Житомирська політехніка	Міністерство освіти і науки України Державний університет «Житомирська політехніка»

ЛЕКЦІЯ 14

Інформаційне протиборство

Лобанчикова Н.М.

ОСНОВНІ ПОНЯТТЯ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Інформаційна війна [information warfare] розглядається як комплекс підходів і операцій, спрямованих на забезпечення інформаційної переваги по підношенню до потенційного або реального противника

інформаційне протиборство [information confrontation], яке характеризується, з однієї сторони, впливом на системи добування, обробка, розповсюдження та зберігання інформації противника, а з іншої - застосуванням заходів захисту своїх подібних систем від деструктивного та керуючого впливу.

Інформаційна війна належить до великих інформаційних технологій соціального впливу з метою дестабілізації ситуації, в якій перебуває опонент, зміни масової свідомості ворога, послаблення його позицій.

ОСНОВНІ ПОНЯТТЯ ІНФОРМАЦІЙ НОГО ПРОТИБОРСТ ВА

Перше і головне завдання інформаційних агресій полягає в маніпулюванні масами, у впливі на еліту певних держав або й своєї країни.

- внесенні у суспільну

та індивідуальну свідомість ворожих, шкідливих ідей та поглядів;

- дезорієнтації та дезінформації мас;
- послабленні певних переконань, устоїв;
- залякуванні свого народу образом ворога;
- залякуванні супротивника своєю могутністю;
- підрив морально-політичного стану особового складу збройних сил і населення противника, паралізація їх волі до боротьби;
- мобілізація свого населення на широку підтримку військових дій, сковування пацифістських настроїв та виступів;
- забезпечення моральної підтримки дій своїх військ збройними силами та населенням союзників;
- введення супротивника в оману, дезінформація суспільної свідомості з метою приховування істинних замислів.

ОСНОВНІ ПОНЯТТЯ ІНФОРМАЦІЙ НОГО ПРОТИБОРСТ ВА

Метою інформаційної війни є послаблення моральних і матеріальних сил супротивника, посилення власних.

Вона передбачає заходи пропагандистського впливу на свідомість людини в ідеологічній та емоційній галузях.

ІВ охоплюють наступні області:
1) інфраструктуру систем життєзабезпечення країни-телекомунікації, транспортні мережі, електростанції, банківські системи тощо;
2) промислове шпигунство -розкрадання патентованої інформації, спотворення або знищення особливо важливих даних, послуг; збір інформації тощо;
3) злам і використання особистих паролів VIP-персон, ідентифікаційних номерів, банківських рахунків, даних конфіденційного плану, виробництво дезінформації;

4) електронне втручання в процеси командування і управління військовими об'єктами і системами, "штабна війна", виведення з ладу мереж військових комунікацій;
5) всесвітня комп'ютерна мережа Інтернет, в якій, за деякими оцінками, діють 150.000 військових комп'ютерів, і 95% військових ліній зв'язку проходять за відкритими телефонними лініями.

ДО СКЛАДОВИХ ЧАСТИН ІНФОРМАЦІЙНОЇ ВІЙНИ НАЛЕЖАТЬ:

1) психологічні операції - використання інформації для впливу на аргументацію солдатів ворога.
2) електронна війна - не дозволяє супротивнику отримати точну інформацію.
3) дезінформація - надає ворогові неправдиву інформацію про наші сили і наміри
4) фізичне руйнування - може бути частиною інформаційної війни, якщо має на меті вплив на елементи інформаційних систем.
5) заходи безпеки - прагнуть уникнути того, щоб ворог дізнався про наші можливості та наміри.
6) прямі інформаційні атаки - пряме перекручування інформації без видимої зміни сутності.

Серед основних засобів, що застосовуються в процесі інформаційної війни, можна відзначити інформаційно-психологічні та інформаційно-комп'ютерні впливи, а також радіоелектронну боротьбу.

КОНЦЕПЦІЯ ІНФОРМАЦІЙНОЇ ВІЙНИ

- **Концепція інформаційної війни** [information warfare conception] — це система поглядів на інформаційну війну та шляхи її ведення.
- **Включає**:
  - заглушення елементів інфраструктури державного і воєнного управління; електромагнітний вплив на елементи інформаційних і комунікаційних систем (РЕБ);
  - одержання розвідувальної інформації шляхом перехоплення і декодування (дешифрування) інформаційних потоків, що передаються каналами зв'язку, а також побічним випромінюванням і за рахунок спеціально впроваджених у приміщення технічних засобів і електронних пристроїв перехоплення інформації (радіоелектронна розвідка);
  - здійснення несанкціонованого доступу до інформаційних ресурсів (шляхом використання програмно-апаратних засобів зламу систем захисту інформаційних і телекомунікаційних мереж противника) із наступним їх спотворенням, знищенням або викраденням чи порушенням нормального функціонування цих систем, (“хакерна війна”);
  - формування і масове розповсюдження інформаційними каналами противника або глобальними мережами інформаційної взаємодії дезінформації або тенденційної інформації для впливу на оцінки, наміри і орієнтацію населення і осіб, що приймають рішення (психологічна війна); одержання необхідної інформації шляхом перехоплення і обробки відкритої інформації, що передається незахищеними каналами зв'язку або циркулює в інформаційних системах, а також опублікованої у засобах масової інформації.

СИСТЕМА КІБЕРНЕТИЧНИХ ДІЙ

- Система кібернетичних дій – це сукупність взаємопов'язаних підсистем кібернетичної розвідки, кібернетичного захисту та кібернетичного впливу, які утворюють єдину цілісну систему на яку покладаються функції із забезпечення кібернетичної безпеки людини, суспільства та держави.

- Кіберрозвідка – дії з використанням окремого комп'ютера чи взаємозалежних інформаційно-керуючих систем, що передбачають збір розвідданих або забезпечення реалізації окремих розвідувальних завдань як в кібернетичному, так і в реальному просторі.

