ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

АНАЛІЗ МЕТОДИК ОЦІНКИ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У БАНКІВСЬКИХ СИСТЕМАХ

Керівник роботи:
к.т.н., доц. Король О. Г.

Виконала:
студентка 4 курсу, ф-ту ЕІ
Юрченко А. А.

АКТУАЛЬНІСТЬ РОБОТИ

- ***Мета роботи:***

  Визначення проблеми забезпечення інформаційної безпеки, розробка методу, що дає змогу оцінити фінансові збитки від застосованої кібератаки, на основі аналізу методик оцінки ризиків.

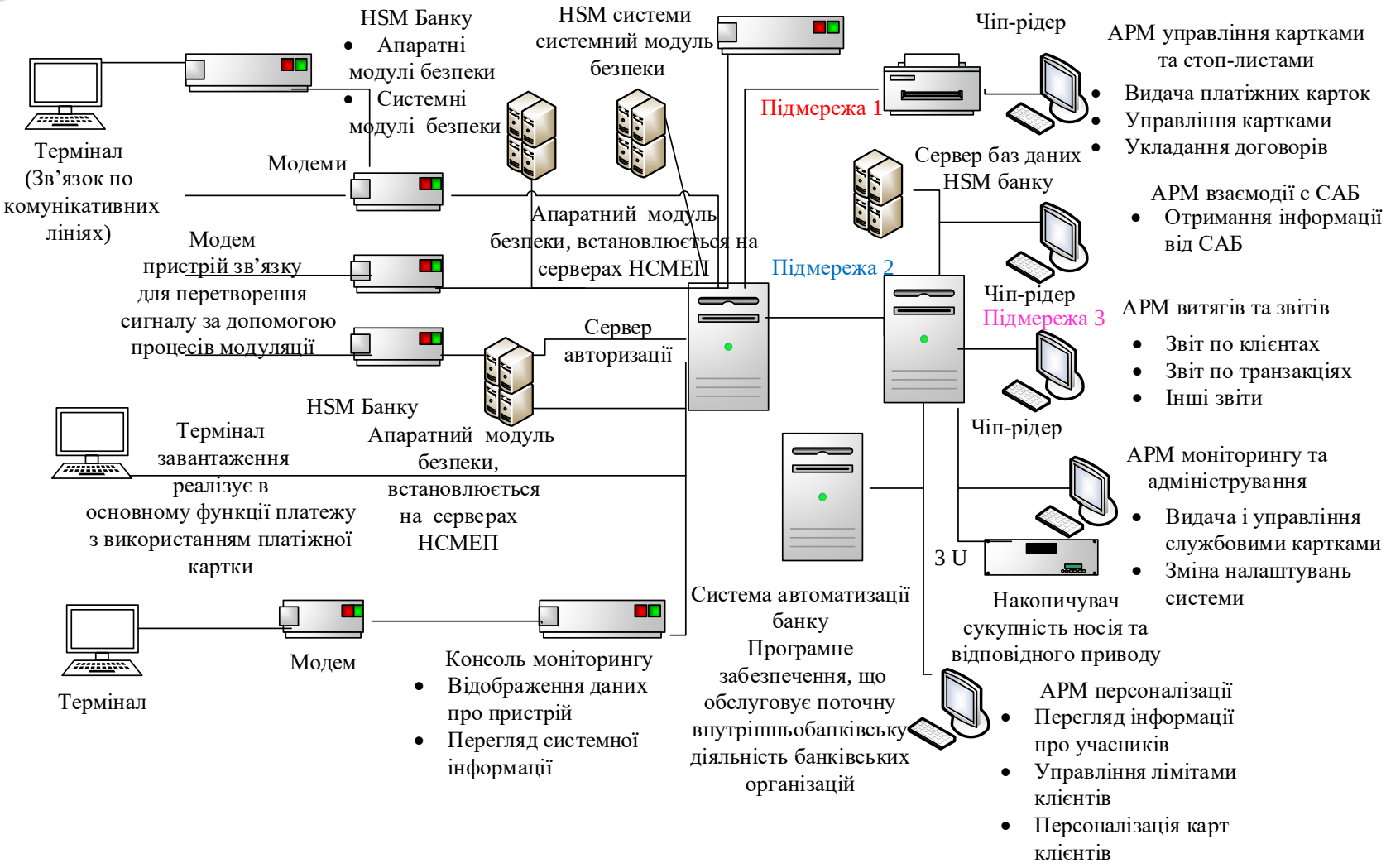
- ***Об'єкт дослідження:***

  Процес забезпечення інформаційної безпеки в банківських системах.

