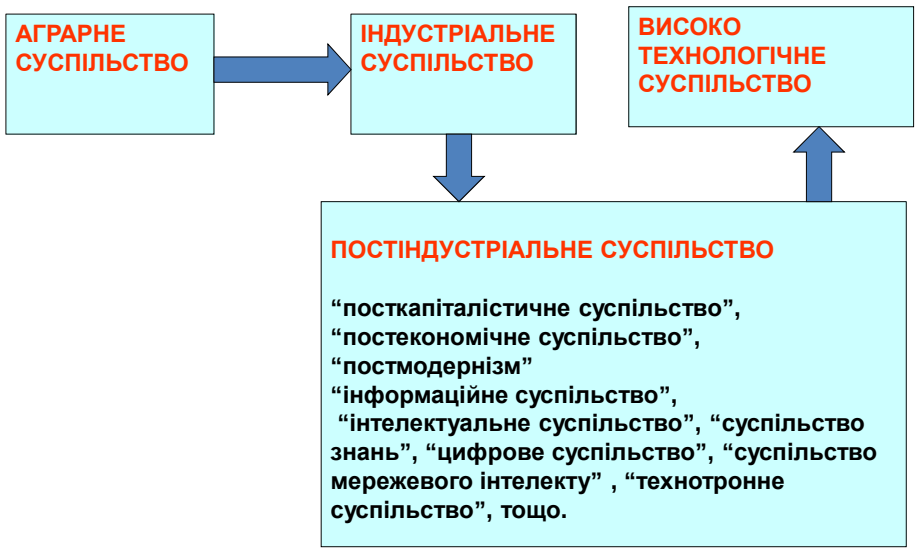
ДОПОВІДЬ
“Аспекти забезпечення кібернетичної безпеки у високотехнологічному суспільстві”

В ЯКІЙ СТАДІЇ СУСПІЛЬНОГО РОЗВИТКУ ЗНАХОДИТЬСЯ ЛЮДСТВО?



ВИСОКОТЕХНОЛОГІЧНЕ СУСПІЛЬСТВО

ВИСОКОТЕХНОЛОГІЧНЕ СУСПІЛЬСТВО - СУСПІЛЬСТВО, В ЯКОМУ:

основним предметом праці переважної більшості людей є високі технології;

знаряддям праці є продукти високих технологій;

засобами - високотехнологічна техніка;

основним видом діяльності переважної більшості людей є управління.

У розвинутих країнах вже сьогодні існуючі суспільні відносини багато в чому визначаються саме цією обставиною.

Відповідно економіка і суспільство орієнтовані на виробництво, насамперед, інноваційних високотехнологічних продуктів та їх продаж, як товару.

ВИСОКІ ТЕХНОЛОГІЇ:

До високих технологій (англ. high technology, hi-tech) традиційно відносять найбільш нові і прогресивні технології сучасності:

напівпровідникові технології;
космічні технології;
інформаційні технології;
інноваційні електромеханіку та електроніку;
нано- та біотехнології;
нові матеріали, «чисті» та енергозберігаючі технології (cleantech);
телекомунікаційні технології та технології управління і автоматизації;
інноваційні суто оборонні технології і технології подвійного призначення.

На цей час в світі існує більше 40 ключових макротехнологій, які за думкою провідних експертів визначають рівень економіки країн в сучасних умовах. Їх провідна роль обумовлена потужним інноваційним впливом як на національні економіки країн, так і на світову економіку в цілому.

КІБЕРНЕТИКА - НАУКА ПРО ЗАГАЛЬНІ ЗАКОНОМІРНОСТІ ПРОЦЕСІВ УПРАВЛІННЯ І ПЕРЕДАЧІ ІНФОРМАЦІЇ В ЖИВИХ ОРГАНІЗМАХ, СУСПІЛЬСТВІ ТА МАШИНАХ.

5

До поняття кіберпростору (еволюція поглядів, США):

Поняття "кіберпростір" (cyberspace), вперше використано у 1984 р. американським письменником Уіл'ямом Гібсоном для позначення усієї сукупності інформації, що міститься у комп'ютерних мережах.

