KAPITEL 2 / *CHAPTER 2* [2]
THE METHODOLOGY OF BUILDING THE COGNITIVE MODEL OF CRITICAL INFRASTRUCTURE'S SECURITY

DOI: 10.30890/2709-2313.2022-11-01-009

Вступ

Нині, з неминучістю ведення інформаційних війн, все частіше проявляються аспекти безпеки в усіх сферах соціуму: від побутових до науково-виробничих. При цьому значущість оцінювання стану безпеки будь-яких сучасних об'єктів, передусім критично-важливих об'єктів (КВО), для держави і суспільства з їх інформаційними інфраструктурами по забезпеченню повноти і достовірності задіяної інформації завжди була актуальна, а нині – вкрай потрібна. Саме тому набуває ще більшої актуальності тенденція по створенню і вдосконаленню методів і інструментальних засобів, спрямованих на усунення конкретних пізнавальних, юридично-правових і технічних проблем з безпекою і захистом об'єктів критичної інфраструктури (ОКІ).

2.1. Сучасний стан законодавчої бази по захисту та безпеці ОКІ України

Останнє підтверджується на законодавчому рівні України [1-3]. Зокрема, пріоритетами забезпечення кібербезпеки (КБ) є [1, п.5]:

– «убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства;

– захист прав, свобод і законних інтересів громадян України у кіберпросторі;

– європейська і євроатлантична інтеграція у сфері кібербезпеки».

Так, на рисунку 1 відображені цілі "нової якості національної системи кібербезпеки" з позицій "формування потенціалу стримування" (Ст), "набуття кіберстійкості" (Кс) та "вдосконалення взаємодії" (Вв), що мають бути досягнуті протягом періоду реалізації Стратегії Кібербезпеки України [1, п.5]. (Для рисунку 1 використовувані наступні скорочення: РПД – розвідувально-

[2] ***Authors:*** *Klym Viktoriia Yuryevna, Tarasenko Yuri Stanislavovich*

підривна діяльность, КП – кіберпростір, КТ –кібертероризм).