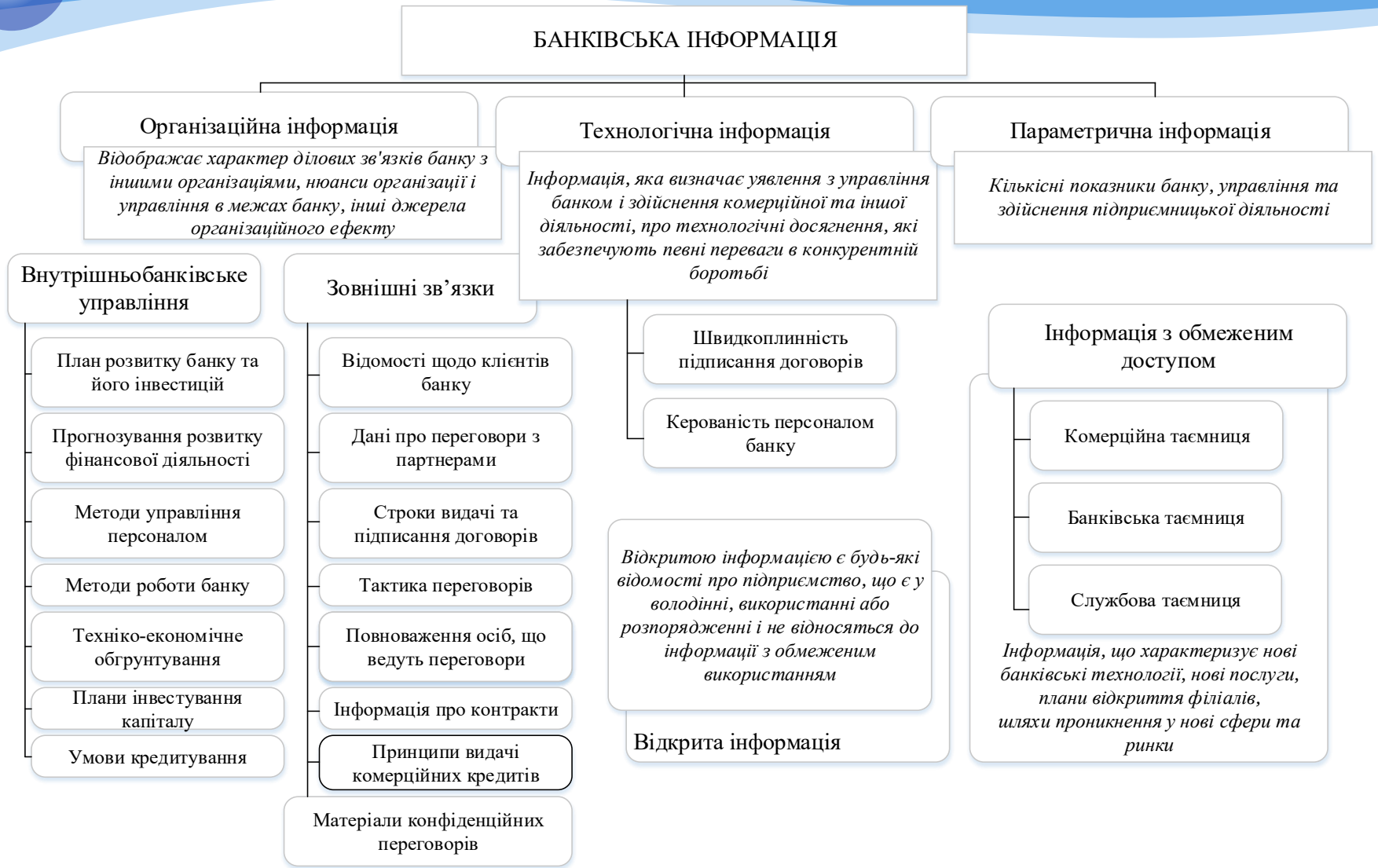
- ***Предмет дослідження:***

  Аналіз методів та методик оцінки порушення інформаційної безпеки

СТРУКТУРА НСМЕП



КЛАСИФІКАЦІЯ БАНКІВСЬКОЇ ІНФОРМАЦІЇ



НОРМАТИВНА БАЗА НСЕП

ЗАКОНОДАВЧА БАЗА БАНКІВСЬКОЇ БЕЗПЕКИ

Закон України «Про банки та банківську діяльність»

Визначає основи побудови і організації банківської системи

Закон України «Про Національний банк»

Закон регулює відносини, що виникають під час заснування, реєстрації, діяльності, реорганізації і ліквідації банків

Закон України «Про електронні документи та електронний документообіг»

Закон встановлює основні організаційно-правові заходи електронного документообігу та використання електронних документів

Постанова Управління НБУ № 57 від 15.07.93 «Про нову систему міжбанківських розрахунків в Україні»

Закон України «Про електронний цифровий підпис»

Визначає правовий статус ЦП і регулює відносини, пов'язані з використанням ЦП

Постанова КМУ № 903-2004 «Про затвердження Порядку акредитації ЦСК»

Постанова КМУ № 1452-2004 «Про затвердження Порядку застосування ЦП органами держ. влади, органами місцевого самоврядування...»

Постанова КМУ № 1454-2004 «Про затвердження Порядку обов'язкової передачі документованої інформації»

Постанова КМУ № 551-2009 «Про заходи щодо впровадження системи електронної державної реєстрації юридичних осіб та фізичних осіб - підприємств»

Закон України «Про державну таємницю»

Регламентує і визначає дії та заходи з охорони держтаємниці в Україні

Закон Україні «Про захист інформацію»

Закріплює право громадян на інформацію, визначає правові основи інформаційної діяльності

СОУ Н НБУ 65.1 СУІБ 1.0:2010

Визначає модель розробки, впровадження, функціонування, моніторингу, аналізу, підтримки та вдосконалення системи управління інформаційною безпекою