/Погляди МО США на забезпечення національної безпеки в кіберпросторі/

ОСНОВИ КІБЕРНЕТИЧНОЇ РОЗВІДКИ

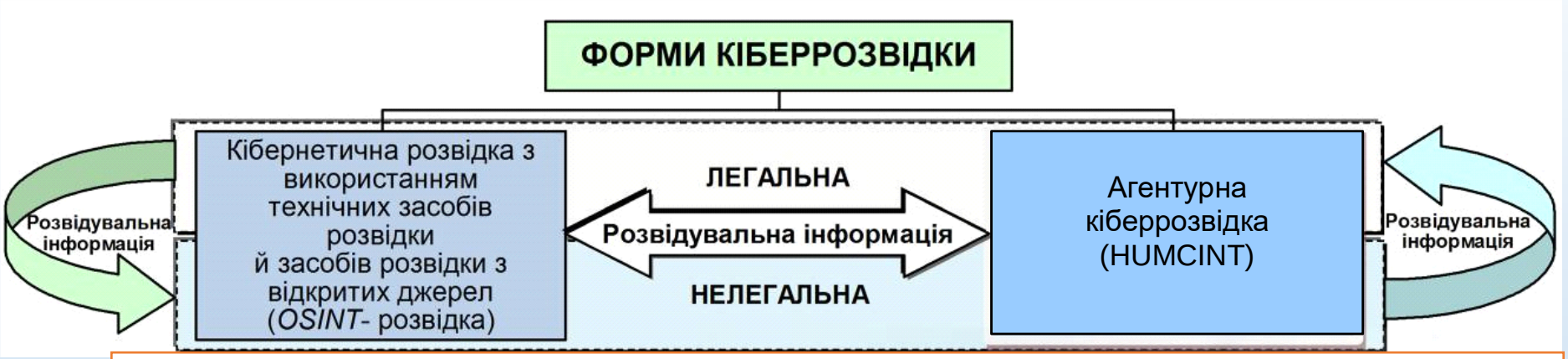
- **Кібернетична розвідка** – процес добування усіма наявними технічними засобами розвідки (космічної, повітряної, радіоелектронної, мережевої, програмно-комп'ютерної, розвідки систем управління тощо) й засобами розвідки з відкритих джерел (*OSINT*- розвідка) інформації наявної в кіберпросторі про протиборчу сторону та подальша її обробка, що здійснюються за єдиним задумом і планом з метою викриття процесів управління, які протікають в кібернетичних системах під час їх функціонування та формування вихідних даних для здійснення заходів кібернетичного захисту та кібернетичного впливу на технічні, соціальні та соціотехнічні кібернетичні системи.

Розвідка відкритих джерел (англ. *Open source intelligence*, ***OSINT***) - концепція, методологія і технологія добування і використання військової, політичної, економічної та іншої безпекової інформації з відкритих джерел, без порушення законів - для підтримки прийняття рішень у сфері національної оборони і безпеки. Включає в себе, більш детально, для прикладу: пошук інформації; реєстрацію і облік інформації; аналіз інформації і синтез знань з різних джерел (аналітико-синтетичну переробку первинної інформації); адміністрування і розповсюдження інформації; забезпечення безпеки інформації. Первинна інформація з відкритих джерел після її аналітико-синтетичної переробки може стати дуже цінними знаннями, які можуть стати секретними - якщо вони не відносяться до категорії інформації, яка не може бути віднесеною до державної таємниці.

ОСНОВНІ ФУНКЦІЇ КІБЕРНЕТИЧНОЇ РОЗВІДКИ

- постійний пошук і добування розвідувальної інформації про процеси управління в кібернетичних системах протиборчої сторони, що становлять інтерес з використанням усіх наявних технічних засобів розвідки й засобів розвідки з відкритих джерел інформації з кіберпростору;
- обробка, систематизація, класифікація, узагальнення та аналіз добутої розвідувальної інформації;
- підготовка розвідувальної інформації на підставі проведеного аналізу для прийняття обґрунтованих управлінських рішень;
- формуванні вихідних даних для здійснення заходів кібернетичного захисту власних кібернетичних систем та здійснення кібернетичного впливу на кібернетичні системи протиборчої сторони;
- прогнозування можливих проявів кібернетичних загроз та їх наслідків.

ФОРМИ КІБЕРНЕТИЧНОЇ РОЗВІДКИ



Основними формами кібернетичної розвідки є:

- кібернетична розвідка з використанням технічних засобів розвідки й засобів розвідки з відкритих джерел (*OSINT*- розвідка);
- агентурна кіберрозвідка (*HUMCINT*- розвідка).

Кібернетична розвідка з використанням технічних засобів розвідки – це одна з основних форм добування легальним та (або) нелегальним шляхом розвідувальної інформації з кіберпростору про процеси управління, які протікають в кібернетичних системах протиборчої сторони.

Агентурна кіберрозвідка (*HUMCINT*- розвідка) – це одна з форм добування інформації, що становить інтерес. Агентурна кіберрозвідка здійснюється за рахунок залучення людських ресурсів з обов'язковим використанням новітніх ІТ- рішень, у тому числі й інтегрованих у мережу інтернет.

ПРИНЦИПИ КІБЕРНЕТИЧНОЇ РОЗВІДКИ

Розвідувальне співтовариство США

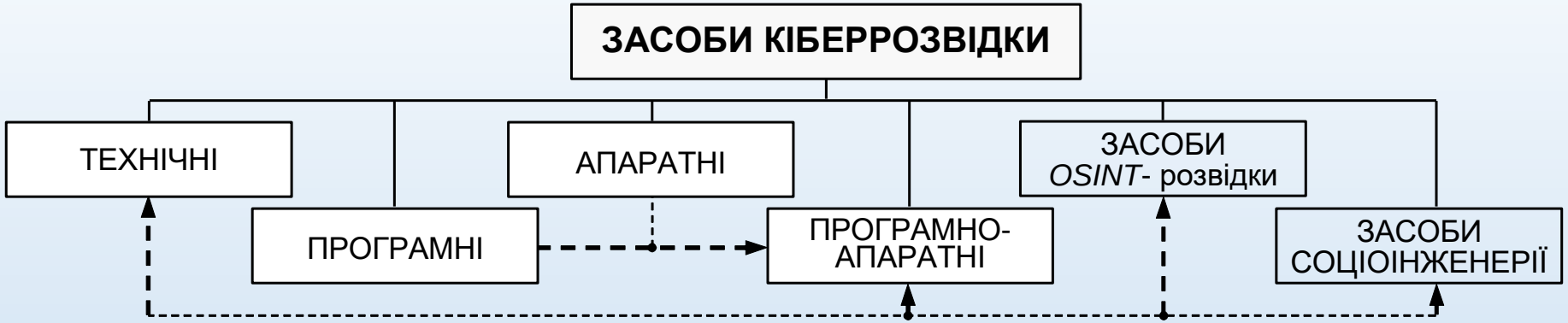
в США в межах свої компетенції для вирішення завдань кібернетичної розвідки задіяні усі 17 членів розвідувального співтовариства, які працюють як окремо, так і разом

