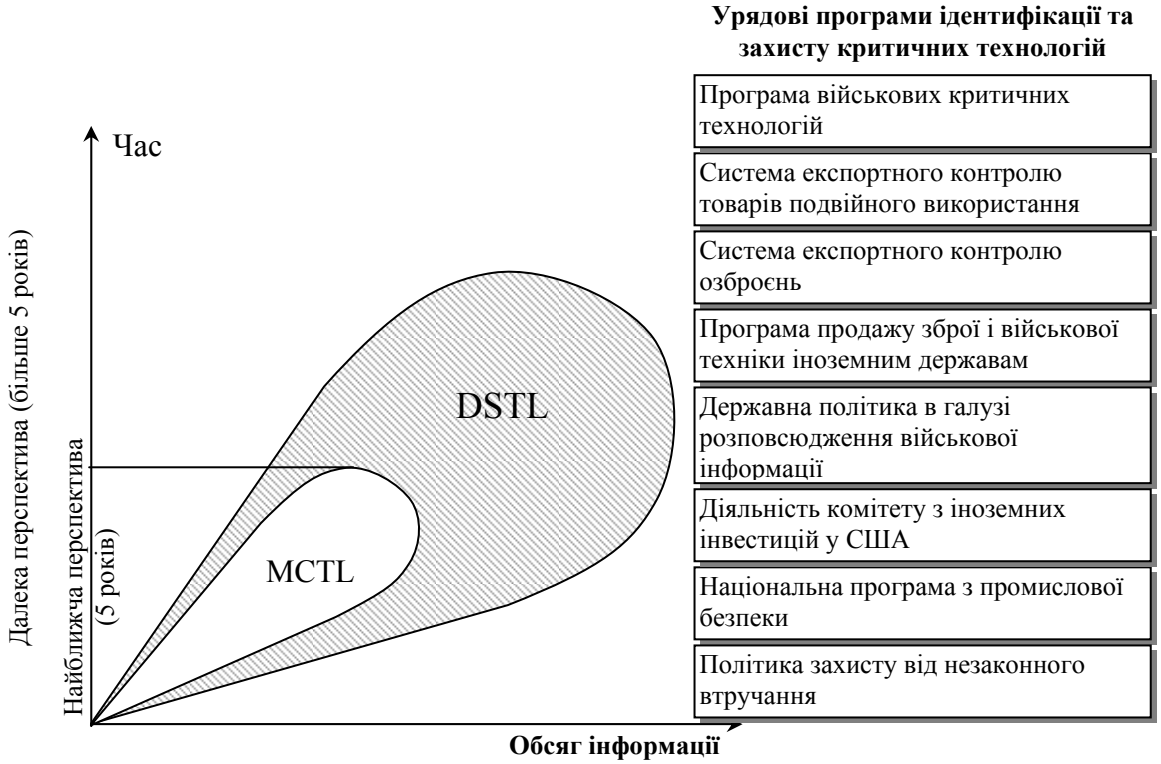


Рис. 1. Порівняльна оцінка відмінностей функціонального призначення каталогів MCTL і DSTL

Таблиця 1

Кількість паспортів технологій за розділами MCTL

№ з/п	Назва розділу	Кількість підрозділів	Кількість паспортів технологій
1.	Авіаційні технології	5	19
2.	Озброєння та високоенергетичні матеріали	13	53
3.	Біологічні технології	4	14
4.	Біомедичні технології	2	2
5.	Хімічні технології	3	19
6.	Технології систем спрямованої енергії	2	9
7.	Технології систем енергетики	4	25
8.	Технології електроніки	5	47
9.	Технології наземних систем	3	3
10.	Технології інформаційних систем	6	25
11.	Лазерні, оптичні та сенсорні технології	9	78
12.	Технології виробництва та обробки	6	50
13.	Технології морських систем	5	34
14.	Технології обробки матеріалів	3	26
15.	Ядерні технології	2	6
16.	Технології позиціонування, навігації та часу	5	30
17.	Технології інформаційної безпеки	3	16
18.	Технології управління сигнатурою	3	22
19.	Технології космічних систем	12	61
20.	Технології ефектів озброєння	4	29

Параграф С визначає правову основу для переліку критичних технологій; у ньому перераховано юридичні підстави створення переліку.