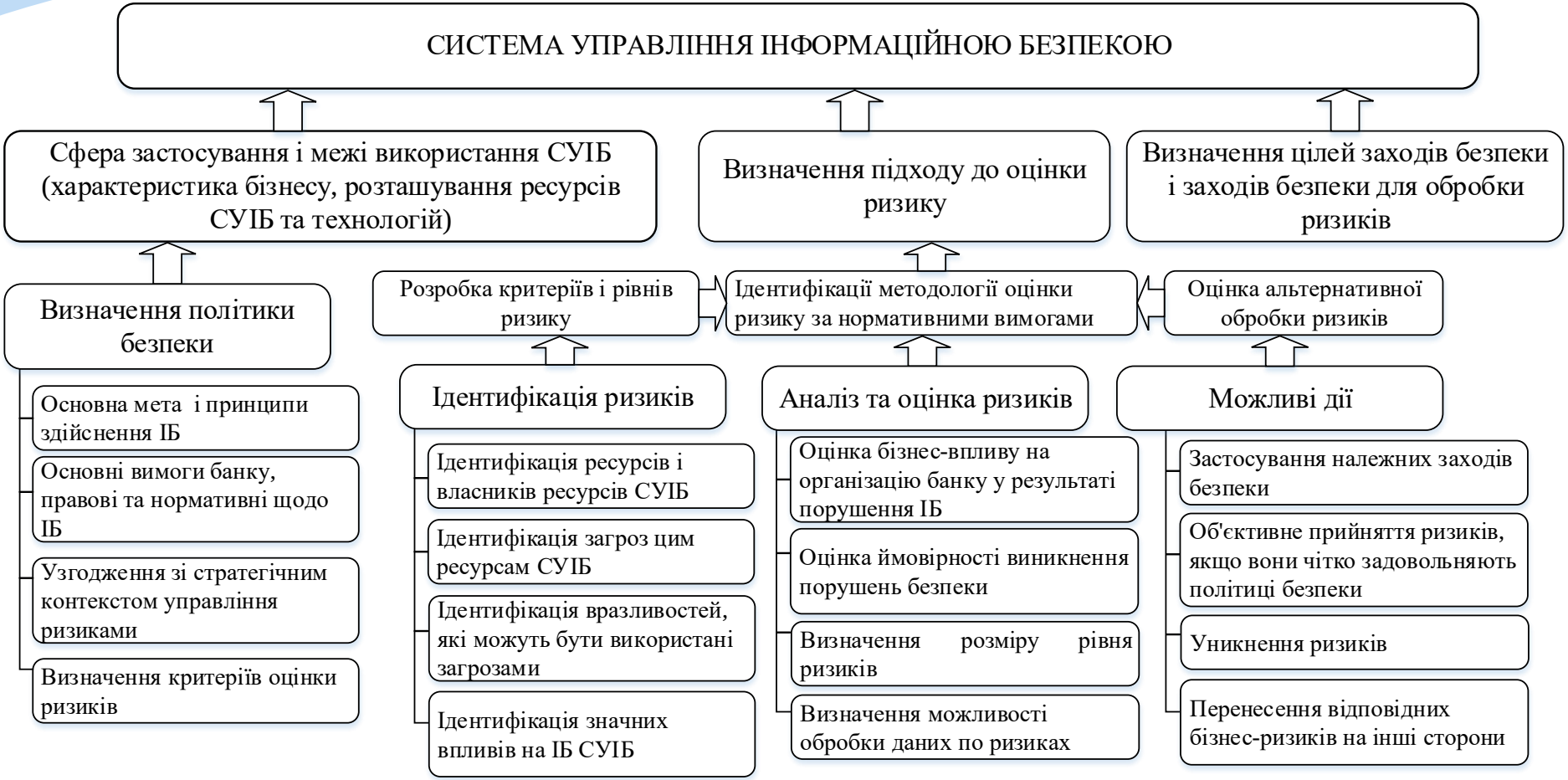
СОУ Н НБУ 65.1 СУІБ 2.0:2010

Визначає методи захисту у банківській діяльності, зведення правил щодо управління інформаційною безпекою

Закон України «Про інформацію»

Закріплює право громадян на інформацію, визначає правові основи інф. діяльності

СУІБ КОМЕРЦІЙНОГО БАНКУ



ВІДОМІ МОДЕЛІ АНАЛІЗУ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Модель тріади CIA

- Конфіденційність (Confidentiality)
  - *гарантія того, що інформація може бути прочитана і проінтерпретувана тільки тими людьми і процесами, які авторизовані це робити*
- Цілісність (Integrity)
  - *гарантування того, що інформація залишається незмінною, коректною та автентичною*
- Доступність (Availability)
  - *гарантування того, що авторизовані користувачі можуть мати доступ і працювати з інформаційними активами, ресурсами і системами, які їм необхідні, при цьому забезпечується необхідна продуктивність*

Модель Гексада Паркера

- Конфіденційність (Confidentiality)
  - *гарантія того, що інформація може бути прочитана і проінтерпретувана тільки тими людьми і процесами, які авторизовані це робити*
- Цілісність (Integrity)
  - *гарантія того, що інформація залишається незмінною, коректною та автентичною*
- Доступність (Availability)
  - *гарантія того, що авторизовані користувачі можуть мати доступ і працювати з інформаційними активами, ресурсами і системами, які їм необхідні, при цьому забезпечується необхідна продуктивність*
- Автентичність (Authenticity)
  - *вірогідність того, що дані були створені заявленим джерелом*
- Керованість або володіння (Possession or Control)
  - *гарантія того, що законний власник є єдиною особою, у владі якого змінити інформацію або отримати до неї доступ на читання*
- Корисність (Utility)
  - *«практичність», зручність доступу*