Слід зауважити те, що основний акцент у здійсненні розвідувальних місій у кіберпросторі при цьому покладається на “Офіс операцій зі спеціалізованого доступу” (*TAO* Агентства національної безпеки).

Кібернетична розвідка ґрунтується на ряді принципів:

- цілеспрямованість;
- безперервність;
- активність;
- оперативність;
- скритність;
- достовірність;
- комплексне використання сил та засобів.

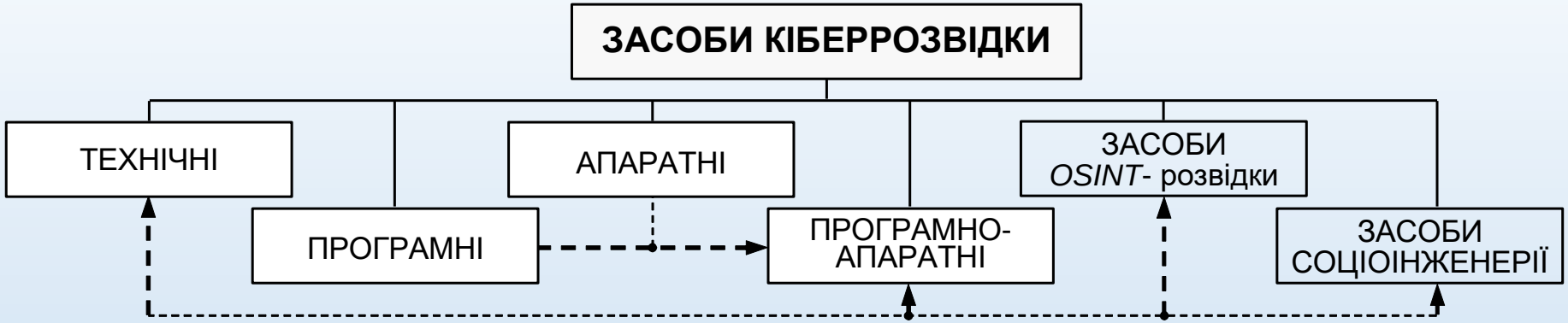
ОСНОВНІ ТИПИ ЗАСОБІВ КІБЕРРОЗВІДКИ



- технічні засоби;
- програмні засоби;
- апаратні засоби;
- програмно-апаратні засоби;
- засоби кіберрозвідки з відкритих джерел (OSINT- засоби);
- засоби соціальної інженерії.

Технічні засоби кіберрозвідки – це сукупність розвідувальної апаратури (апаратів, машин та виготовлених з їх використанням спеціалізованого обладнання або технічних засобів, інструментів, речовин тощо), що призначені для несанкціонованого одержання розвідувальної інформації про процеси управління в кібернетичних системах протиборчої сторони шляхом контролю кіберпростору й окремих його складових.

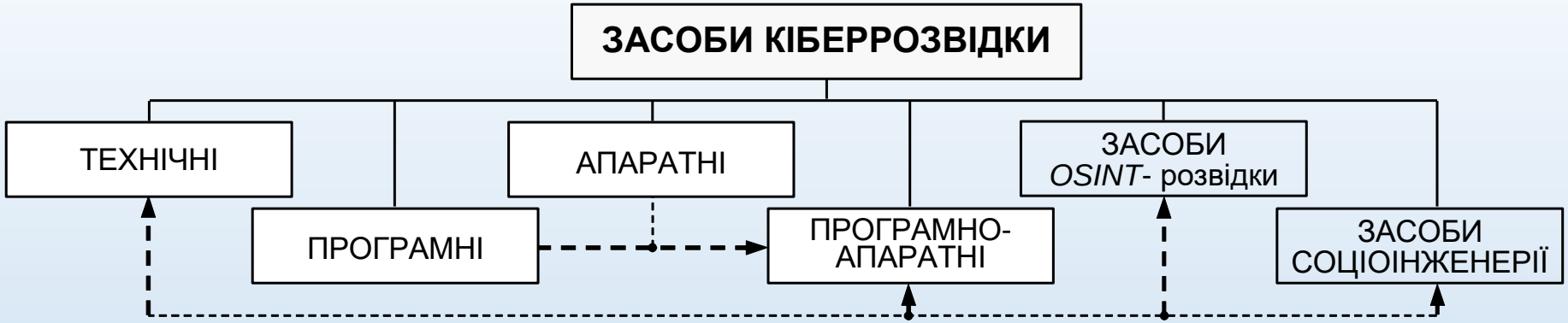
ОСНОВНІ ТИПИ ЗАСОБІВ КІБЕРРОЗВІДКИ



Програмні засоби кіберрозвідки – це сукупність спеціалізованих програмних модулів, які створені з метою добування розвідувальної інформації з кіберпростору про процеси управління в кібернетичних системах протиборчої сторони.

Апаратні засоби кіберрозвідки – це сукупність спеціалізованих апаратних засобів, що забезпечують добування розвідувальної інформації шляхом дослідження апаратури, обладнання, модулів їх аналізу та випробування тощо, задіяних в управлінні кібернетичними системами протиборчої сторони з метою виявлення їх технічних характеристик та потенційних можливостей.

ОСНОВНІ ТИПИ ЗАСОБІВ КІБЕРРОЗВІДКИ



Програмно-апаратні засоби являють собою сукупність програмних та апаратних спеціалізованих засобів, призначення та функції яких випливають з основного призначення та функцій їх складових.