У параграфі D описано використання переліків, зазначається, що вони не є переліками товарів і технологій, які підлягають експортному контролю. Якщо якісь вироби визначаються військовими як критичні, то технології їх розробки та виробництва також рекомендуються для контролю.

Передмова складається із двох параграфів.

У параграфі А описується структура переліків.

Кожен розділ містить підрозділи, присвячені конкретним технологічним напрямам. Вступна частина розділу містить такі складові:

Сфера застосування – визначає технологічні групи, які розглядаються у розділі. Кожна група розглядається в окремому підрозділі.

Основна інформація – визначає ключові елементи розділу.

Огляд – розглядає групи технологій, визначених сферою застосування.

Довідкова інформація – містить додаткову інформацію.

Кожна група технологій, визначених сферою застосування, містить підрозділ, що містить таке:

Основна інформація – визначає ключові елементи підрозділу.

Огляд – визначає і розглядає технології, перераховані в паспортах, що слідують.

Довідкова інформація – містить додаткову інформацію.

Паспорти технологій містять дані щодо окремих критичних технологій. Основні числові значення наводяться у графі "*параметр(и) критичної технології*". Саме тут визначається, де

технологія дозволить досягти значних успіхів у розробці, виробництві і використовуванні військових можливостей.

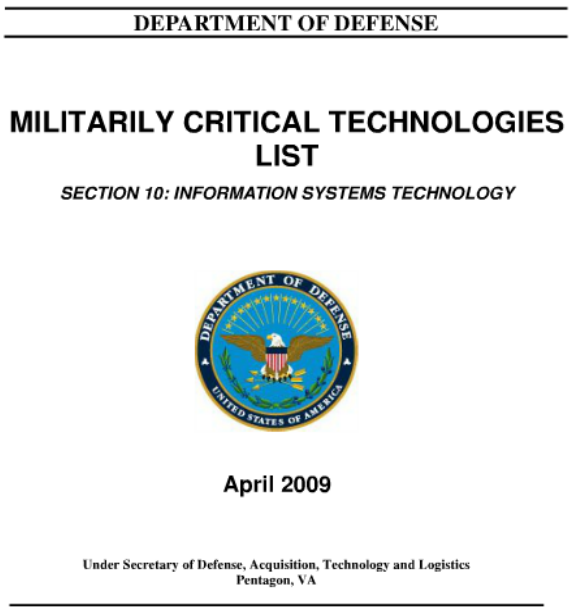
Параграф В містить загальний опис і структуру паспортів технологій. У ньому міститься детальна параметрична інформація для служб експортного контролю, яка буде розглянута далі у самих паспортах технологій.

Аналіз структури і змісту переліку MCTL проведемо на прикладі розділу 10 "Технології інформаційних систем" (Рис. 2) [3].

До сфери застосування технологій за розділом 10 "Технології інформаційних систем" належать такі:

10.1. "Технології збору даних".
10.2. "Технології обробки даних".
10.3. "Технології обробки інформації".
10.4. "Людино-машинні системи".
10.5. "Передача інформації та комунікації".
10.6. "Інформаційні операції".

У параграфі "Основна інформація" зазначається:


DEPARTMENT OF DEFENSE

MILITARILY CRITICAL TECHNOLOGIES LIST

SECTION 10: INFORMATION SYSTEMS TECHNOLOGY

April 2009

Under Secretary of Defense, Acquisition, Technology and Logistics
Pentagon, VA

Рис. 2. Титульний аркуш розділу 10 "Технології інформаційних систем"

доступ до інформації є критично важливим для успіху мережево-центричних бойових дій та забезпечення солдата на полі бою інформацією про бойову обстановку;

збір та узагальнення даних є критичною технологією для розвитку глобальної інформаційної мережі (ГІМ) і для виконання вимог мережево-центричних бойових дій;