З розвитком і розповсюдженням цифрових технологій поняття розширилось до позначення сукупності усіх електронних систем:

- Настанова КНШ США 2006 р. «Інформаційні операції»: «сфера, в якій застосовуються різні радіоелектронні засоби (зв'язку, радіолокації, розвідки, навігації, автоматизації, управління і наведення), у широкому діапазоні електромагнітного спектру для приймання, передавання, обробки, зберігання і обміну інформації, і відповідна інформаційна інфраструктура» (переважна позиція армії США).
- «Національна військова стратегія ведення операцій у кіберпросторі (2006): "середовище (сфера), в якому електронний і електромагнітний спектр використовується для зберігання, модифікації і обміну даними через мережеві системи і відповідні фізичні інфраструктури".
- Доктрина ВПС США «Операції у кіберпросторі» (2010): «глобальна сфера (домен) в інформаційному просторі - взаємопов'язана сукупність інфраструктур і інформаційних технологій: Інтернет, телекомунікаційні мережі, комп'ютерні системи, вбудовані в РЕС процесори і контролери».

До поняття кіберпростору (США):

«Кіберпростір складається із 4-х рівнів: інфраструктурного, фізичного, синтаксичного й семантичного; і контроль над одним рівнем не забезпечує контролю над іншими» (Джон Б. Шелдон, професор кіберстратегії Школи кіберборотьби Технологічного інституту ВПС, АвБ Райт-Паттерсон, Огайо).

«…Інфраструктурний рівень складається з радіоелектронної апаратури, ліній зв'язку, супутників, комп'ютерних мереж тощо. Фізичний рівень складається з всього того, що відноситься до ЕМС - електронів, фотонів, частот і т.п. - рівню, що дає життя, інфраструктурному. Синтаксичний рівень складається з формату інформації й правил, що направляють і контролюють інформаційні системи, що утворюють кіберпростір. Семантичний рівень складається з інформації, корисної й зрозумілої користувачеві - людині і, по суті, є зв'язкою кібернетичного й когнітивного.

Контроль над інфраструктурним рівнем кіберпростору необов'язково має на увазі контроль над фізичним, семантичним і синтаксичним рівнями. Семантичний контроль також не вимагає контролю інфраструктурного, про що на сьогоднішній день свідчить перевага кібер-злочинів, що ефективно використовують семантичний рівень. Останнє в цілому вірно, але залежно від поставленого завдання можуть бути виключення. Якщо маємо завдання зруйнувати й вивести з ладу мережу, атаки на інфраструктурний рівень може виявитися цілком достатньо. Якщо ж, з іншого боку, маємо завдання обманом змусити ворожого командира прийняти якісь рішення, контроль над інфраструктурним рівнем мало що дає, а от контроль над семантичним рівнем вирішує все».

Це визначає комплексний характер боротьби у кіберпросторі, що включає проведення усього спектру інформаційних операцій, у т.ч. психологічних операцій (інформаційно-психологічної протидії)!

Типова структура видових компонентів USCYBERCOM, до яких входять з'єднання:

- ✓мережевих операцій (network warfare);
- ✓інформаційних операцій (information operation);
- ✓радіоелектронної боротьби (electronic warfare);
- ✓підтримки і забезпечення операцій у кіберпросторі (combat communikations) (частини і підрозділи зв'язку і телекомунікаційних систем, радіоелектронної, космічної та інших технічних видів розвідки, технічного захисту інформації, криптографічної підтримки тощо);
- ✓операційні (командні) центри (operations center) (центри управління у кризових ситуаціях) тощо.

До поняття кіберпростору (Україна)

Кіберпростір – це простір (середовище) здійснення функцій управління в живих організмах, машино-технічних системах і суспільстві. Кіберпростір – це інформаційний простір (Центр воєнно-стратегічних досліджень).

Кіберпростір - віртуальний простір, сформований інформаційними, телекомунікаційними та інформаційно-телекомунікаційними системами (локальними комп'ютерами, локальними та глобальними мережами), у яких здійснюється виготовлення, зберігання, обробка, обмін та знищення інформації в електронному вигляді (СБ України).