Засоби OSINT- розвідки – це сукупність, технічних, програмних, апаратних, програмно-апаратних та інших засобів, що використовуються підрозділами кібернетичної розвідки для добування розвідувальної інформації з відкритих та відносно відкритих джерел кіберпростору про процеси управління, що протікають у кібернетичних системах протиборчої сторони.

Засоби соціальної інженерії – засоби добування розвідувальної інформації про процеси управління в кібернетичних системах протиборчої сторони, орієнтовані на її отримання від суб'єкта кібернетично розвідки. Саме соціальна інженерія вважається фахівцями одним із найбільш перспективних способів ведення кібернетичної розвідки.

ПРОГРАМНІ ЗАСОБИ АНАЛІЗУ ТА ПОДОЛАННЯ СИСТЕМ ЗАХИСТУ

1 ГРУПА — ЗАСОБИ АНАЛІЗУ

1 тип — ДАНИХ
- Програми-каталогізатори
- Програми-пошуку файлів і даних
- Аналізатори файлової системи
- Аналізатори портів вводу/виводу
- Аналізатори мережевої активності
- Аналізатори активних задач та вікон

2 тип — АЛГОРИТМІВ
- Аналізатори викликів сервісів ОС
- Аналізатори міжпрограмної взаємодії
- Програми розпакувальники/дешифратори
- Засоби дизасемблювання програм
- Засоби декомпіляції об'єктних модулів
- Засоби відлагодження об'єктних модулів
- Засоби симуляції центрального процесора та ОС

2 ГРУПА — ЗАСОБИ ПОДОЛАННЯ

3 тип — БЕЗПОСЕРЕДНЬОГО ПОДОЛАННЯ
- Програми копіювання областей ПЗП до ЗЗП
- Засоби пошуку та заміни даних
- **Засоби редагування «ресурсів»**
- Засоби динамічної модифікації
- Засоби модифікації контексту процесів
- Програми симуляції апаратних засобів
- Засоби криптоаналізу

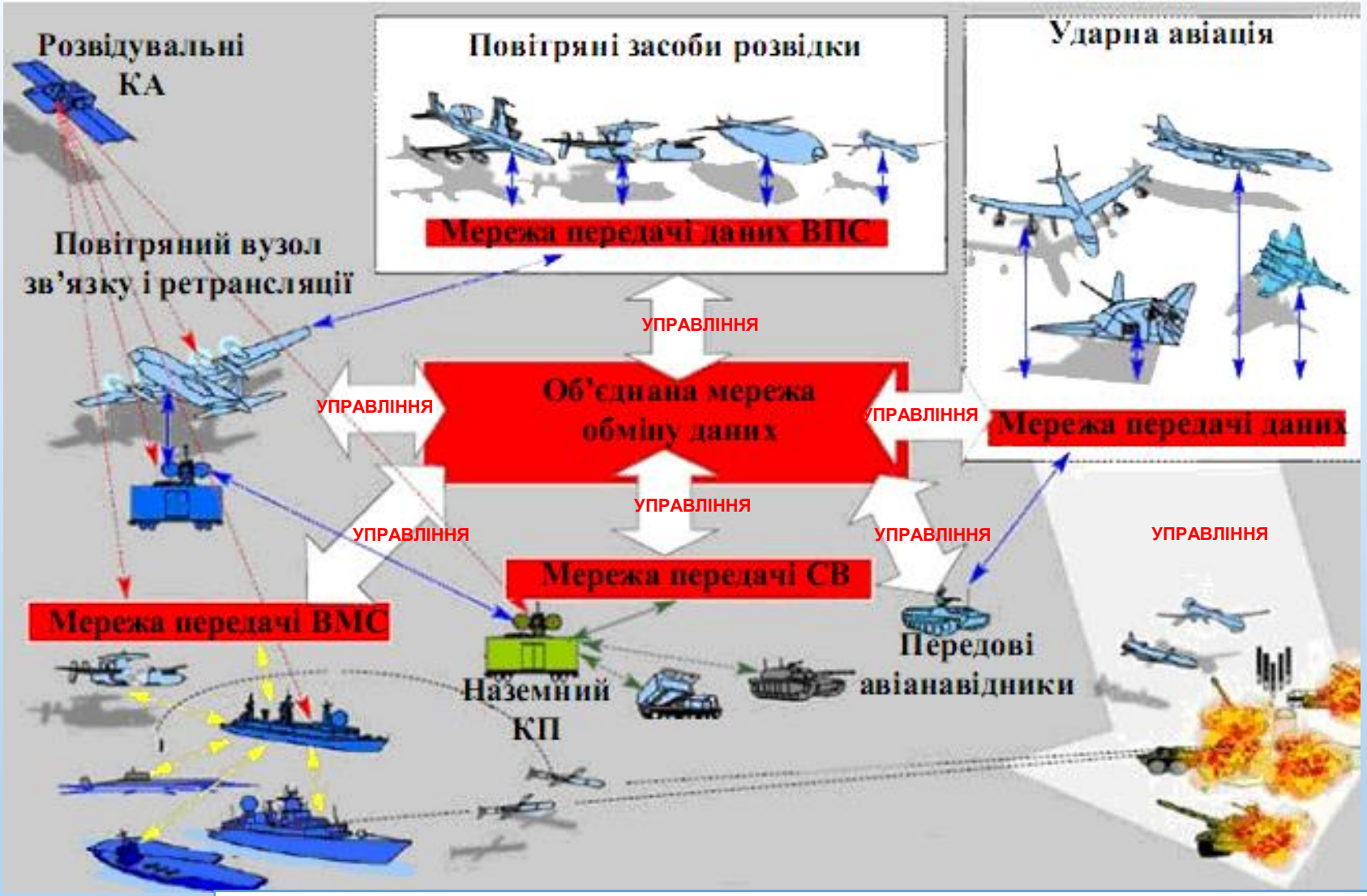
4 тип — В ОБХІД
- Програми перехоплення клавіатурного введення
- Програми відновлення видалених файлів
- Програми побайтового копіювання дисків
- Засоби симуляції ОС або системи захисту
- Засоби пакетної обробки команд
- **Засоби генерації паролів та ключів**
- Засоби ОС з контролю доступу