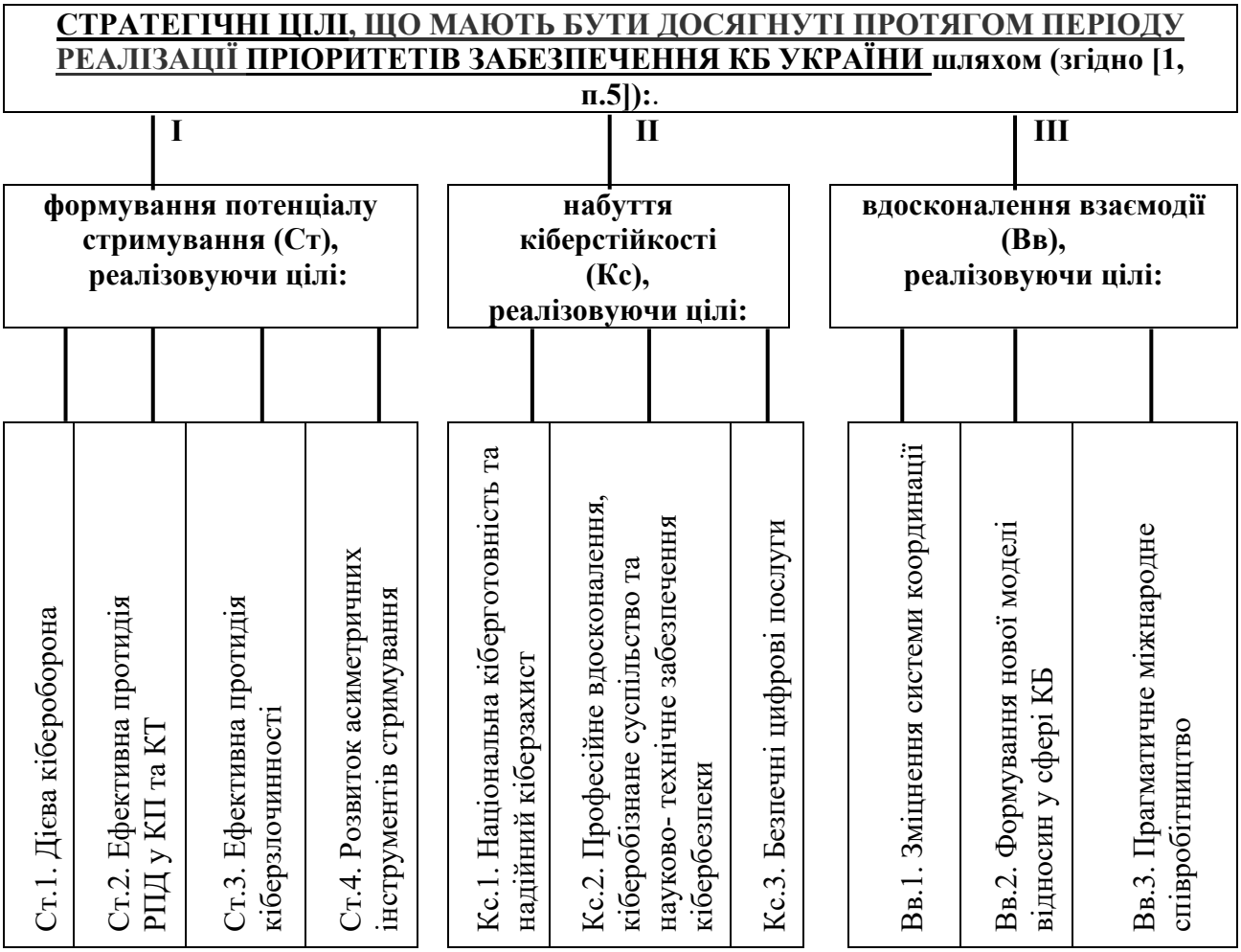

Рисунок 1 - Структурно-лінгвістична схема (СЛС) "Пріоритети забезпечення кібербезпеки України та стратегічні цілі"

Згідно [2, Ст.8, п.2], "віднесення об'єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг, свідчать про існування загроз для них, можливість виникнення кризових ситуацій через несанкціоноване втручання в їх функціонування, припинення функціонування, людський чинник чи природні лиха, тривалість робіт для усунення таких наслідків до повного відновлення штатного режиму". Наведена деталізація належності критеріїв до ОКІ, згідно [2. Ст.8, п.3] (рис. 2).

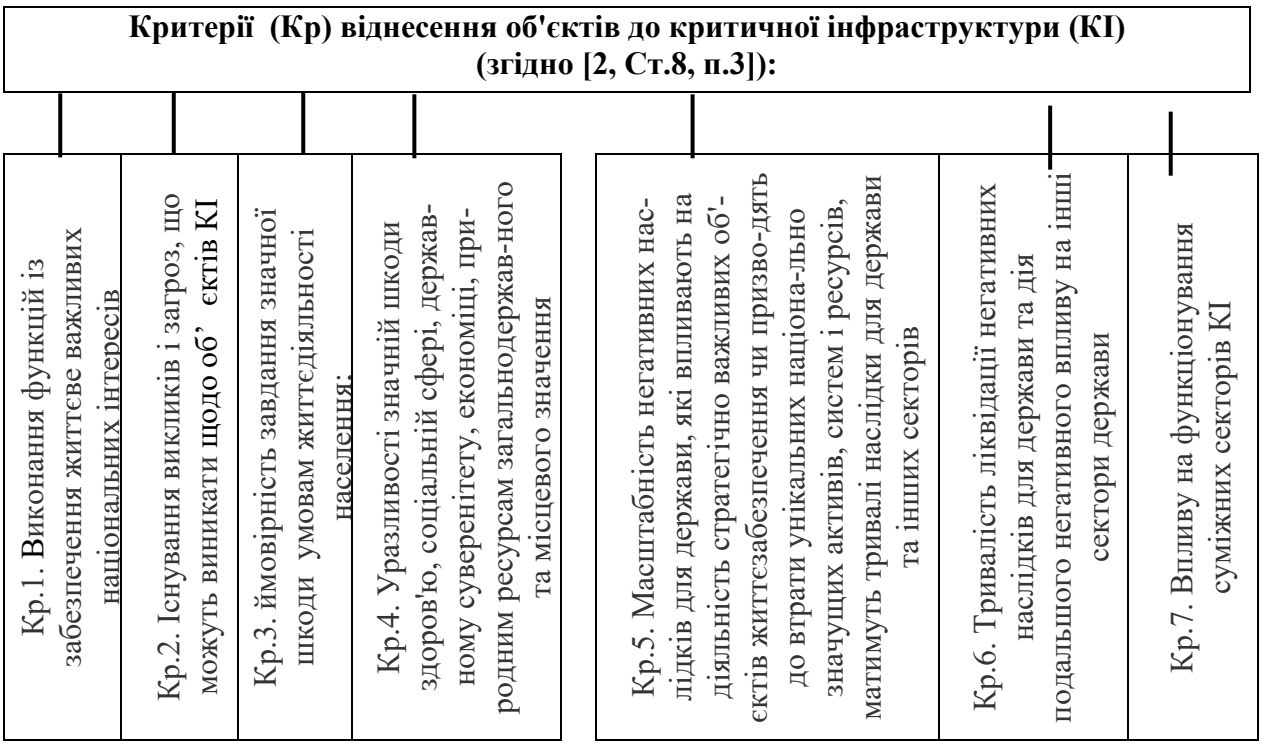

Рисунок 2 - СЛС "Критерії віднесення об'єктів до критичної інфраструктури (КІ)"

Нажаль, критеріям властивий ймовірнісний характер, що заважає вибору оптимального варіанту захисту ОКІ, залежного від багатопрофільних аспектів експлуатації, включаючи і нечітку передбачуваність (невизначеність) довкілля. Тому зазвичай прийнято оцінювати безпеку будь-якого об'єкту з позиції його штатної експлуатаційної надійності, безвідмовності, довговічності та інших площин експлуатаційної технологічності, в основі яких, як правило, закладені конкретні багатоцільові метрологічні методики дослідження, більшість з яких задекларовані державними або галузевими стандартами, наприклад, як в [4. стр.176, 5. стр.11], включаючи і область менеджменту інформаційної безпеки з аспектами захисту інформації через формування загальних понять і етапів управління. Причому, в межах організації ефективного забезпечення безпеки і непорушності системи захисту критичної інфраструктури (СЗКІ), введені сектори (С) [2, Ст.9, п.3, 4] (табл.1).