Кіберпростір - середовище, сформоване у рамках поєднання віртуального і реального просторів, пов'язаних між собою інформаційних, комп'ютерних та телекомунікаційних систем, а також мережевих технологій цивільного та/або військового призначення, які в процесах обробки, передачі й зберігання інформації використовують електромагнітний спектр і діють як єдине ціле.

Кіберпростір – комунікаційний простір, який охоплює комп'ютерні мережі та електронні пристрої, що використовуються для збереження, обробки й обміну інформацією.

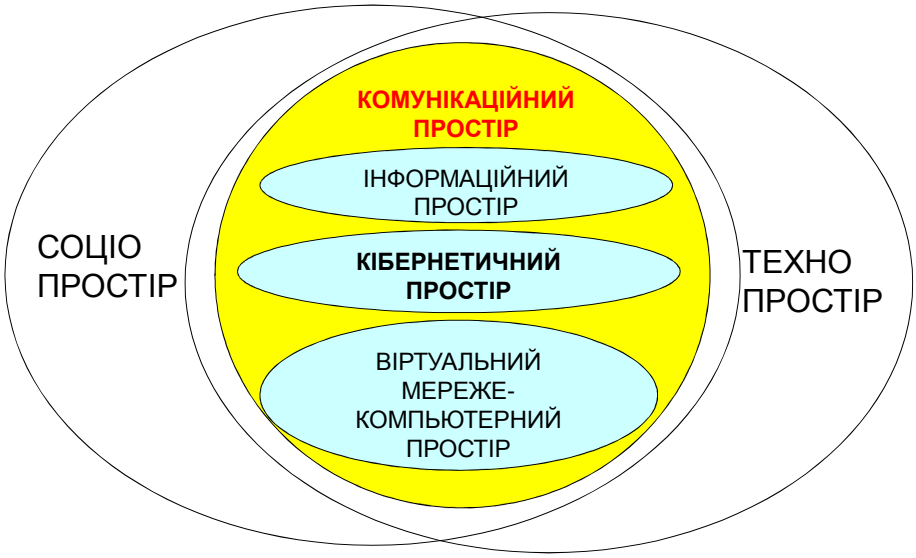
До поняття кіберпростору

Кібернетичний простір (КП, загальний аспект) – простір, у якому готуються і відбуваються процеси управління та здійснюються управлінські відносини. Складовими КП є комунікаційний, віртуальний комп'ютерно-мережний та соціотехнічний простори.

КП (військовий аспект) – єдиний простір, сформований об'єднанням системою зв'язків комунікаційного, віртуального комп'ютерно-мережного та соціотехнічного просторів, у якому відбувається створення, зберігання, модифікація та передача інформації, управління об'єктами (системами) та зброєю, вплив на об'єкти (системи) протидіючої сторони, захист власних об'єктів (систем) в існуючих полях і середовищах.

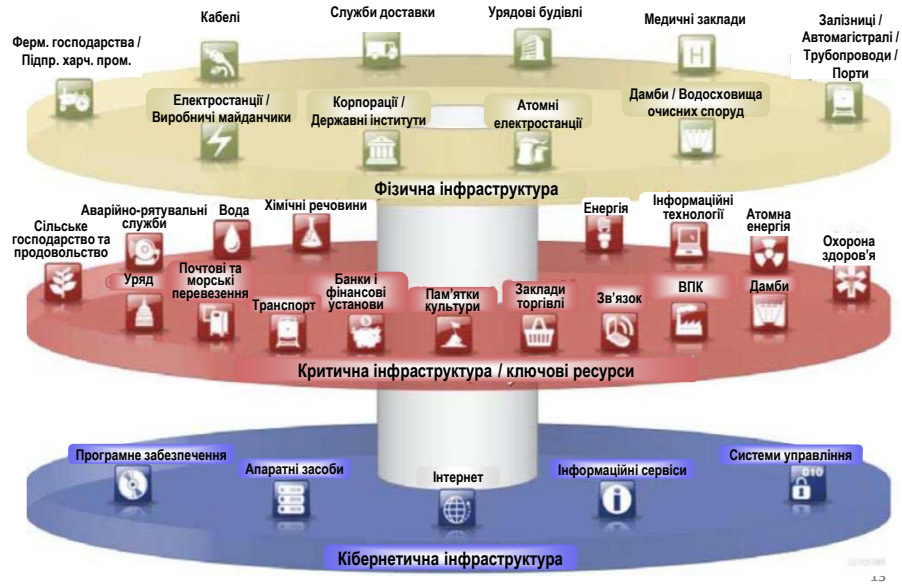
КІБЕРНЕТИЧНИЙ ПРОСТІР – ПРОСТІР В ЯКОМУ ГОТУЮТЬСЯ І ВІДБУВАЮТЬСЯ ПРОЦЕСИ УПРАВЛІННЯ ТА ЗДІЙСНЮЮТЬСЯ УПРАВЛІНСЬКІ ВІДНОСИНИ.