Найбільш поширені в світі пошукові системи

Серед *засобів добування розвідувальної інформації та спеціалізованого програмного забезпечення з пошуку визначеного контенту,* особлива роль відводиться пошуковим системам. Основними засобами пошуку такої інформації виступають інформаційні пошукові системи. Найбільш поширеними в світі з них є такі, як *Google* (46,2%), *Yahoo (22,5%), msn* (12,6%), *AOL* (5,4%), *My Way* (2,2%), *Netscape* (1,6%) та ін. (7,9%)

ВИДИ КИБЕРНЕТИЧНОЇ РОЗВИДКИ

МЕРЕЖЕЦЕНТИЧНА КОНЦЕПЦІЯ



втілення мережевих технологій у військову сферу дозволяє підвищити бойову ефективність застосування збройних сил, що досягається за рахунок синергетичного ефекту від застосування наявних сил та засобів у рамках відомої мережецентичної концепції

БАЗОВІ МЕРЕЖІ УПРАВЛІННЯ

- **Мережева розвідка** – це комплекс спланованих спеціальних заходів щодо отримання даних й оброблення розвідувальної інформації про визначену мережу та її фізичну й логічну топологію, її ресурси, засоби захисту, використані пристрої і програмне забезпечення та їх вразливості.

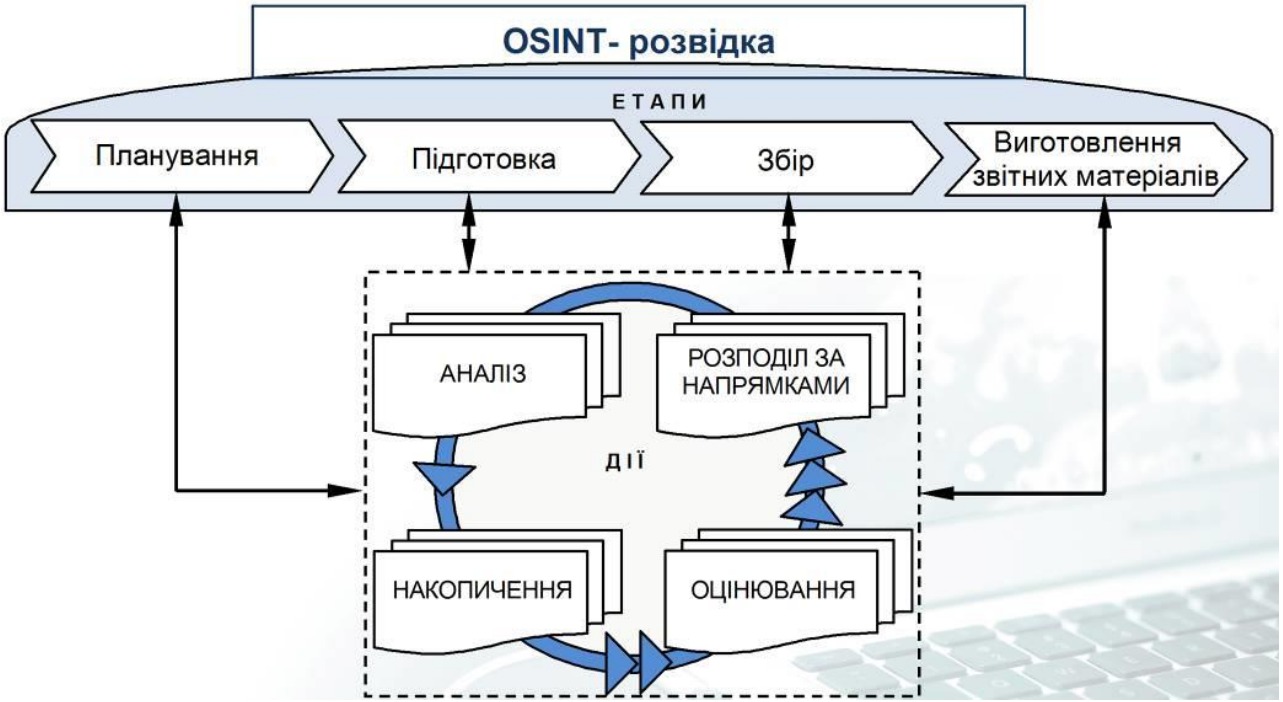
- **мережева розвідка комп'ютерних мереж** – це комплекс спланованих спеціальних заходів, що здійснюються з метою добування даних й оброблення розвідувальної інформації про комп'ютерні мережі для визначення їх фізичної й логічної топології, ресурсного та інших видів забезпечення, а також їх вразливостей.

ПРОГРАМНО-КОМП’ЮТЕРНА РОЗВІДКА

➘ **Програмно-комп’ютерна розвідка** – це узгоджені за місцем, часом проведення та задачами розвідувальні заходи, що здійснюються з метою добування даних й оброблення розвідувальної інформації про склад, призначення та характеристики апаратного та системного й спеціалізованого програмного забезпечення кібернетичних систем протиборчої сторони, в контурі управління яких здіяні комп’ютеризовані засоби та системи.

При цьому:

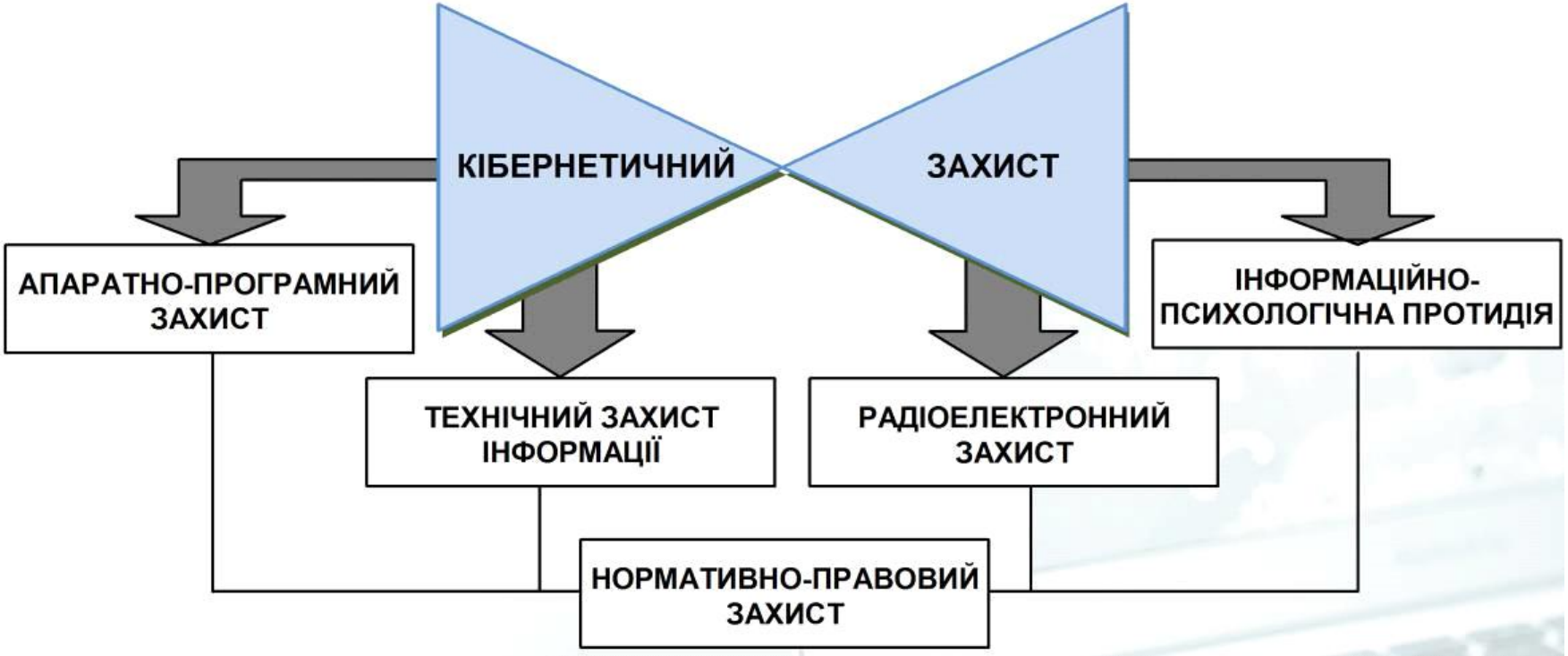
- під апаратним забезпеченням в наведеному визначенні розуміється комплекс технічних засобів, який включає комп’ютерна система типової конфігурації, наприклад, контролери, процесори, мережеві адаптери, периферійне обладнання тощо;
- під програмним забезпеченням розуміється сукупність програм системи обробки інформації і програмних документів, необхідних для експлуатації цих програм. Воно може бути системним та прикладним. Системне програмне забезпечення забезпечує коректне функціонування комп’ютерної системи в цілому, наприклад, операційна система, графічний інтерфейс користувача тощо.



OSINT- РОЗВІДКА ЯК СКЛАДОВА КІБЕРНЕТИЧНОЇ РОЗВІДКИ

- ***OSINT*- розвідка –** це вид кібернетичної розвідки, що ведеться шляхом систематичного збору інформації з відкритих джерел, її аналізу, підготовки та своєчасного надання кінцевого продукту замовнику з метою забезпечення його потреб у такій інформації.

ОСНОВИ КІБЕРНЕТИЧНОГО ЗАХИСТУ



Види кібернетичного захисту

- **Кібернетичний захист** – це сукупність організаційних, нормативно-правових та технічних заходів здійснюваних в інтересах забезпечення кібербезпеки, протидії кібернетичній розвідці об’єктів національного кібернетичного простору, запобіганню та припиненню кібернетичних впливів на них.

ОСНОВНІ ЦІЛІ КІБЕРНЕТИЧНОГО ЗАХИСТУ

Апаратно-програмний захист – це комплексне застосування апаратних та програмних засобів для забезпечення кібернетичного захисту комп'ютерної системи.