Крім того, передбачено чотири режими функціонування СЗКІ: штатний; готовності та запобігання реалізації загроз; реагування на виникнення кризової ситуації; відновлення штатного функціонування [2, Ст.15, п.1].

Таблиця 1 - СЛС "Сектори КІ, за порушення життєве важливих функцій та/або послуг яких, призводить до негативних наслідків"

Позначення	Зміст секторів КІ згідно [2, Ст.9, п.3, 4]
С1	Урядування та надання найважливіших адміністративних послуг
С2	Енергозабезпечення (у тому числі постачання теплової енергії)
С3	Водопостачання та водовідведення
С4	Продовольче забезпечення
С5	Охорона здоров'я
С6	Фармацевтична промисловість
С7	Виготовлення вакцин, стале функціонування біолабораторій
С8	Інформаційні послуги
С9	Електронні комунікації
С10	Фінансові послуги
С11	Транспортне забезпечення
С12	Оборона, державна безпека
С13	Правопорядок, здійснення правосуддя, тримання під вартою
С14	Цивільний захист населення та територій, служби порятунку
С15	Космічна діяльність, космічні технології та послуги
С16	Хімічна промисловість
С17	Дослідницька діяльність

У контексті статті, серед основних завдань для операторів (ЗО) КІ (ОпКІ) [2, Ст.21, п.1], акцентуємо увагу на необхідність "захисту інформації про системи управління, зв'язку, фізичну безпеку та кібербезпеку", вказану в ЗО14 (табл.2). Таким чином, реальна безпека КВО як "Сукупності об'єктів критичної інфраструктури" (СОКІ) [2, Ст.1, п.1, поз.9] залежить від штатної працездатності реалізованих систем у вигляді об'єктів кібербезпеки (ОКБ) і киберзахисту (рис.3) [3, Ст.4, п.1, 2] та критичної інфраструктури (рис. 4) [3, Ст.6, п.1], з відповідним з боку ОпКІ контролем по отриманню, обробці, зберіганню і передачі інформації по виділених сегментах (перешкодам) захисту із задекларованою їх експлуатаційною надійністю в умовах апріорної неоднозначності поведінки довкілля.

Таблиця 2 - СЛС "Основні завдання операторів КІ України"

Позначення	Зміст ЗО згідно [2, Ст.21, п.1]
ЗО1	Забезпечення захисту ОКІ, зокрема створення, налагодження та підтримання функціонування ефективної системи фізичної безпеки, безпеки операційних систем та кібербезпеки
ЗО2	Розроблення, оновлення та забезпечення виконання об’єктових планів заходів щодо забезпечення безпеки і стійкості критичної інфраструктури,

Позначення	Зміст ЗО згідно [2, Ст.21, п.1]
	правил управління ризиками безпеки, планів локалізації та ліквідації наслідків аварій, а також заходів кіберзахисту
ЗО3	Проведення оцінки ризиків на об'єктах критичної інфраструктури та обмін інформацією про ризики та загрози з іншими суб'єктами національної системи захисту критичної інфраструктури, а також створення умов для належного виконання правоохоронними, розвідувальними та контррозвідувальними органами своїх завдань щодо захисту критичної інфраструктури
ЗО4	Створення окремого структурного підрозділу або визначення відповідальної особи за організацію захисту критичної інфраструктури та забезпечення постійного зв'язку з відповідними суб'єктами національної системи захисту критичної інфраструктури
ЗО5	Оперативне реагування на протиправні дії, фізичні атаки, спрямовані на відключення або пошкодження роботи операційних систем чи систем забезпечення фізичної безпеки об'єкта критичної інфраструктури
ЗО6	Організація заходів з реагування на інциденти, кризові ситуації, а також ліквідації їх наслідків на ОКІ у взаємодії з іншими суб'єктами національної системи захисту критичної інфраструктури (СЗКІ)
ЗО7	Забезпечення відновлення функціонування ОКІ в разі виникнення аварій та інших небезпечних подій, вчинення протиправних дій
ЗО8	Участь у заходах із захисту повітряного простору над визначеними об'єктами критичної інфраструктури
ЗО9	Інформування органів у сфері захисту КІ про загрози та ризики диверсій, терористичних актів, актів КТ, надзвичайних ситуацій або інших подій, які небезпечни на державних об' єктах
ЗО10	Забезпечення постійного зв'язку з відповідальними за реагування на протиправні дії та з іншими компетентними організаціями та установами
ЗО11	Забезпечення постійної взаємодії з підприємствами: централізоване водопостачання, постачання теплової енергії, енергопостачання, функціонування електронних комунікаційних мереж, транспортне обслуговування, медичну допомогу, безпеку та інші послуги, від яких залежить процес реагування на кризові ситуації та відновлення функціонування ОКІ
ЗО12	Створення і використання необхідних резервів фінансових та матеріальних ресурсів для реагування на кризові ситуації та ліквідації їх наслідків
ЗО13	Проведення навчань та тренінгів, підготовка та перевірка персоналу, який відповідає за охорону, безпеку та захист ОКІ
ЗО14	Захист інформації про системи управління, зв'язку, фізичну безпеку та КБ, забезпечення відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про ОКІ
ЗО15	Забезпечення захисту персоналу ОКІ, організація та здійснення евакуаційних заходів у разі виникнення надзвичайних ситуацій