польові командири повинні будуть покладатися на технології обробки інформації для навчання та прийняття рішень на полі бою;

технології сфери передачі інформації та комунікаційних можливостей також широко поширені і критичні для життєво-важливих операцій інфраструктури національної безпеки;

сучасна політична обстановка та тероризм роблять інформаційну систему головною мішенню для здійснення атак або використання у своїх цілях;

у той же час, сучасне апаратне забезпечення є легко доступним на міжнародному ринку;

як результат, виникає необхідність приділити увагу ідентифікації та персоналізації виключно військових масивів даних.

Назва "Технології інформаційних систем" (TIC) відображає міждисциплінарний характер критично важливих військових аспектів технології. На сучасному етапі розвитку техніки ця технологія включає в себе найважливіші аспекти апаратного та програмного забезпечення, причому більша частина апаратних засобів залежить від наявних комерційних технологій, що не піддаються ефективному експортному контролю. Є, однак, унікальні військові аспекти інформаційних технологій, пов'язані з володінням даними, інформацією або знаннями, незалежно від програмного/апаратного забезпечення, які впливають на індивідуальне та групове сприйняття в бойових умовах. У цьому розділі розглядаються критичні технології необхідні для отримання інформаційної переваги для збирання, обробки і передачі знань:

"Збір даних" включає в себе як отримання інформації з фізичного світу, за рахунок різних датчиків так і отримання інформації, яка генерується, повідомляється або отримується із баз даних у символьній формі. Він також спрямований на можливості інтеграції інформації, отриманої від датчиків різного типу.

"Технології обробки даних" стосуються засобів, за допомогою яких дані отримуються, зберігаються, відбувається керування ними та перетворення в інформацію. Об'єднуючою ланкою є залежність від пропускної здатності техніки на сучасному етапі. Так як об'єми пам'яті і потужності для зберігання даних збільшилися, методи для швидкого зберігання і пошуку інформації з великих, територіально розподілених наборів даних стають все більш важливими.

Складові:
обчислювальне апаратне забезпечення;
пристрої і методи обробки;
розробка програмного забезпечення.

На відміну від прямого маніпулювання даними "Технології обробки інформації" включають управління інформацією для ефективного формування і використання людських знань. Загалом, вони відрізняються від управління даними з акцентом на об'єктно-орієнтовані методи.

Складові:
розвиток знань;
імітаційне моделювання;
підтримка прийняття рішень.

Підрозділ "Людино-машинні системи" включає набір технологій, які необхідні для створення повної системи, в тому числі її людських елементів, для ефективної роботи в якості інтегрованої системи. Вона включає в себе методи для ефективного подання людського знання для виконання машиною своїх функцій, подання інформації для використання людиною, аспекти людського сприйняття і пізнання, які безпосередньо впливають на працездатність людини (індивідуальну та групову) як складової інформаційної системи, а також комп'ютерне моделювання діяльності людини.

Складові:
представлення (відображення) знань;
людино-машинні фізичні інтерфейси;
людське сприйняття і пізнання.

Технології "Передачі інформації та комунікацій" включають методи для електронної

передачі даних (аналогового або цифрового сигналу).

Складові:

розповсюдження даних та робота мереж;

телекомунікації (включно радіо- і телепередачі).

Критичні технології, пов'язані з керуванням мережею, підпадають під експортний контроль за розділом, що стосується інформаційної безпеки (розділ 17).

Підрозділ "Інформаційні операції" включає можливості інформаційного впливу на противника та його інформаційні системи, захищаючи власні інформаційні системи.

Складові:

інформаційний напад;

інформаційний захист;

електронна боротьба;

захист та живучість.

У "Довідковій інформації" зазначається, що ТІС відіграють ключову роль у багатьох аспектах військової справи: вбудовані комп'ютери, розподілені обчислення, підвищення швидкодії процесорів за рахунок використання оптичних, молекулярних (у тому числі біомолекулярних) або квантових методів обробки даних.