ОСНОВИ КІБЕРНЕТИЧНОГО ВПЛИВУ

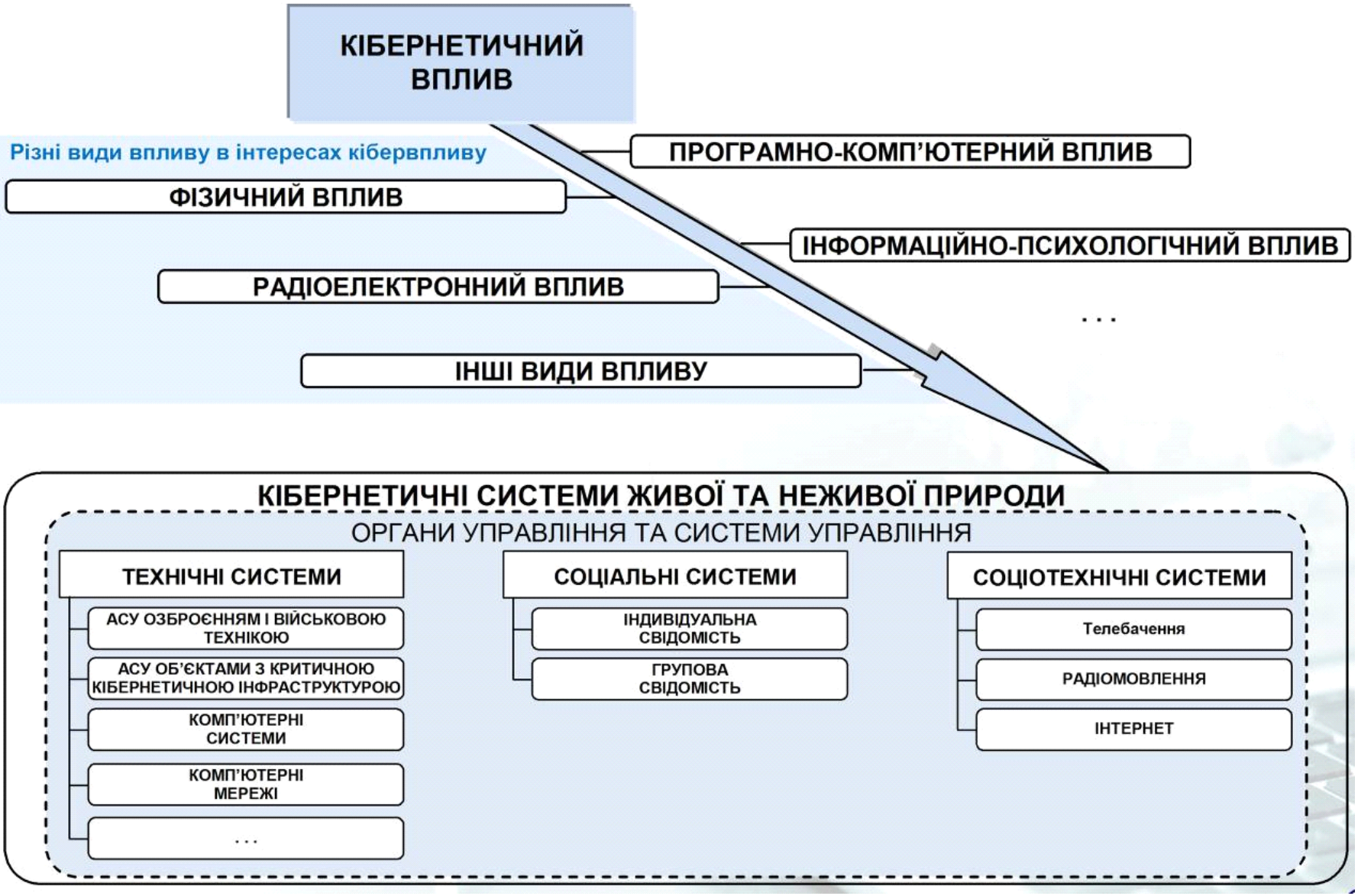
➘ **Кібернетичний вплив** – це цілеспрямований процес застосування усього наявного комплексу сил та засобів, призначених для впливу на визначені елементи кіберпростору з метою порушення процесів управління в кібернетичних системах протиборчої сторони шляхом зміни нормальних режимів їх функціонування з подальшим, або співвимірним у часі впливу узяттям їх під власне управління та контроль.

Об’єктами кібернетичного впливу можуть виступати органи управління та системи управління кібернетичних систем живої та неживої природи, а саме:

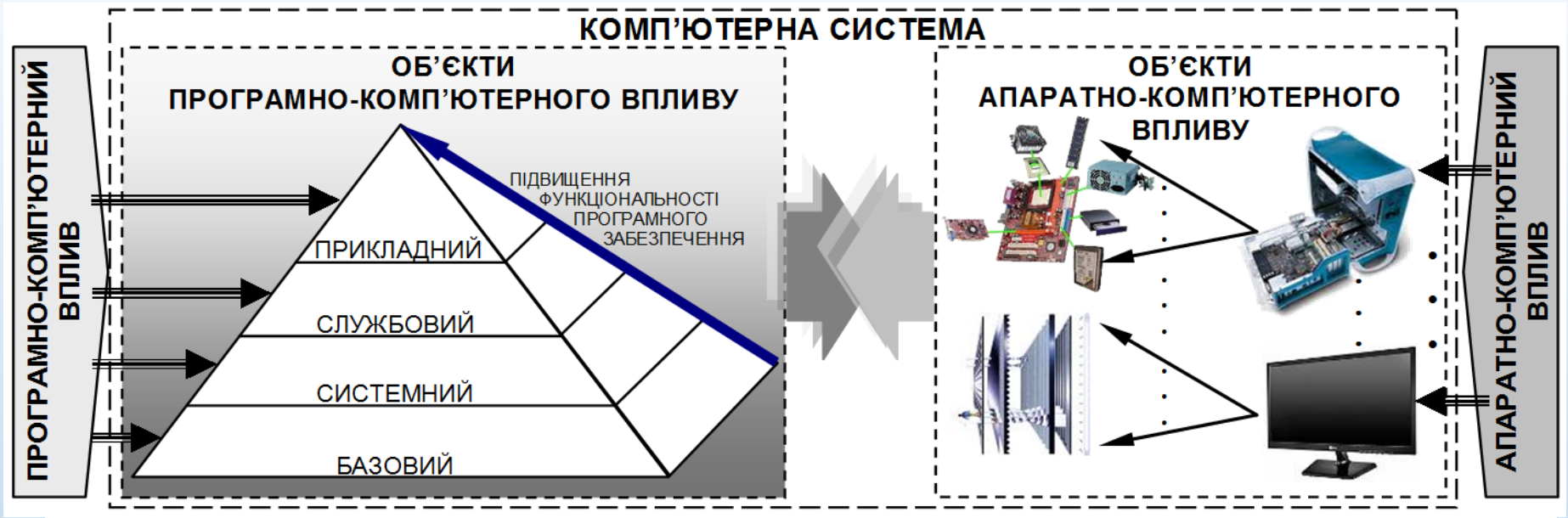
- технічні системи різного призначення;
- соціум;