Модель класифікація 5A

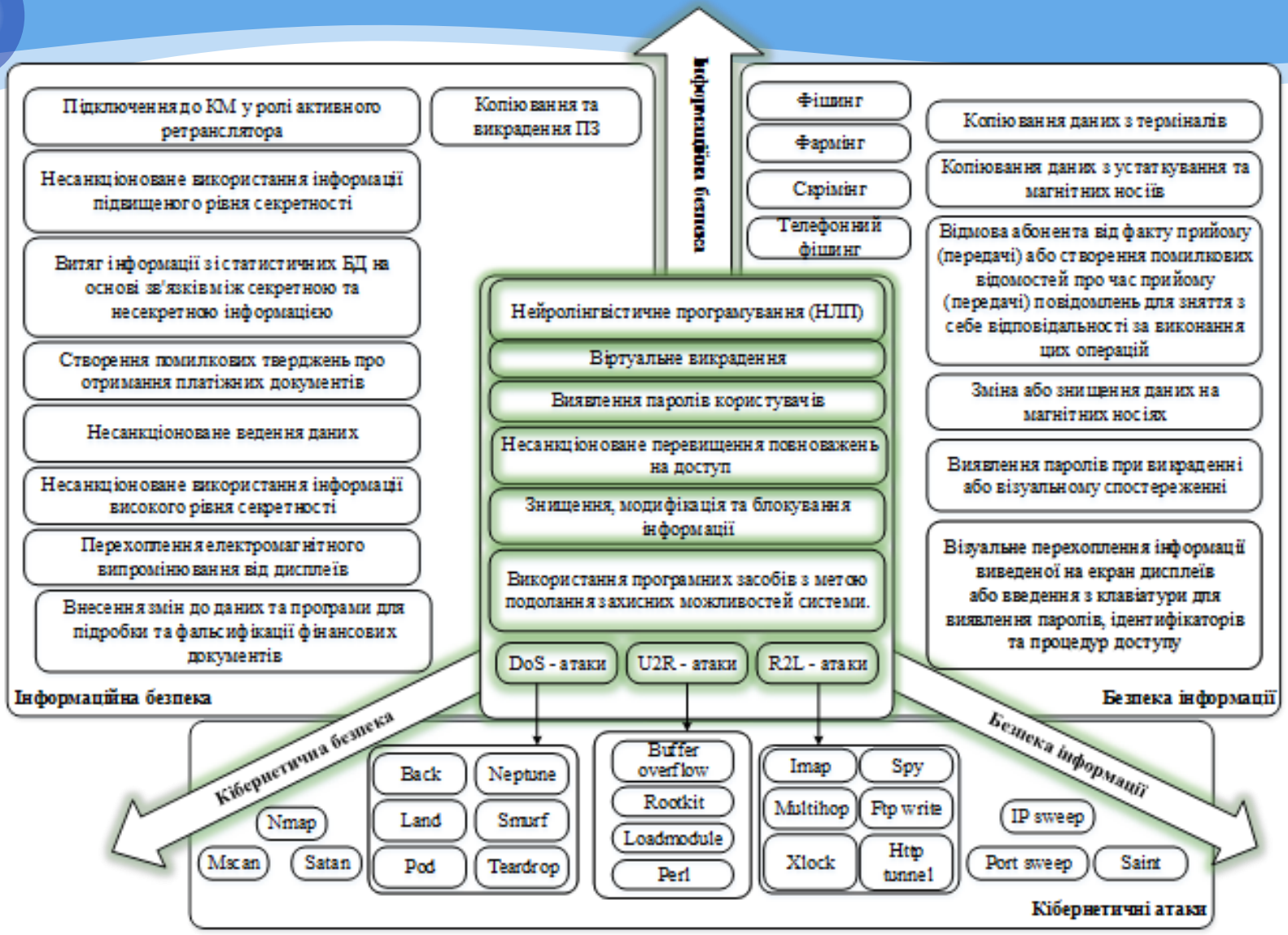
- Автентифікація (Authentication)
  - *хто ти?*
- Авторизація (Authorization)
  - *що тобі дозволено робити?*
- Доступність (Availability)
  - *чи можна отримати доступ для роботи з даними?*
- Вірогідність (Authenticity)
  - *чи не пошкоджені дані зловмисником?*
- Припустимість (Admissibility)
  - *чи є дані достовірними, актуальними і корисними?*

Модель STRIDE

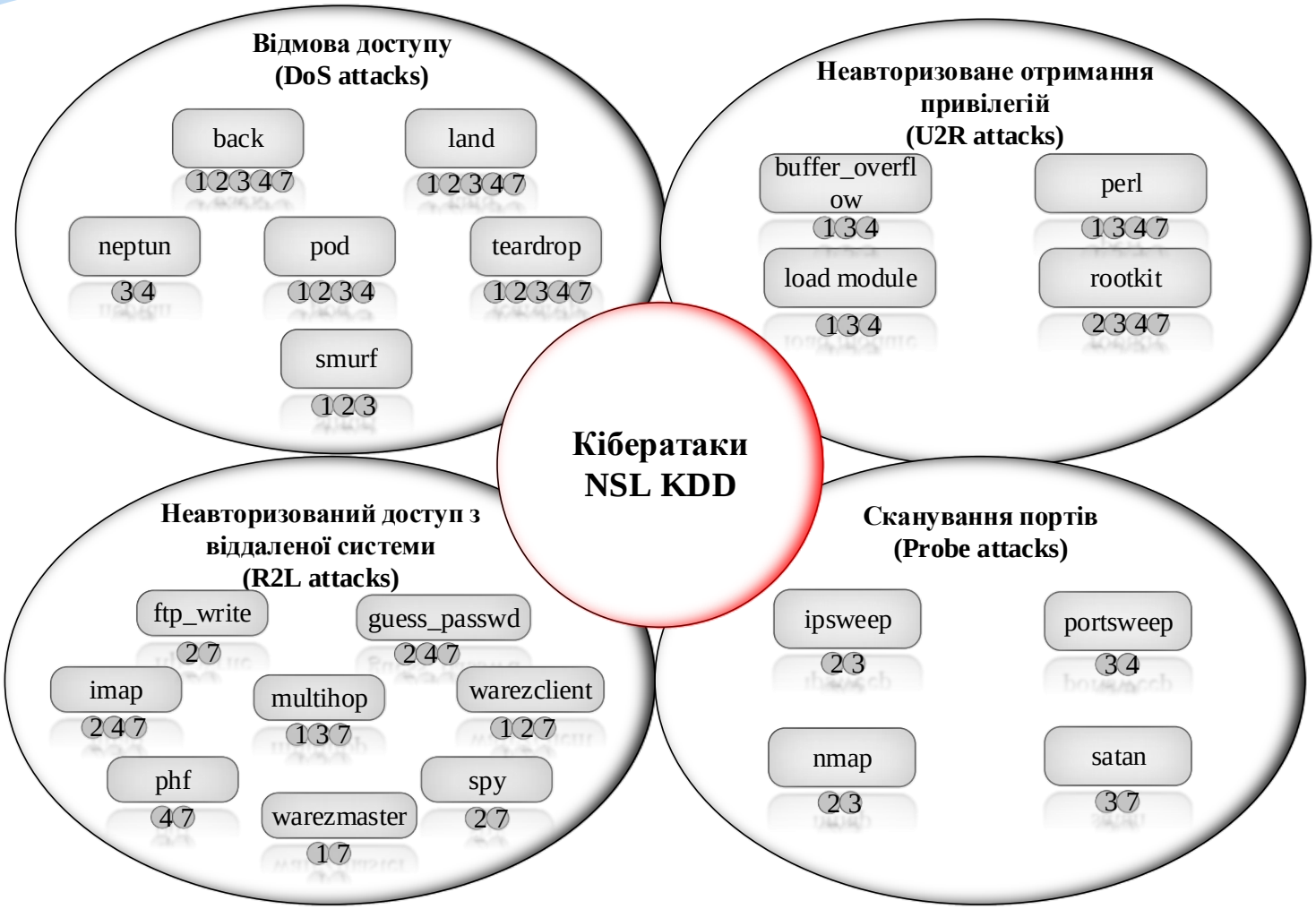
- Удавання (Spoofing)
  - *Підміна об'єктів. надійні методи автентифікації (базова HTTP авторизація, автентифікації на основі кеша); підміна серверів; DNS spoofing; модифікатор записів DNS кеша*
- Зміна (Tampering)
  - *навмисне псування даних*
- Відмова від відповідальності (Repudiation)
  - *можливість порушника відмовитися від здійснюваних ним дій*
- Витік даних (Information Disclosure)
  - *розголошення інформації особам, для яких доступ до даної інформації заборонено*
- Відмова в обслуговуванні (Denial of Service)
  - *можливість порушити функціонування системи або перезавантажити комп'ютер через мережу*
- Захоплення привілеїв (Elevation of Privilege)
  - *можливість порушника підвищити свої привілеї в системі*

