ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи

на тему:

«ТЕХНОЛОГІЇ РОЗВИТКУ І ЗАХИСТУ КІБЕРПРОСТОРУ ВІД ІНФОРМАЦІЙНОГО ВПЛИВУ В УМОВАХ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА»

Виконав: студент 6 курсу, групи БСДМ-61
Спеціальності 125 Кібербезпека
Освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Кравченко Б.А.
(прізвище та ініціали)
Керівник Власенко В.О.
(прізвище та ініціали)
Рецензент_____
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2020

РЕФЕРАТ

Текстова частина магістерської роботи: 79 сторінки основного тексту, 12 рисунків та 74 джерела.

Об'єктом дослідження є: інформаційні впливи в умовах інформаційного протиборства. **Предметом дослідження** є інформаційні системи, кіберпростір, методи та моделі.

Метою дипломної роботи є: аналіз розвитку сучасних методів оцінювання інформаційних впливів на основі підходів провідних держав та оптимізації методів захисту кіберпростору від інформаційних впливів.

Методи дослідження. Для вирішення поставленого завдання в роботі застосовуються методи теорії систем і системного аналізу, теорії ймовірностей та математичної статистики, теорії прийняття рішень, теорії інформації, методів моделювання.

В роботі проведено аналіз сучасних методів моделювання інформаційних впливів, систематизовано проблеми оптимізації систем захисту кіберпростору від інформаційних впливів. А також досліджено методи оцінювання загроз в кіберпросторі та розроблено рекомендації щодо оптимізації методів захисту кіберпростору від інформаційних впливів.

Галузь використання - інформаційна безпека держави, безпека підприємства.

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ, ІНФОРМАЦІЙНИЙ ВПЛИВ, ЗАГРОЗА, АТАКА, ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРПРОСТІР, СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

БД	-	база даних
БЗ	-	база знань
ЗМІ	-	засоби масової інформації
ІБ	-	інформаційна безпека
ІБД	-	інформаційна безпека держави
ІП	-	інформаційний простір
ІС	-	інформаційна система
КС	-	комп’ютерна система
СЗІБД	-	система забезпечення інформаційної безпеки держави
СІБ	-	система інформаційної безпеки
СІС	-	соціальна інформаційна система
СППР	-	система підтримки прийняття рішень
ССП	-	системи спеціального призначення
ARIS	-	архітектура інтегрованих інформаційних систем
ISO	-	міжнародна організація зі стандартизації
UML	-	уніфікована мова моделювання

ВСТУП

Актуальність теми. Наслідками стрімкого розвитку інформаційних технологій у світі та Україні є суттєве прискорення інформатизації суспільної діяльності, посилення процесів глобалізації та інтернаціоналізації. Активізація інформаційних процесів вплинула й на систему стратегічних комунікацій суспільства, у якій провідна роль відводиться комунікативній складовій. Зважаючи на постійне удосконалення інформаційного середовища, кіберпростір перетворився на домінуючий канал поширення інформації та комунікації громадян. Інформаційна система надає користувачам засоби для обміну контентом різного типу, утворення зв'язків з іншими користувачами, саморозвитку, об'єднання у віртуальні спільноти за спільними інтересами тощо. Інформаційна система створює потужні можливості залучення грошових, людських, інформаційних ресурсів у національну економіку для зміцнення конкурентних позицій та сталого розвитку держави. Одночасно інформаційна система виступає ефективним і дієвим інструментом становлення громадянського суспільства. Завдяки наявності засобів створення контенту у мережі Інтернет, його збереження та використання з метою задоволення інформаційних інтересів і потреб громадян, соціальний інформаційний простір представляє собою невід'ємну складову національного кіберпростору.

Зважаючи на останні події, ІС перетворилась на джерело загроз інформаційній безпеці держави (ІБД). У результаті поширення недостовірного, неповного або упередженого контенту у поєднанні з технологіями інформаційно-психологічного впливу на індивідуальну, колективну і масову свідомість, у суспільстві можуть мати місце прояви національної та релігійної ворожнечі, закликів до зміни конституційного ладу насильницьким шляхом або порушення суверенітету й територіальної цілісності держави. Досвід збройної агресії Російської Федерації проти України вперше продемонстрував, що ІС є однією з ефективних інструментів ведення нової форми протистояння – гібридної війни. У

той же час Російською Федерацією ведеться інформаційна війна проти України, Європейського Союзу та Сполучених Штатів Америки. При цьому слід враховувати те, що вона поєднує в собі дві частини однієї проблеми – інформаційний вплив (інформаційні операції) і психологічний вплив (психологічні операції), які в ході інформаційного протиборства, що ведеться зокрема з використанням ІС, застосовуються для маніпулювання особистістю, групою людей та масами. У дипломній роботі розглядаються тільки інформаційні впливи. Тому, зважаючи на комплексний характер загроз інформаційній безпеці в інформаційній сфері, проблема розроблення ефективних підходів до побудови системи забезпечення ІБД у ІС в умовах глобалізації та вільного обігу інформації є особливо актуальною.