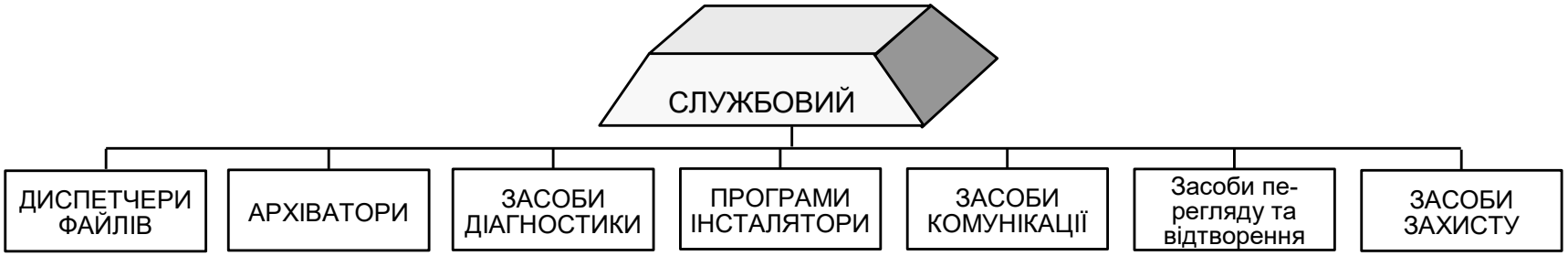
соціотехнічні системи

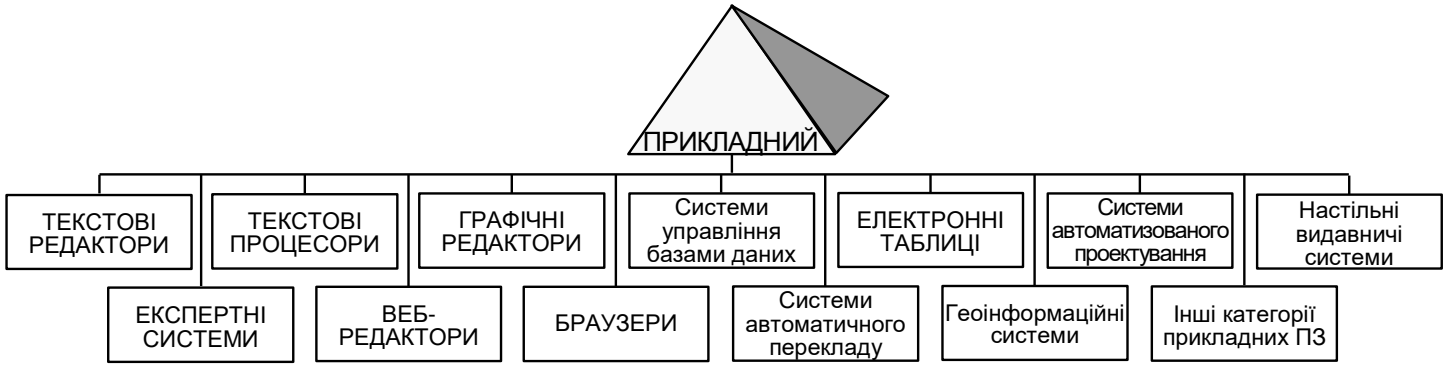
ВИДИ ТА ОБ’ЄКТИ КІБЕРНЕТИЧНОГО ВПЛИВУ



ДЕКОМПОЗИЦІЯ ОБ’ЄКТІВ ПРОГРАМНО-КОМП’ЮТЕРНОГО ТА АПАРАТНО-КОМП’ЮТЕРНОГО ВПЛИВУ







ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИЙ ВПЛИВ

Інформаційно-психологічний вплив здійснюється з метою впливу на емоційний стан, мотивацію й аргументацію дій, рішення, що приймаються, поведінку керівників (керуючих центрів) соціальних чи національних груп, окремих осіб іноземної держави та її військовослужбовців у сприятливому напрямі для сил, що їх застосовують.

Під **масовим впливом** слід розуміти такі дії фахівців у галузі масової комунікації стосовно суб'єктів впливу, які призводять до збудження в них керованих психоемоційних процесів, що обумовлюють однакові настрої, однакові або схожі думки за порушеною проблемою.

Як наслідок фахівці формують масову свідомість, яка і об'єднує суб'єктів впливу в керовану масу, публіку або натовп. У натовпі кожен окремо узятий суб'єкт впливу здатен проявляти передбачувані або й не передбачувані фахівцем однакові (схожі) емоційно-вольові, інтелектуальні або фізичні реакції.

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИЙ ВПЛИВ

Незалежно від сфери впливу – політична, економічна, духовна, військова тощо рівень ефективності інформаційно-психологічного впливу залежить від:

- змісту матеріалу, його складності, конкретності, суспільної значимості тощо. Наприклад, за рівних умов, чим простіша інформація, тим більше шансів на те, що дії, до яких вона спонукає, можуть виконуватися автоматично, особливо, якщо не суперечать переконанням об'єкта: чим більш конкретний заклик до дії – тим вищий ступінь автоматизму відповідної реакції;
- психічного стану, що характеризується наявністю високого рівня автоматизму відповідної реакції. Страх, пригніченість, апатія сприяють некритичному й неусвідомленому сприйняттю впливу. Ступінь автоматизму відповіді особистості пов'язана з рівнем усвідомленості й критичності прийняття інформації. Якщо вплив приймається підсвідомо й некритично, то відповідь аудиторії може бути автоматичною;
- часового інтервалу між впливами й відповідною реакцією: із збільшенням часового інтервалу автоматизм відповідних реакцій зменшується унаслідок підвищення критичності і розумової активності об'єкта).

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИЙ ВПЛИВ

основними видами інформаційно-психологічного є:

- психогенний вплив;
- нейролінгвістичний вплив;
- психоаналітичний (психокорекційний) вплив;
- психотропний вплив.

Психогенний вплив – це психічний або фізичний вплив явищ або подій визначеного змісту на мозок, свідомість людини, при якому спостерігається порушення вищої нервової діяльності: з'являється відчуття страху й паніки.

Нейролінгвістичний вплив – це вид психологічного впливу, що передбачає використання спеціальних прийомів, спрямованих на створення позитивної мотивації, психологічної корекції внутрішніх джерел поведінки й світогляду особистості людини.

Психоаналітичний (психокорекційний) вплив – це вплив на підсвідомість людини, що здійснюється унаслідок "подолання опору" свідомості людини під час гіпнотичного сну або у нормальному стані.

Психотронний вплив (парапсихологічний, екстрасенсорний) – це вплив, що здійснюється за допомогою передачі енергії мислення через позачуттєве сприйняття і яке охоплює опосередковане свідомістю і процесами сприйняття дистантної взаємодії між живими організмами й навколишнім середовищем.

СХЕМА ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНОГО ВПЛИВУ

- **Основа успішного інформаційно-психологічного впливу у будь-якій сфері визначається якістю вивчення об'єктів та суб'єктів впливу, й створенням на основі цих відомостей відповідних засобів поширення матеріалів впливу.**