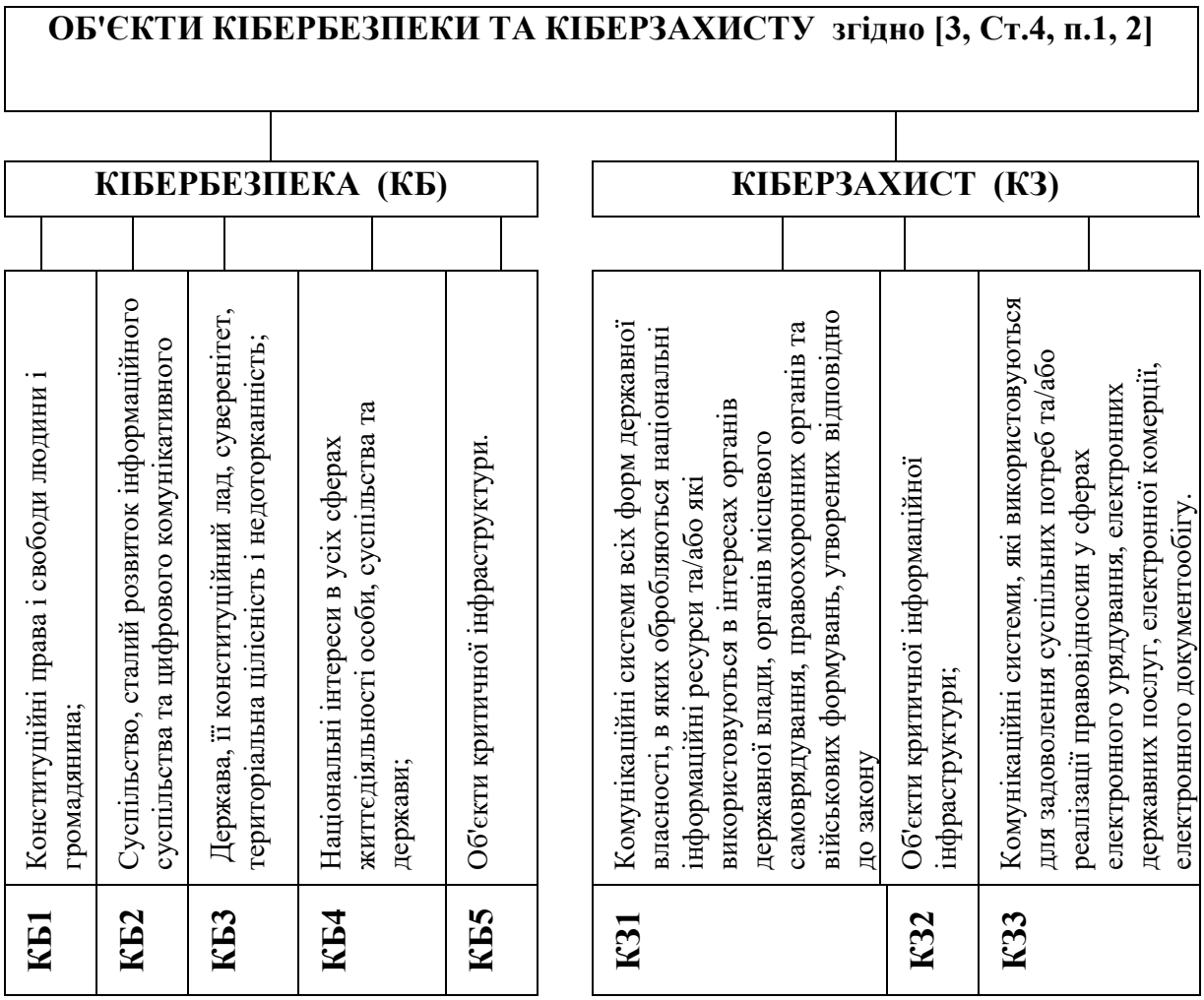

Рисунок 3 - СЛС "Об'єкти кібербезпеки та кіберзахисту"