У параграфі *Основна інформація* підрозділу 10.6 "Інформаційні операції" зазначаються сучасні тренди цієї сфери: критична важливість захисту інформації; залежність від безперервності і точності інформації; загрози інформаційній системі з урахуванням світової політичної обстановки та з боку терористів; доступність технологій впливу на інформацію та програмних засобів для її злому через Інтернет; доступність технологій прямого електронного впливу на різні сенсори, елементи космічного зв'язку та прилади.

У параграфі *Огляд* наводяться визначення основних понять: інформаційні операції (оборонні та наступальні) та інформаційна боротьба; електронна боротьба та три її складові (електронний напад, електронний захист та підтримка електронної боротьби). Зазначається, що електронна боротьба згрупована з інформаційними операціями.

Параграф *Довідкова інформація* визначає тенденції розвитку інформаційних операцій: зростаюча доступність електронних компонентів; швидке просування ТІС практично в усіх сферах діяльності; зростаюча залежність від комерційних продуктів і технологій.

Підрозділ 10.6. "Інформаційні операції" містить шість паспортів технологій.

10.6-1 Інформаційний напад

10.6-2 Системна живучість та зміцнення, які пов'язані з електронною боротьбою (ЕБ)

10.6-3 Оптичні та інфрачервоні засоби попередження та контрзаходи

10.6-4 ЕБ – радарне попередження та перехоплення загроз

10.6-5 ЕБ – наступ (електронні контрзаходи)

10.6-6 Групова ідентифікація, свій-чужий

Окремо розглянемо паспорт технології 10.6-1 "Інформаційний напад". У вступі окреслюється застосування таких засобів як віруси, черв'яки, "троянські коні" для нападу на ворожі комп'ютерні мережі з метою виведення з ладу, псування або знищення даних та заволодіння критичною/важливою інформацією (таблиця 2).

Таблиця 2

Паспорт технології 10.6-1. "Інформаційний напад"

Критичні технологічні параметри	Інформаційний напад не піддається опису конкретними технологічними параметрами. Скоріше, він являє собою набір з інтелектуального ноу-хау та інструментів, які можуть бути застосовані для нападу практично на будь-який тип інформаційного ресурсу, що підключений до Інтернету
Критичні матеріали	Не визначено
Унікальні тести, обладнання для виробництва і перевірки	Не визначено
Унікальне програмне забезпечення	Хакерські інструментальні та програмні засоби, що можуть бути використані для нападу на американські військові засоби, або проти комерційних продуктів (інформаційних систем або підсистем), які знаходяться на озброєнні або плануються для використання збройними силами США
Важливе комерційне застосування	Інформаційна безпека, технологія для створення "троянських коней" і аналогічних законних функцій моніторингу і технічного обслуговування
Економічний ефект	Більшість критичних технологій доступні в Інтернеті
Документи експортного контролю	WA ML 11.a; USML XI(a)(4)

У параграфі *Довідкова інформація* зазначається, що цей паспорт технології розглядає ключові аспекти інформаційного нападу на системному рівні. Технології забезпечення інформаційної безпеки, як такої, розглядаються в розділі 17 MCTL, Технології інформаційної безпеки.

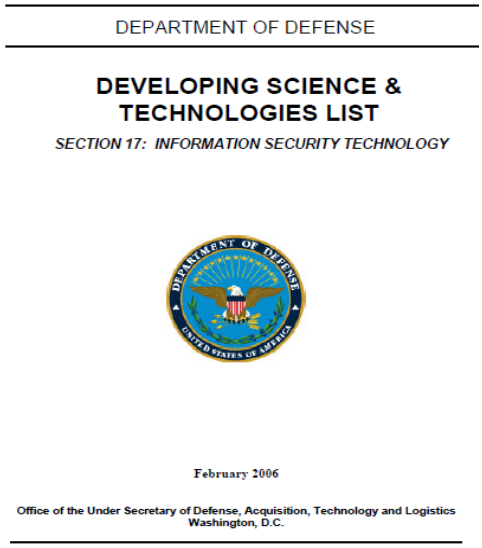
Серед найбільш розповсюджених методів зовнішнього нападу є: віруси, черв'яки, "Троянські коні" та комбіновані загрози. Режими атаки і цілі атак досить різноманітні. З точки зору інформаційних операцій цілі включають: відключення або погіршення якості сервісів, як правило, через перенасичення або вимкнення критично важливих інформаційних ресурсів, злам або знищення даних та заволодіння критичною/важливою інформацією.