11



12

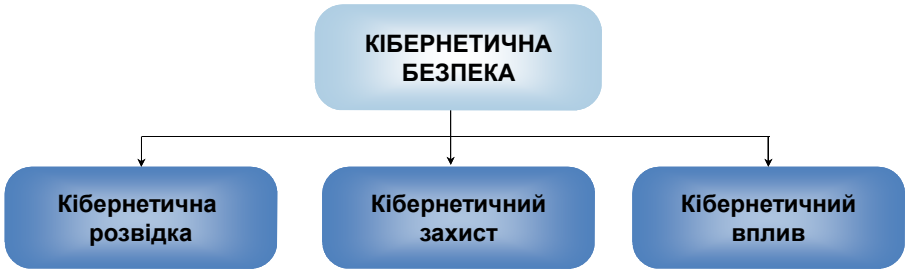
Перехід складових фізичної інфраструктури під контроль кібернетичної



КІБЕРНЕТИЧНА БЕЗПЕКА - СТАН ЗАХИЩЕНОСТІ УПРАВЛІННЯ В УСІХ СФЕРАХ (СОЦІАЛЬНІЙ, ТЕХНІЧНІЙ, СОЦІОТЕХНІЧНІЙ) ЗА ЯКОГО ЗАБЕЗПЕЧУЄТЬСЯ ЙОГО ЕФЕКТИВНЕ ЗДІЙСНЕННЯ

14

Складові кібернетичної безпеки



15

Складові кібернетичної безпеки

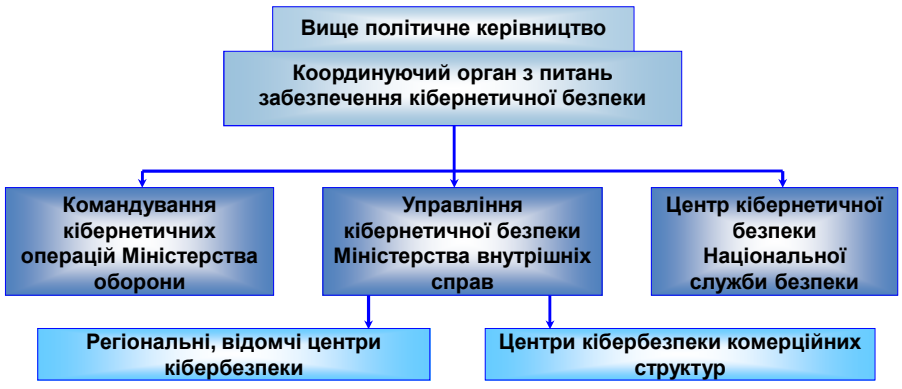
1. Кібернетична розвідка (КР) – добування інформації, наявної в КП, моніторинг кібернетичних систем та процесів, які в них протікають під час їх функціонування. КР базується на комплексному веденні за єдиним задумом і планом розвідки технічними засобами (радіоелектронної, космічної, повітряної, програмно-комп'ютерної, мереже-комп'ютерної тощо), розвідки з відкритих джерел та комплексної інтегральної обробки отриманих даних з метою викриття процесів управління в соціальній, технічній, соціотехнічній сферах та виявлення кібернетичного впливу противника.
2. Кібернетичний захист – сукупність організаційних, нормативно-правових та технічних заходів для забезпечення КБ. Його складові: апаратно-програмний захист; технічний захист інформації; радіоелектронний захист; інформаційно-психологічна протидія; інші заходи організаційного та нормативно-правового захисту.
3. Кібернетичний вплив – комплекс заходів на визначені елементи кіберпростору противника з метою порушення їх функціонування (стану). Його складові: програмно-комп'ютерний вплив; фізичний вплив на органи і системи управління; радіоелектронне подавлення (ураження); інформаційно-психологічний вплив тощо.