ВЗАЄМОЗВ'ЯЗОК МІЖ КІБЕРБЕЗПЕКОЮ ТА ІНШИМИ ДОМЕНАМИ БЕЗПЕКИ

ЗАГАЛЬНА КЛАСИФІКАЦІЯ ЗАГРОЗ АБС



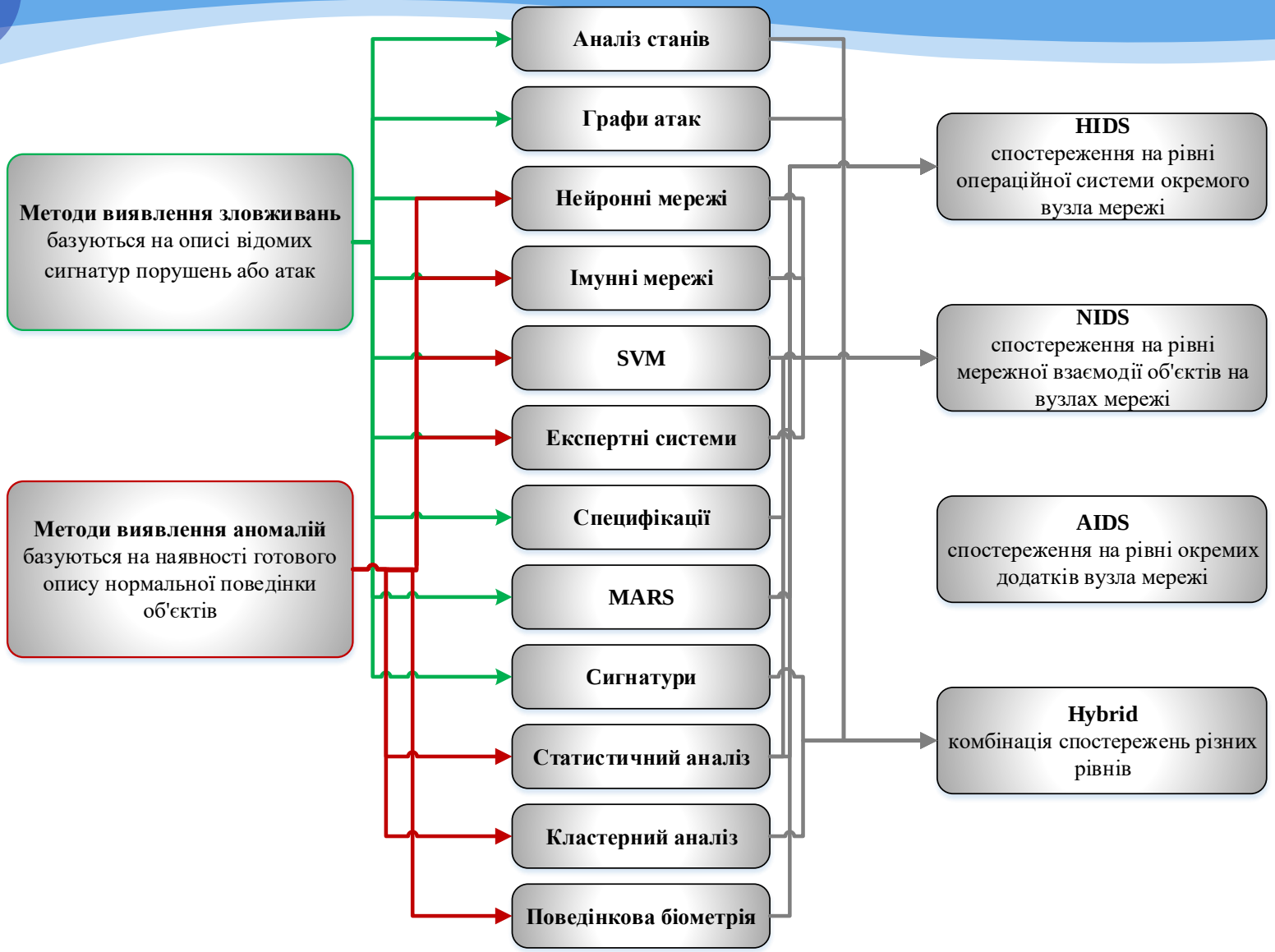
КЛАСИФІКАЦІЯ КІБЕРАТАК



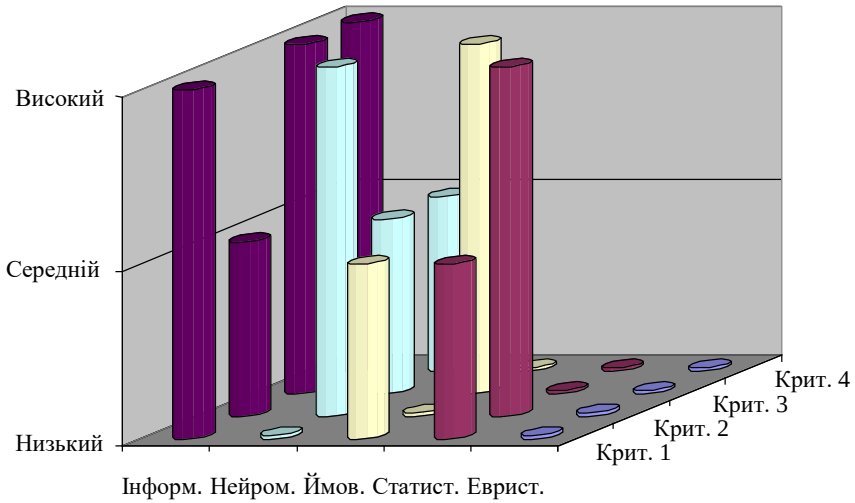
- **Прикладний (7)**
- **Транспортний (4)**
- **Мережевий (3)**
- **Канальний (2)**
- **Фізичний (1)**

Рівні моделі OSI

МЕТОДИ ВИЯВЛЕННЯ АТАК