Аналіз переліку DSTL проведемо на основі розділу 17 "Технології інформаційної безпеки", виданому у 2006 році [4] (Рис. 3).

Перелік DSTL фокусується на світових державних і комерційних наукових і технологічних розробках, які мають потенціал, щоб значно поліпшити або погіршити американський військовий потенціал у майбутньому. До нього включається нові та перспективні технології, а також ті, які можуть бути модернізовані і інтегровані завдяки технологічним досягненням. Він визначає значення і параметри технологій і охоплює спектр технологій з усього світу.

DSTL використовується в якості довідкової інформації при розробленні міжнародних програм співробітництва з розвитку технологій.

Розділ 17 "Технології інформаційної безпеки" складається з двох підрозділів: 17.1. "Криптологія" та 17.2. "Криптографічні протоколи та методики".


DEPARTMENT OF DEFENSE

DEVELOPING SCIENCE & TECHNOLOGIES LIST

SECTION 17: INFORMATION SECURITY TECHNOLOGY

February 2006

Office of the Under Secretary of Defense, Acquisition, Technology and Logistics
Washington, D.C.

Рис. 3. Титульний аркуш розділу 17 “Технології інформаційної безпеки”

У параграфі *Сфера застосування* розділу 17 розкриваються основні аспекти сфери застосування технологій; визначаються ключові компоненти захищеної інформації та систем захисту інфраструктури (персонал, засоби, обладнання, стандарти, навчання, програми випробовування і оцінювання систем безпеки, а також оборонні інформаційні операції та безпека операцій); зазначається важливість інформаційної безпеки в умовах переходу збройних сил до концепції мережецентричних бойових дій.

У *Огляді* зазначається, що інформаційна безпека охоплює ширшу сферу ніж технології та вироби, описані в цьому розділі; визначається зв’язок цього розділу з іншими (“Інформаційні технології” (розділ 10) та “Технології позиціонування, навігації і часу” (розділ 16)).

Країни-підписанти Вассенаарської домовленості визначають “Інформаційну безпеку” як засоби і функції, що забезпечують доступність, конфіденційність або цілісність інформації або зв’язку, виключаючи засоби і функції, призначені для захисту від збоїв. До них відносяться криптографія, криптоаналіз, захист від викриваючих випромінювань і комп’ютерна безпека [5]. *Огляд* містить також визначення понять сфери інформаційної безпеки та цитати з різних друкованих джерел щодо місця технологій інформаційної безпеки у структурі національної безпеки, боротьби з тероризмом, захисті національної інфраструктури. Крім того, відзначається важливість рівня відбору і підготовки персоналу, який управляє і використовує систему інформаційної безпеки.

У параграфі *Довідкова інформація* зазначається, що інформаційна безпека, як правило, розглядається в якості найважливішої функціональної області, сегментованої системи або функції всіх військових інформаційних систем і більшості цивільних систем, які вимагають унікальних, емпірично підтверджених застосуванням комплексів системного проектування та комплексування, методів і програмного забезпечення в процесі розробки, виробництва і життєвого циклу експлуатації сегментів інформаційної безпеки в захищених інформаційних системах.

Підрозділи 17.1 і 17.2 містять по сім паспортів технологій.

Розглянемо паспорт технології 17.2-7. “Цифрова стеганографія даних” (таблиця 3).

У вступі до паспорту зазначається, що стеганографія є розділом криптології, яка вивчає приховування існування даних за рахунок використання прихованих каналів. Незашифрований текст або зашифрована інформація можуть бути випадковим чином вбудовані в шум квантування цифрових зображень або інших неточних цифрових файлів даних без помітного збільшення розміру “файлу-господаря”.