Умовний розподіл системи кібернетичної безпеки за рівнями та сферами безпеки

		Сфера				
		Інформаційна	Політична	Економічна	Воєнна	. . .
Рівень	Державний	Елемент СКБ	Елемент СКБ	Елемент СКБ	Елемент СКБ	
	Регіональний	Елемент СКБ	Елемент СКБ	Елемент СКБ	Елемент СКБ	
	Відомчий	Елемент СКБ	Елемент СКБ	Елемент СКБ	Елемент СКБ	

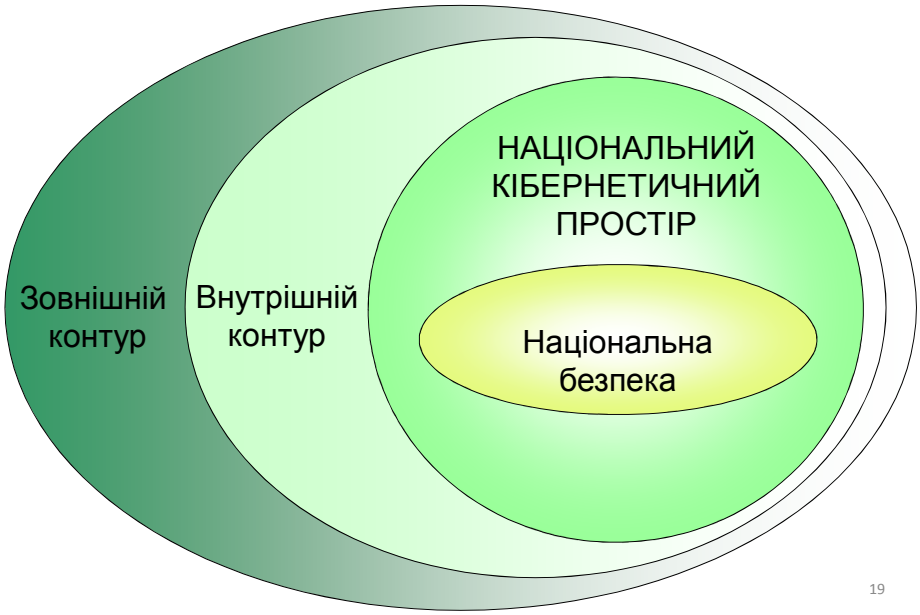
17

Узагальнена організаційна структура системи кібернетичної безпеки



18

Контури кібернетичної безпеки



19

Проблеми забезпечення кібербезпеки

1. Відсутність чіткого усвідомлення ролі та значення кібербезпекової складової у системі забезпечення національної безпеки держави.
2. Дифініційна, термінологічна та нормативно-правова невизначеність у сфері кібернетичної безпеки.
3. Відсутність належної координації діяльності відповідних відомств та як наслідок неузгодженість дій зі створення окремих елементів СКБ.
4. Залежність держави від програмних та технічних продуктів іноземного виробництва.
5. Складнощі із методичним забезпеченням та кадровим наповненням відповідних структурних підрозділів.