2.2. Мета та завдання роботи

Метою роботи є оцінка (розгляд) структурно-лінгвістичних та структурно-функціональних схем (СЛС і СФС) як базових, з метою побудови пізнавальної моделі безпеки критичної інфраструктури, її наступної реалізації і вивчення ефективності штатної секторальної життєдіяльності СОКІ залежно від безперервних розвідувальних (і не лише ворожих) вторгнень в зону кіберпростору, що захищається. Завданням дослідження є методологія побудови пізнавальної інтегральної моделі безпеки СОКІ на основі структурно-лінгвістичних представлень згідно сучасного юридично-правового рівня України [1-3].

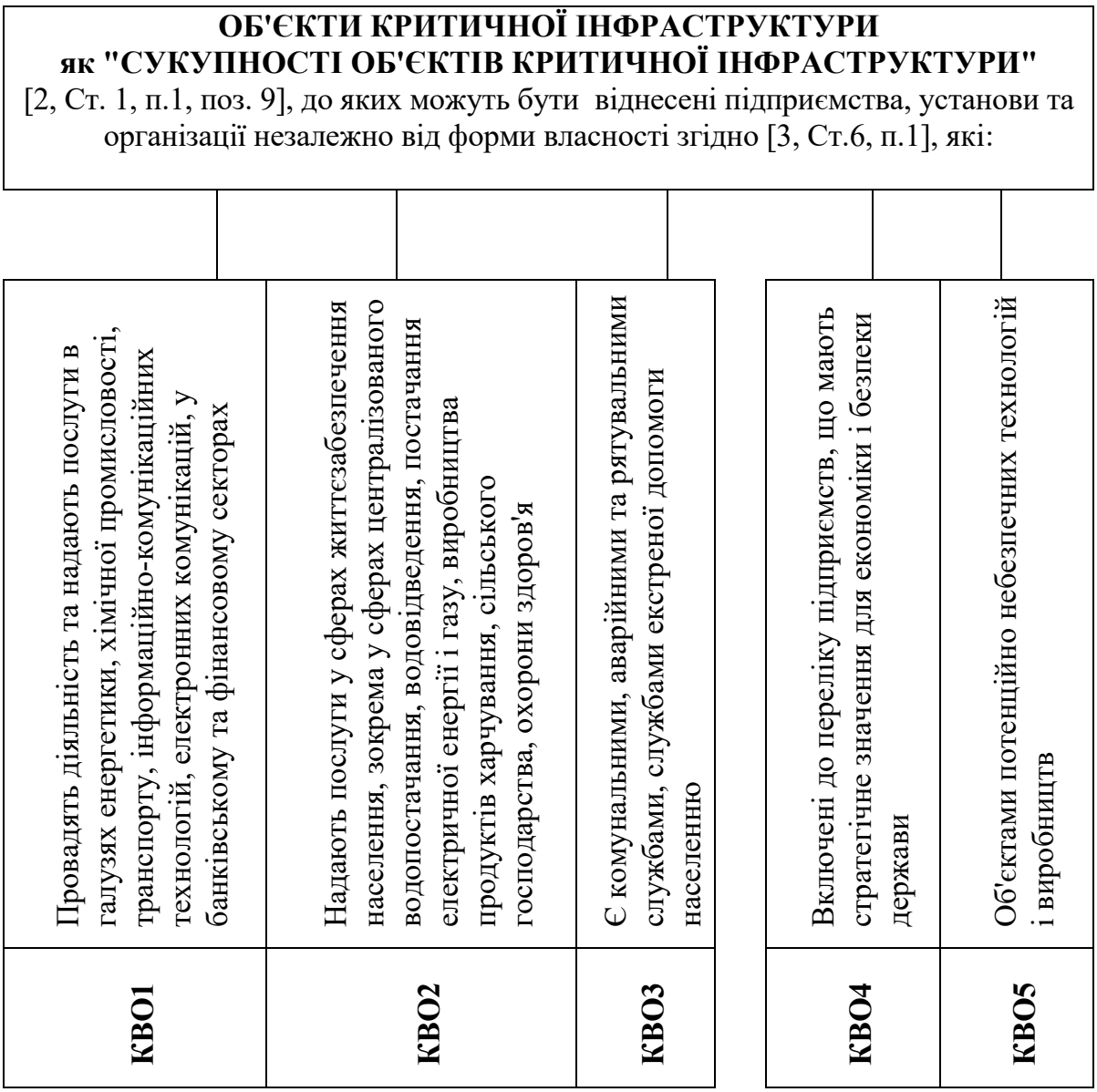

Рисунок 4 - СЛС "Сукупність об'єктів критичної інфраструктури"

2.3. Аспекти побудови системи захисту та безпеки сукупності об’єктів критичної інфраструктури