Таблиця 3

Паспорт технології 17.2-7. “Цифрова стеганографія даних”

Параметр(и) технології	Виявити визначену точку у прикладному біометричному масштабі, в якому вкладені приховані дані знаходяться нижче порогу виявлення для кожного типу цифрових даних (наприклад, 2 біти інформації на піксель у 8-бітних файлах зображень, призначених для людського ока). При такому рівні файл зображення може містити 5–10 відсотків випадково вбудованої інформації встановлених перш ніж вона стане такою, що може бути візуально або статистично виявленою.
Критичні матеріали	Не визначені
Унікальне випробувальне, виробниче та діагностичне обладнання	Високопродуктивні комп’ютери, спеціально розроблені для виконання статистичних тестів для визначення здатності піддаватися виявленню замаскованих або прихованих даних у процесі розроблення, тестування та оцінювання цифрових стеганографічних систем
Унікальне програмне забезпечення	Системи проектування та комплексування програм створення цифрових стеганографічних зображень, інтерфейси користувача, протоколи, алгоритми і вбудовані генератори повинні мати нуль дефектів і відповідати “Вимогам до безпеки криптографічних модулів” (FIPS PUB 140-2).
Основне комерційне застосування	Ключовими факторами розвитку технології є розвиток комерційних продуктів і вимог до них: персональні і комерційні стеганографічні додатки для нанесення водяних знаків та вкладення закритих даних в зображення, відео-, аудіо-, або текстові файли для аутентифікації, захисту авторського права і патентного захисту; дослідницькі прототипи та експериментальні додатки є визначальними факторами для цієї технології; сучасний стеганографічний ринок, заснований на цифрових зображеннях, має потенціал до розширення для захисту інтелектуальної власності

Споживчі можливості (доступність)	Доступність не повинна бути основною проблемою придбання для програмних продуктів створення цифрових стеганографічних зображень. Нові конкурентні продукти цього класу, які відповідають військовим вимогам, продовжують з'являтися на відкритому ринку. Якщо такі продукти відповідають військовим вимогам, то їхня адаптація та інтеграція коштує дешевше ніж розроблення на замовлення і може усунути потреби з інвентаризації, зберігання, а також пов'язані з цим витрати життєвого циклу. Тим не менше, вартість додаткового персоналу для управління та підтримки стеганографічної функціональності для великих складних систем може вимагати серйозних витрат. Більшість функцій можуть бути автоматизовані, однак, є ще потенційно дорогі вимоги для залучення й утримання технічно кваліфікованого, надійного і відповідального персоналу для роботи, управління і підтримки навчання кінцевих користувачів, стандартизації і програм тестування та оцінювання, необхідних для оптимальної експлуатації інформаційної системи безпеки

У довідковій інформації до паспорту зазначається, що графічна стеганографія може бути використана для приховування зашифрованих повідомлень. Методика об'єднання графічної стеганографії і шифрування або множинного шифрування може представляти проблему для національної безпеки і криптоаналітиків правоохоронних агентств. Навіть якщо відомо про існування повідомлення в електронному зображенні, потрібно ще ідентифікувати і виділити біти повідомлення для криптоаналізу. Процес відновлення відкритого тексту може вимагати багато часу або, навіть, бути нездійсненним.

Функціонування МСТР. У 2008 році на виконання інструкції № 3020.46 МО США взяло на себе зобов'язання кожні два роки здійснювати відбір і складати переліки критично важливих технологій, які використовуються при розробці науково-технічної та фінансової політики щодо розвитку озброєнь, а також оголосило плани міграції DSTL до MCTL [6].