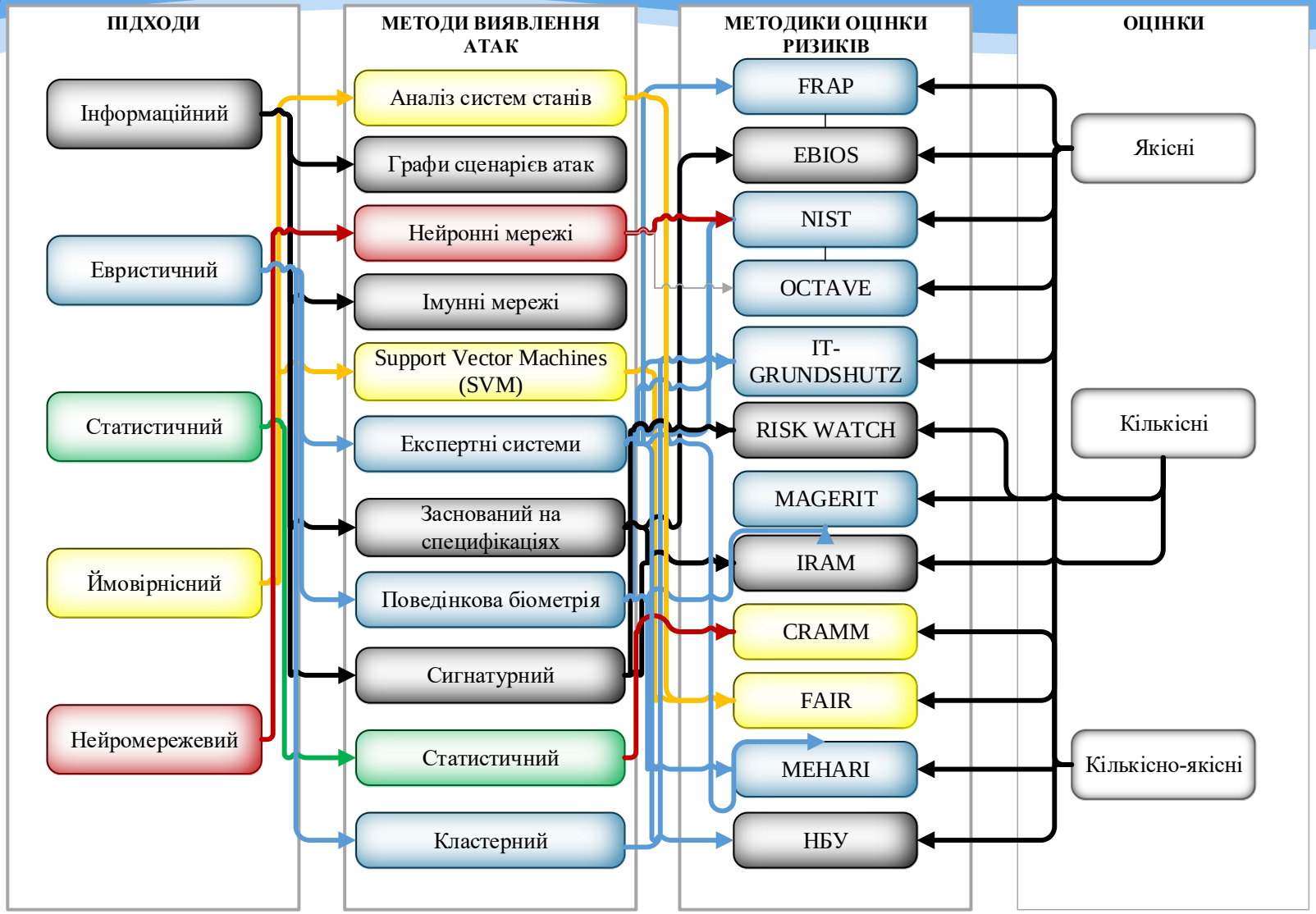


ОЦІНКА ІНФОРМАТИВНОСТІ ПАРАМЕТРІВ



Підходи	Оцінка ефективності	
	кількісна	якісна
Інформаційний	0.22	достатня
Нейромережевий	0.36	достатня
Ймовірнісний	0.4	задовільна
Статистичний	0.4	задовільна
Евристичний	0.5	низька

МЕТОДИ ТА МЕТОДИКИ ОЦІНКИ РИЗИКІВ



МЕТОДИКА CRAMM

МЕТОДИКА FAIR

1 етап. Визначення компонентів сценарію

актив (об'єкта)