Завдяки задекларованій нормативно-правовій інформації, приведеній вище, послідовно реалізуємо згідно СЛС (рис.1 – 4, табл.1,2) сегментарну побудову системи захисту та безпеки об'єктів критичної інфраструктури (СЗБОКІ), в якій передбачені підсистеми забезпечення фізичної безпеки (ПсФБ) та кібербезпеки (ПсКБ), і система управління та зв'язку за наявності підсистеми підтримки прийняття рішень (ПсППР). Відповідно до методології побудови

пізнавальної моделі КВО з СЗБОКІ також доцільне введення підсистеми розпізнавання (ПсР): кіберзлочину, кібершпигунства, кібертероризма та інших киберінцидентів, тобто подій "або ряд несприятливих подій ненавмисного характеру (природного, технічного, технологічного, помилкового, у тому числі внаслідок дії людського чинника) та/або таких, що мають ознаки можливої (потенційної) кібератаки, які становлять загрозу безпеці систем електронних комунікацій, систем управління технологічними процесами, створюють імовірність порушення штатного режиму функціонування таких систем (у тому числі зриву та/або блокування роботи системи, та/або несанкціонованого управління її ресурсами), ставлять під загрозу безпеку (захищеність) електронних інформаційних ресурсів" [3.ст.1, п.3].

Останнє свідчить про багатофакторний характер безпеки кіберпростіру (тобто середовища – "(віртуальний простір), яку надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних" [3.ст.1, п.11]), де прояв різних критерійних імовірнісних аспектів кіберзагроз істотно впливає на кінцевий вердикт людини, що приймає рішення. В такому разі "кіберзагроза – наявні та потенційно можливі явища і чинники, що створюють небезпеку життєве важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів" [3.ст.1, п.6]).

Проте, незалежно від того, що з прийняттям нормативних документів України [1-3] фактично знівелювала нев'язка в термінологічному сприйнятті використовуваних термінів, тлумачення понять «кібербезпека» і «кіберзахист» вимагає уточнення, оскільки існує деяка відмінність між поняттями «безпека» і «захист». Зокрема, інформаційна безпека – це стан захищеності інформаційного середовища, а захист інформації – є діяльність по запобіганню просочуванню інформації, що захищається, у вигляді несанкціонованих і неумисних дій на інформацію, що захищається, тобто процес, спрямований на досягнення цього стану. Тому безпосереднє поняття захищеності об'єкту вказує на його (об'єкту)

захист від зовнішніх джерел небезпеки, тоді як безпека об'єкту – це внутрішня властивість об'єкту не бути джерелом небезпеки для довкілля [6, 7, с.95].

Очевидно, що СЛС та СФС об'єктів КЗ (ОКЗ) і КБ (ОКБ) можуть мати схожу за побудовою інформаційну схему підтримки прийняття рішень (ІСППР), оскільки відомо, що схема – це своєрідний графічний план, який визначає місце розташування основних компонентів конструкції та їх зв'язок. При цьому, процес вироблення рекомендацій з безпеки КІ лежить у площині прояву загроз, пов'язаних як з людським чинником, так і в площині проявів техногенних аварій, включаючи їх природне походження [8, с. 27]. А управління системою забезпечення захисту інформації критичної інфраструктури (ІКІ), як і у разі управління будь-якою соціально - технічною структурою [9, с.11], також пов'язане зі значними трудностями, спричиненими неповнотою інформації, конфліктами інтересів та цілей, швидкими та численними змінами у різних галузях, включаючи і здійснення інформаційної боротьби за потенційну безпеку КІ. Тому алгоритм прийняття рішень на всіх рівнях ієрархії з управління захистом ІКІ, за аналогами з [10], має відповідати сучасним математичним моделям щодо оптимізації ієрархічних структур.

Отже, основою побудови СЛС та СФС для випадку оцінювання КІ дійсно може бути лінгвістичний опис об'єкта пізнання з відображенням його внутрішніх та зовнішніх причинно-наслідкових зв'язків та врахування існуючих загроз з їхньою імовірнісною гіпотетичною оцінкою. Причому, відмінність СЛС від СФС, головним чином у тому, що перша дозволяє проводити аналіз статичної картини об'єкта пізнання із зазначенням прив'язки (локації) функціональних елементів (ланок). Друга ж, тобто СФС, дозволяє оцінити динамічні можливості об'єкта пізнання, оскільки, крім вказівки локації задіяних елементів і вузлів з них, відображає їхню взаємодію. Завдяки цьому для стохастичних систем, лінгвістичний опис яких у процесі дослідження (пізнання) реалізовано, існує можливість побудови конструктивних моделей з елементами інтелектуальної кіберфізичної системи, що включають інженерно - взаємодіючі мережі фізичних та обчислювальних компонентів, тобто через комп'ютерні мережі і вбудовані контролери забезпечується (автономно або за участю людини) управління фізичними процесами за допомогою реалізації

зворотних зв'язків [11. стор. 34, 12, стр.29].