20

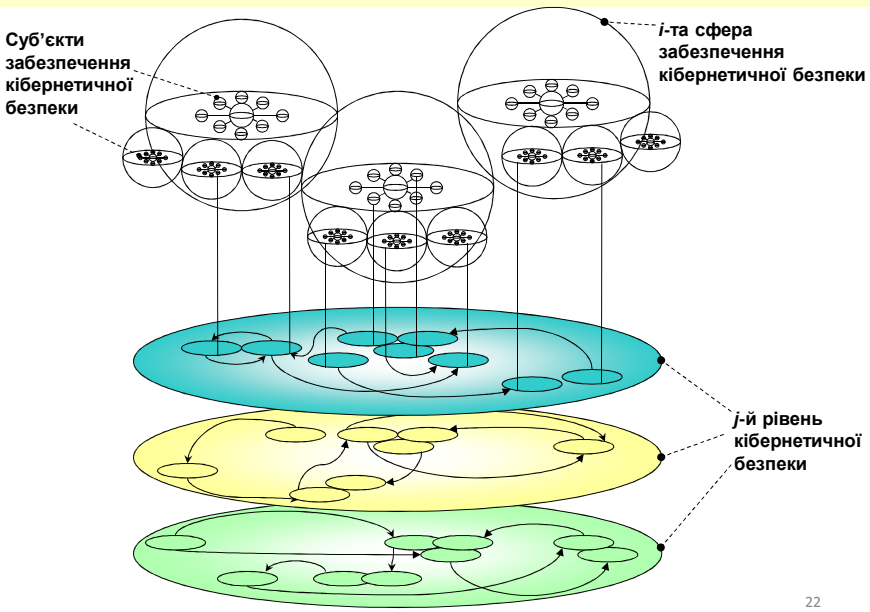
Комплексна сутність кібернетичної безпеки

КІБЕРНЕТИЧНА БЕЗПЕКА

Аспекти	Сфери	Рівні
•соціальний; •технічний; •інформаційний; •комунікаційний.	•зовнішньополітична; •державної безпеки; •воєнна; •внутрішньополітична; •економічна; •соціальна та гуманітарна; •науково-технологічна; •екологічна.	•нормативно-правовий; •організаційний; •технічний; •методичний.

21

Сфери та рівні кібернетичної безпеки



22

Прискорений розвиток світового інформаційного суспільства, інтенсивне впровадження складних інтегрованих систем управління усіх рівнів (складних кібернетичних систем) суттєво підвищує значення систем кібернетичної безпеки (СКБ).

Більше 70 країн готові до дій у кібернетичному просторі, перші з них: США, Китай, Росія, Ізраїль та Франція. Тільки у 2007-2012 роках цілісні національні СКБ чи їх елементи створені у США, КНР, Франції, Великобританії, Германії, Росії, Ізраїлі, Австралії, Кореї, Естонії та ін.

Провідні країни світу на даний час:

✓сформували підходи до нормативно-правового визначення кіберпростору як простору війни, прийняли національні та коаліційні нормативні документи у сфері кібернетичної безпеки;

✓розгорнули галузеві компоненти національних СКБ та проводять їх бойове злагодження через систему національних і коаліційних (міжнародних) навчань;

✓створили власні системи підготовки військових фахівців КБ.

Прискорений розвиток національних і коаліційних СКБ США, НАТО інших провідних країн визначив деякі спільні підходи до їх організації:

✓інтеграція національних СКБ (їх елементів) на коаліційному рівні (країни НАТО з 2011 року, країни ОДКБ – на перспективу розвитку коаліційної СКБ);

✓інтеграція галузевих елементів національних СКБ на основі централізації управління на державному рівні;

✓комплексний характер організаційної структури воєнних компонентів СКБ. Створені СКБ виконують широкий спектр завдань, не обмежуючись тільки спеціальними мережними операціями. В їх компетенції: інформаційні операції в цілому; здійснення інформаційно-психологічного впливу; кібернетична розвідка (технічна розвідка різних видів); радіоелектронна боротьба (РЕБ); захист інформаційних систем; підтримання функціонування інтегрованих систем управління збройними силами та системами озброєння тощо.


ЖВІНАУ
ДЯКУЮ ЗА УВАГУ!