Проте за даними рахункової палати [2] скорочення бюджетних видатків за програмою військових критичних технологій у 2011 році до 1,5 млн. долл (з 4 млн. долл. у попередньому році) призвело до припинення оновлення переліку. У подальшому МО США з березня 2011 року припинило доступ до публічної версії переліку через Інтернет, розміщеної на сайті міноборони, та оприлюднило попередження про те, що закрита версія MCTL також не оновлюється і може використовуватися лише у інформаційних цілях (таблиця 4). У той же час офіційними особами визнається, що у деяких випадках інформація встигала застаріти ще за час публікації відповідного каталогу. За аналогією з MCTL перелік розроблюваних технологій DSTL також визнано застарілим: станом на початок 2013 року два розділи не оновлювалися з 1999 року.

Таблиця 4

Оновлення розділів MCTL за календарними роками

Розділ	Роки					
	2007	2008	2009	2010	2011	2012
Авіаційні технології			+			
Озброєння та високоенергетичні матеріали		+	+			
Біологічні технології		+				
Біомедичні технології			+			
Хімічні технології			+			
Технології систем спрямованої енергії			+			
Технології систем енергетики			+			
Технології електроніки			+			
Технології наземних систем	+			+		
Технології інформаційних систем			+			
Лазерні, оптичні та сенсорні технології	+			+		
Технології виробництва та обробки	+		+			
Технології морських систем			+			
Технології обробки матеріалів	+		+			
Ядерні технології			+			
Технології позиціонування, навігації та часу			+			
Технології інформаційної безпеки			+			
Технології управління сигнатурою		+	+			
Технології космічних систем		+				+
Технології ефектів озброєння				+		

Складності з оновленням переліків критичних технологій свідчать про необхідність розроблення спрощених (дешевих) процедур ідентифікації критичних технологій. На думку авторів, при розробленні програми оборонних ключових технологій в Україні доцільно розробити спрощені процедури відбору технологій і, водночас, жорсткі вимоги до термінів оновлення переліків. Проте, на теперішній час одні технології знаходяться у стадії бурхливого розвитку (інформаційні технології, нанотехнології, робототехніка, лазери тощо), а інші переживають стадію сталого розвитку. Отже, інтервали оновлення деяких каталогів можуть варіюватися.

Враховуючи оборонну спрямованість Воєнної доктрини України, економічний потенціал, можливості оборонно-промислового комплексу, автори вважають недоцільним у найближчій перспективі сформувати і підтримувати в актуальному стані повний перелік оборонних ключових технологій, аналогічний переліку США. У цьому сенсі кориснішим буде досвід прогнозних

досліджень у Чехії 2001 року, які проводилися під егідою міністерства освіти, молоді та спорту. За результатами проведеної роботи повний національний перелік критичних технологій склав лише 90 найменувань [7]. Такий скорочений перелік дозволив би Міністерству оборони України визначити пріоритетні напрями розвитку озброєння та військової техніки, які мають високий потенціал для реалізації при оптимальному використанні обмежених коштів.

Крім того, у зв'язку із скороченням фінансування МО США заморожено плани щодо об'єднання переліків MCTL та DSTL. Рахунковою палатою зазначається, що для реалізації державних програм (рис. 1) деякими державними агентствами створено власні переліки на основі MCTL, а, наприклад, управління із захисту оборонних технологій МО США для оновлення переліку створило власну групу з 50 експертів. Для України також було б доцільно в процесі реалізації програми оборонних ключових технологій формувати єдиний перелік ключових і розроблюваних технологій, особливо враховуючи те, що один повинен витікати з одного. Тобто, перспективні технології з часом переходять у стан критичних, або не переходять ніколи.

Висновки

1. На думку авторів, при розробленні програми оборонних ключових технологій в Україні доцільно розробити спрощені процедури відбору технологій і жорсткі вимоги до термінів оновлення переліків. При цьому терміни оновлення переліків за деякими напрямами можуть бути зменшені для забезпечення їхньої актуальності.

2. Враховуючи низку військових, економічних і політичних факторів, автори вважають доцільним формувати скорочений перелік оборонних ключових технологій із залученням пріоритетних технологічних напрямів, а за окремими напрямами проводити прогнозні оборонні дослідження у кооперації з країнами-партнерами.