Отже, доцільно застосування ймовірнісне-статистичних методів для оцінки стану безпеки об'єктів КІ в умовах конкретизації ймовірності випадкових недружніх для них впливів (наприклад, у вигляді ймовірності правильного виявлення або у вигляді ймовірності пропуску загрози), а їх конкретне використання може бути обрано після детального аналізу щодо аналізу СЛС та СФС побудови (у нашому випадку стану безпеки) КІ.

Очевидно, що міцність захисту залежить від тактико-технічних даних (ТТД) і тактико-технічних характеристик (ТТХ) перешкоди і вважається прийнятною, якщо вартість очікуваних витрат на її подолання порушником (хакером) перевищує вартість інформації, що захищається при дотриманні затребуваних реальних тимчасових умов з її подолання [13, с. 80-82]. Отже, якісна побудова цілісної системи захисту вже на етапі створення безпосередньої пізнавальної моделі гіпотетичного захисту від можливих інцидентів і кібератак вимагає встановлення тотожності ТТХ та механізмів функціонування об'єкта, що охороняється, до і після будь-яких нештатних (несанкціонованих) впливів на об'єкт. У подальшому аналіз такої ідентифікації (розпізнавання відмінностей до і після) доцільно використовувати при нівелювання проблем незахищеності об'єктів, що охороняються, і оптимізації при їх експлуатації.

З таких позицій в пізнавальній моделі безпеки ОКІ спільно з ПсР кіберзагроз, кіберінцидентів та кібератак необхідно передбачати як режим захисту від потенційно ворожих дій на СОКІ, так і режим представлення інформації у структурованому, систематизованому та закодованому вигляді за допомогою системи управління і зв'язку з СЗБОКІ у вигляді символічних, графічних, візуальних, словесних та інших знаків. А оскільки кількість перешкод захисту залежить від апріорних (заздалегідь очікуваних) атак, то на противагу кожній з них мають бути передбачені свої схемотехнічні рішення, що забезпечують адекватну реалізацію відповідних перешкод захисту. Більше того, така схема методології побудови системи безпеки та захисту ОКІ (рис.5), має передбачати захист від передбачуваних (очікуваних) видів випадкових впливів, наприклад: у вигляді стихійних відважний та аварій; збоїв та відмов

технічних засобів; навмисних та неусвідомлених помилок персоналу та користувачів, включаючи і руйнівні дії зловмисників, що використовують найширший спектр шляхів обходу та методів доступу до даних у процесі обробки та обміну інформацією.