Визначення середовища загроз

Частота подій-загроз (TEF)

Дуже висока (**VH**) TEF> 100
Висока (**H**) 10 <TEF <100
Середня (**M**) 1 <TEF <10
Низька (**L**) 0.1 <TEF <1
Дуже низька (**VL**) TEF <0.1

Можливість реалізації загрози (Tcap)

Дуже висока (**VH**): перші 2%
Висока (**H**): перші 16%
Середня (**M**): між першими 16% і останніми 16%
Низька (**L**): останні 16%
Дуже низька (**VL**): останні 2%

2 етап. Оцінка частоти несприятливих подій

Ефективність контрзаходів (CS)

Дуже висока (**VH**): захист від перших 2%
Висока (**H**): захист від перших 16%
Середня (**M**): захист між першими 16% і останніми 16%
Низька (**L**): захист від останніх 16%
Дуже низька (**VL**): захист від останніх 2%

Уразливість системи (Vuln)

Tcap \ CS	VL	L	M	H	VH
VH	*VH*	*VH*	*VH*	*H*	*M*
H	*VH*	*VH*	*H*	*M*	*L*
M	*VH*	*H*	*M*	*L*	*VL*
L	*H*	*M*	*L*	*VL*	*VL*
VL	*M*	*L*	*VL*	*VL*	*VL*

3 етап. Оцінка рівня ймовірних втрат

Оцінка втрат в найгіршому випадку (WCLM)

Величина ймовірних втрат (PLM)

Втрати	Нижня межа	Верхний предел
Важливі (**SV**)	10 000 000$	----
Високі (**H**)	1 000 000$	9 999 999$
Значні (**Sg**)	100 000$	999 999$
Середні (**M**)	10 000$	99 999$
Низькі (**L**)	1 000$	9 999$
Значно низькі (**VL**)	0$	999$

4 етап. Виявлення і формулювання ризиків

Аналіз ризиків (LEF+PLM)

PLM \ Риск	VL	L	M	H	VH
SV	*H*	*H*	*C*	*C*	*C*
H	*M*	*H*	*H*	*C*	*C*
Sg	*M*	*M*	*H*	*H*	*C*
M	*L*	*M*	*M*	*H*	*H*
L	*L*	*L*	*M*	*M*	*M*
VL	*L*	*L*	*M*	*M*	*M*

LEF

Рівень ризику (LEF+PLM)+WCLM

Ймовірна частота втрат (LEF)

TEF \ Vuln	VL	L	M	H	VH
VH	*M*	*H*	*VH*	*VH*	*VH*
H	*L*	*M*	*H*	*H*	*H*
M	*VL*	*L*	*M*	*M*	*M*
L	*VL*	*VL*	*L*	*L*	*L*
VL	*VL*	*VL*	*VL*	*VL*	*VL*