3. Для України було б доцільно в процесі реалізації програми оборонних ключових технологій формувати єдиний перелік ключових і розроблюваних технологій, особливо враховуючи те, що один повинен витікати з одного.

4. Формування переліків за зразком MCTL та DSTL потребує глибокого всебічного аналізу розвитку технологій як в Україні, так і в усьому світі, за кожним обраним технологічним напрямом. Для проведення такого аналізу повинні формуватися експертні групи із залученням досвідчених фахівців.

Література

1. Дихановський В.М. Критичні технології: сутність поняття та підходи до формування їх переліків / В.М. Дихановський, Д.Є. Заклевський, О.В. Юрченко // Наука і оборона.– 2013. – №4. – С. 42–45. **2. Protecting** defense technologies: DOD Assessment Needed to Determine Requirement for Critical Technologies List / GAO report to Congressional Committees, 2013. [Електронний ресурс]. – Режим доступу: http://www.gao.gov/products/GAO-13-157. **3. Militarily** Critical Technologies List. Section 10: Information Systems Technology [Електронний ресурс]. – Режим доступу: http://www.docstoc.com/docs/52404982/section-10---information-systems-technology. **4. Developing** science and technologies list. Section 17: Information security technology. – Office of the Under Secretary of Defense, Acquisition, Technology and Logistics Washington, D.C.–2006. – 49p. [Електроний ресурс].– Режим доступу: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.97.9420&rep=rep1&type=pd **5. The Wassenaar** Arrangement List of Dual-Use Goods and Technologies and Munitions List, WA-LIST (05) 1, 12-14-05.– [Електроний ресурс].– Режим доступу: http://www.wassenaar.org/list/wa-listTableOfContents.htm. **6. Department** of Defense Instruction № 3020.46. October 24, 2008 1. [Електронний ресурс]. – Режим доступу: http://www.hsdl.org/?view&did=233670. **7. Key** technologies for Czech National Research Programme / K.Klusacek.– Technology Foresight Summit, Budapest, UNIDO, 2007.

СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПЕРЕЧНЕЙ MCTL И DSTL США

Дмитрий Евгеньевич Заклевский *(канд. техн. наук, ведущий научный сотрудник)*
Олег Васильевич Юрченко *(канд. техн. наук, главный научный сотрудник)*

Воинская часть А0251, Киев

Проанализировано функционирование программы военных критических технологий США МСТР. Проведен сравнительный анализ раздела перечня военных критических технологий MCTL и раздела перечня научных направлений и технологий, что разрабатываются, DSTL. Кратко описана структура и содержание перечней, рассмотрены их общие черты и различия. Внимание сосредоточено на паспортах технологий, которые являются ключевыми элементами указанных перечней. Рассмотрены некоторые понятия, которые используются в сфере военных информационных технологий и информационной безопасности США. Раскрыты специфические моменты формирования и поддержания перечней в актуальном состоянии. Предложены пути использования опыта США для Украины.

Ключевые слова: *перечень военных критических технологий, перечень разрабатываемых научных направлений и технологий, информационные технологии, информационная безопасность.*

THE COMPARATIVE ANALYSIS OF MCTL AND DSTL OF THE USA

Dmytro Zaklevskyi *(Candidate of Technical Sciences, Leading Research Fellow of a Research Section)*
Oleg Yurchenko *(Candidate of Technical Sciences, Principle Research Fellow of a Research Section)*

Military Unit A0251, Kyiv

The functioning of the Military Critical Technologies Program is analyzed. Comparative analysis of the section of the Militarily Critical Technologies List and the section of the Developing Science and Technologies List is done. The structure and content of lists are briefly described, their similarities and differences are examined. The attention is focused on the Data Sheets, which are the key elements of these lists. Some concepts of the area of military information technology and information security of the USA are discussed. Specific moments of the formation and maintenance in actuality of lists are revealed. The ways of using the experience of the United States to Ukraine are suggested.

Key words: *the Militarily Critical Technologies List, the Developing Science and Technologies List, information technology, information security.*