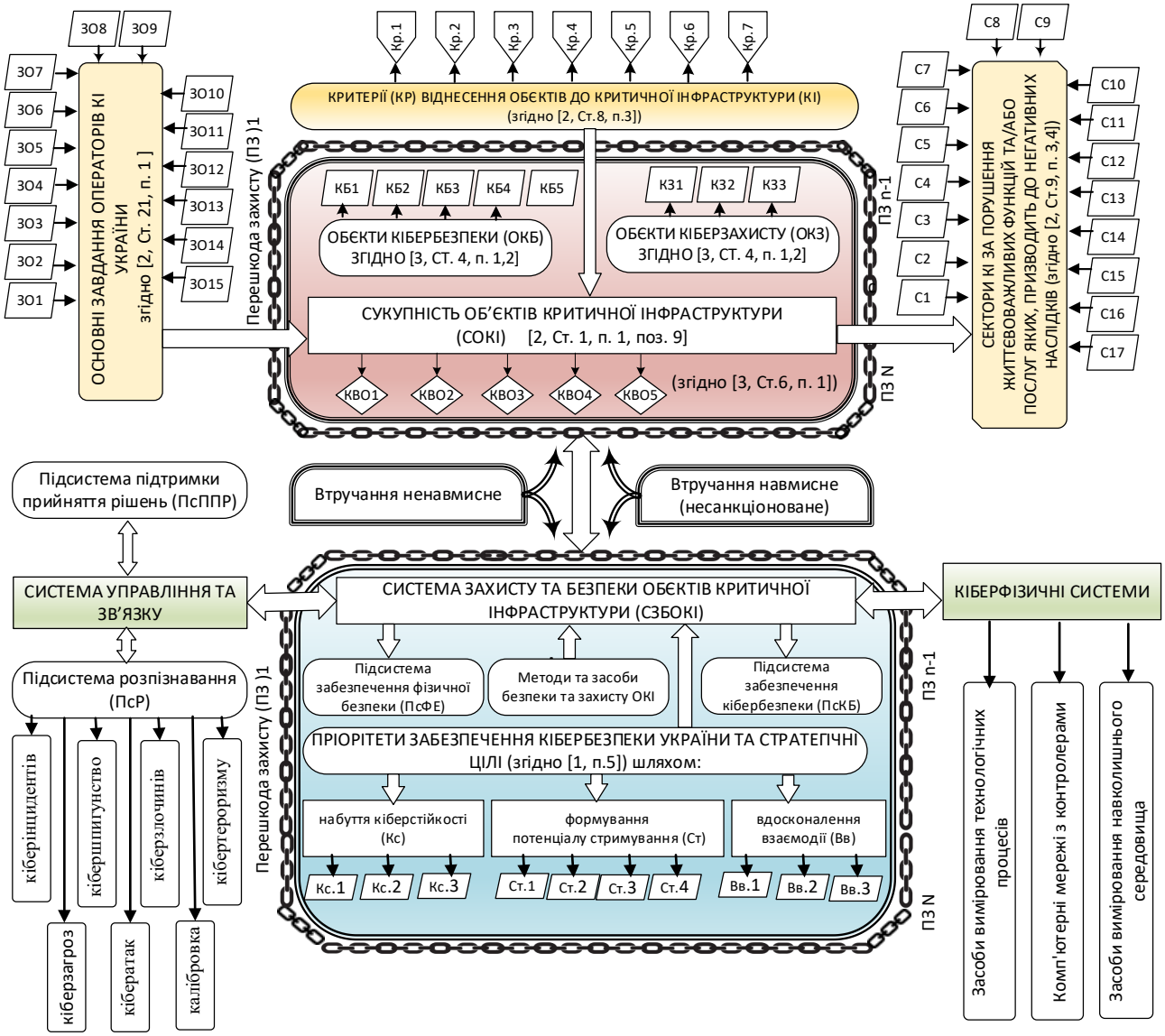

Рисунок 5 - Схема методології побудови системи захисту та безпеки об'єктів критичної інфраструктури

При цьому професійний аналіз апріорних вразливостей, включаючи безпосередньо і саму систему фізичної охорони, адекватно повинний відповідати рівню необхідної (достатньої) безпеки, методики розрахунку ефективності захисних заходів яких дуже різноманітні від рангу (ступеня допуску) інформації, що захищається, і моделі порушника. Отже, правильно

побудована (адекватна реальності) модель СОКІ з його СЗБОКІ, а також модель порушника, в якій відображаються його практичні та теоретичні можливості, апріорні знання, час і місце дії та інші характеристики, є важливою складовою успішного проведення аналізу ризику та визначення вимог до складу та характеристик інтегральної системи захисту.

Проте, навіть в умовах багаторівневої системи перешкод жодна пізнавальна модель не може одночасно виконувати велику кількість завдань "захисного напрямку". Тому доцільно оцінювати ефективність моделі в конкретному обраному аспекті її реалізації [13, с.93]. Зокрема, виявлення несанкціонованих повітряних атак зловмисників до підриву конкретної захисної оболонки об'єкта можливо шляхом реалізації радіолокації ближньої взаємодії (РБВ) [14, с. 66]. При цьому завдання загальної та параметричної ідентифікації розпізнавання потенційного втручання за допомогою дослідження гіпотетичної сигнальної аналогової дії можна звести до кореляційної обробки зондувальних та відбитих сигналів [14, с. 403], наприклад, від дронів, які вторглись у повітряну область КВО, що охороняється. В даному випадку, оптимальність вибору зондувального сигналу залежить, з одного боку, від результату апріорного аналізу його сигнальної функції та відповідного об’ємного тіла невизначеності, а з іншого боку – від вимог забезпечення скритності самого процесу виявлення (дронів) із високою роздільною здатністю за двома параметрами – його дальності та швидкості. Насамкінець зазначимо, що за рахунок схемотехнічної реалізації взаємно-кореляційних пристроїв РБВ, наприклад такого, що використовує шумоподібний безперервний надвисокочастотний (НВЧ) зондувальний сигнал з амплітудною модуляцією у вигляді пачки з N когерентних імпульсів гаусової форми [14, с. 403], доцільно забезпечувати (при створенні сучасних систем управління) моніторинг кіберпростору, в основі якого і простежується ідеологія кореляційного аналізу вхідної обурюючої дії сигналу (або сигнальної функції), що підпадає під виявлення, виміру та розпізнавання.

Висновки

В роботі показаний взаємозв'язок із законодавчою базою України побудованих структурно-лінгвістичних схем: пріоритетів забезпечення кібербезпеки України та стратегічних цілей, критерієв віднесення об'єктів до критичної інфраструктури, секторів критичної інфраструктури, основних завдань операторів критичної інфраструктури, об'єктів кібербезпеки та кіберзахисту, сукупності об'єктів критичної інфраструктури. Також викладена методологія побудови пізнавальної інтегральної моделі безпеки сукупності об'єктів критичної інфраструктури на основі структурно - лінгвістичних представлень згідно сучасного юридично-правового рівня України, та відображена у вигляді схеми з детальним вказанням напрямків співвідношень між структурними елементами. Запропоновано використання шумоподібного безперервного НВЧ зондувального сигналу з амплітудною модуляцією у вигляді пачки з N когерентних імпульсів гаусової форми, який забезпечує скритність функціювання РБВ з метою моніторингу кіберпростору та виявлення несанкціонованого втручання в кіберпростір, що охороняється.