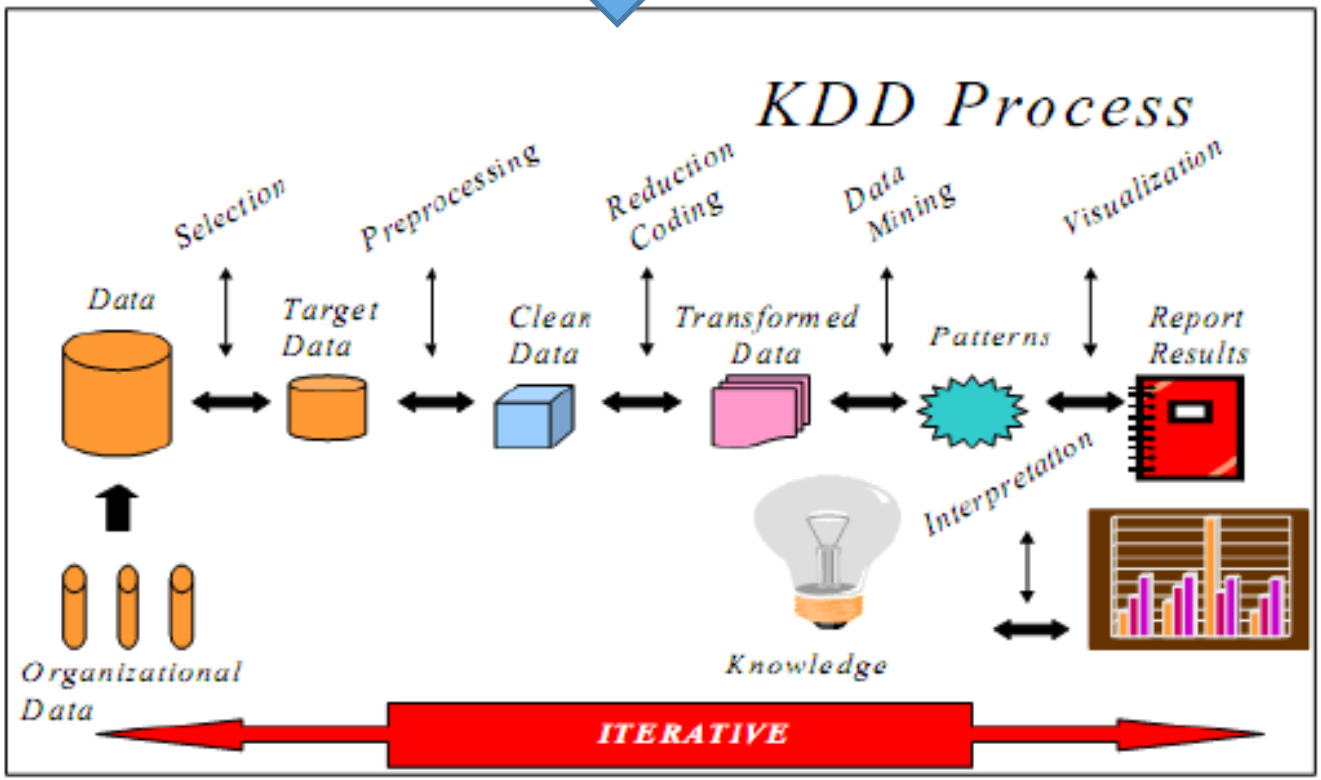
Vuln

ВХІДНІ ДАНІ-БАЗА KDD99

22 типи

5 млн. екземплярів

41 ознака



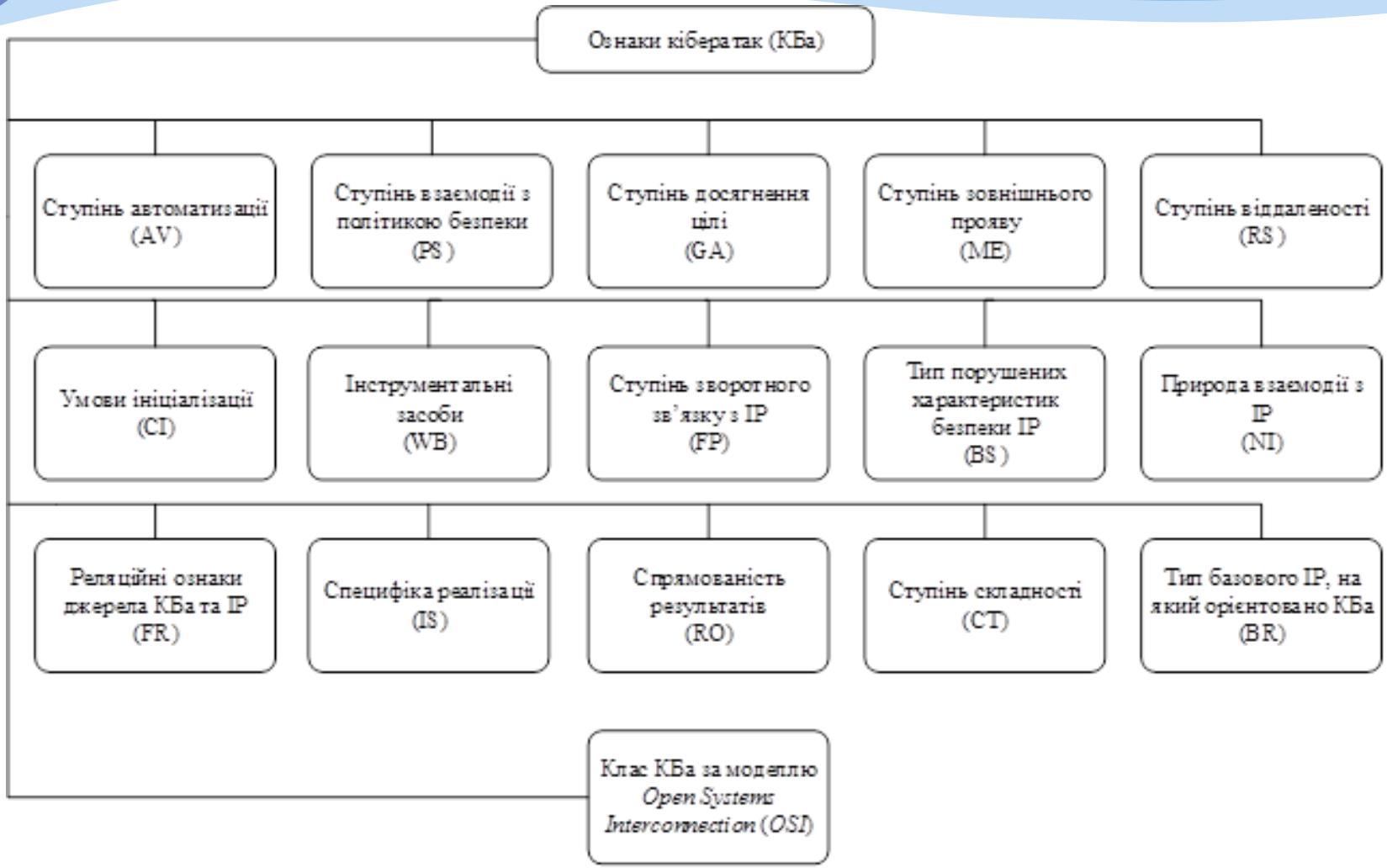
БАЗА ДАНИХ NSL-KDD

22 ознаки

Max кількість виявлених атак

№	Ознака
1	Duration
2	Protocol_type
3	Service
4	Flag
5	Source_bytes
6	Destination_types
7	Land
8	Wrong_fragment
9	Urgent
11	Failed_logins
13	Num_compromised
14	Root_shell
17	Num_file_creations
18	Num_shells
22	Is_guest_login
27	Rerror_rate
28	Srv_rerror_rate
29	Same_srv_rate
31	Srv_diff_host_rate
32	Dst_host_count
35	Dst_host_diff_srv_rate
37	Dst_host_srv_diff_host_rate

УЗАГАЛЬНЕНА КЛАСИФІКАЦІЯ О. Г. КОРЧЕНКО



ВИСНОВКИ

1. Розвиток обчислювальних можливостей дозволив розширити спектр банківських послуг на основі використання Інтернет - ресурсів.

2. Завдання захисту банківської інформації , як правило , включає рішення приватних завдань із забезпеченню надійної і безпечної роботи АБС (автоматизованої банківської системи) .

3. Важливу роль в процесі класифікації кібератак грають вхідні дані. За основу вхідних тестових даних доцільним вбачається застосування загальнодоступної бази даних NSL-KDD, що не містить надлишкових записів і дає більший відсоток виявлення атак порівняно до KDD - 99.

4. Комплексування двох відомих підходів дозволить об'єднати переваги кожного з них, і при цьому відкриє можливості отримання як кількісних, так і якісних їх характеристик для ефективної організації систем захисту.

- За результатами дослідження було опубліковано дві тези на міжнародних наукових конференціях та стаття у фаховому виданні України.

Дякую за увагу!