Мета і завдання дослідження. Метою дипломної роботи є аналіз розвитку сучасних методів оцінювання інформаційних впливів на основі підходів провідних держав та оптимізації методів захисту кіберпростору від інформаційних впливів.

Для досягнення поставленої мети необхідно вирішити такі *основні завдання:*

1. Провести аналіз сучасних методів моделювання інформаційних впливів.

2. Систематизувати проблеми оптимізації систем захисту від інформаційних впливів в умовах інформаційного протиборства.

3. Дослідити методи оцінювання загроз інформації в кіберпросторі.

4. Розробити етапи оптимізації методології захисту кіберпростору від інформаційних впливів.

Об'єктом дослідження є інформаційні впливи в умовах інформаційного протиборства.

Предметом дослідження є інформаційні системи, кіберпростір, методи та моделі.

Методи дослідження. Проведені дослідження базуються на сучасних методах теорії систем і системного аналізу, теорії ймовірностей та математичної статистики, теорії прийняття рішень, теорії інформації, методів моделювання.

Ступінь новизни одержаних результатів. Набув подальшого розвитку метод захисту кіберпростору від інформаційних впливів.

Практичне значення одержаних результатів у сукупності складає методологічне підґрунтя для ефективного функціонування системи забезпечення ІБД у ІС в умовах інформаційного впливу. Отримані результати можуть бути використані для розроблення систем забезпечення інформаційної безпеки та їх складових.

Апробація. Основні тези роботи опубліковані на XIII Науково-практична конференція „Пріоритетні напрямки розвитку телекомунікаційних систем та мереж спеціального призначення. Застосування підрозділів, комплексів, засобів зв'язку, автоматизації та кібербезпеки в операції Об'єднаних сил" 3 грудня 2020 року ВІТІ.

1 АНАЛІЗ РОЗВИТКУ МЕТОДІВ МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ ВПЛИВІВ

1.1. Аналіз ступеня теоретичної обґрунтованості відомих підходів

Зважаючи на політичні тренди провідних держав світу, пов’язані з посиленням національної безпеки, відбувається поступове удосконалення систем забезпечення ІБД відповідно до вимог сьогодення. Головне завдання на цьому шляху полягає у розробленні нормативно-правового забезпечення для регламентації загальних принципів забезпечення ІБД з подальшим їх використанням у відомчих і корпоративних керівних документах та формуванні міжнародних договорів у галузі ІБ [50], [51], [41].

Вперше стратегія ІБД прийнята в США у 2003 р., яким належить лідерство у галузі інформаційних технологій, внаслідок чого вони першими зазнали деструктивного впливу загроз. Національна стратегія досягнення безпеки в кіберпросторі (National Strategy to Secure Cyberspace) спрямовувалася на формулювання засадничих принципів захисту національного інформаційного простору, визначала напрямки підвищення ефективності реагування на інциденти ІБ [41]. Стратегія встановила наступні основні пріоритети держави у напрямку забезпечення ІБ, на базі яких формується діяльність та структура відповідних урядових організацій [53], [54]:

а) розвиток національної системи реагування на загрози ІБД;

б) здійснення комплексних заходів щодо стримування і зменшення загроз ІБД;

в) впровадження програм підготовки фахівців у галузі ІБД;

г) захист інформаційних систем, які функціонують в урядовому сегменті;

д) організація ефективної взаємодії, зокрема міжнародної, з питань забезпечення ІБД.

У свою чергу, визначені в стратегії пріоритети реалізовані у вигляді ряду законодавчих ініціатив, спрямованих на їх реалізацію. Зокрема, у 2009 р. прийнято Акт про кібербезпеку (The Cybersecurity Act of 2009) для закріплення за Президентом США владних повноважень щодо відключення мережі Інтернет у випадку виникнення надзвичайних ситуацій, пов'язаних з впливом загроз ІБД. Одночасно урядом підтримано Акт глобальної відповіді на кібервиклики (Fostering a Global Response to Cyber Attacks Act), згідно з яким визначається можливість взаємодії США з іншими державами для протидії злочинам у сфері ІБД [54], [55].

Особливе значення для забезпечення ІБ США має затверджена у 2011 р. Міжнародна стратегія для кіберпростору (International Strategy for Cyberspase: Prosperity, Security and Openness in a Networked World) [56]. Документ визначає найважливішими характеристиками кіберпростору його відкритість, доступність і безпечність, формує курс міжнародної співпраці для захисту інтересів США та їх союзників у галузі ІБ. При цьому встановлено сім пріоритетних напрямків функціонування уряду [41], [57]:

1. Забезпечення сталого розвитку національної економіки внаслідок формування міжнародного відкритого ринкового середовища, що використовує технологічні інновації та регулюється набором сумісних стандартів.

2. Захист інформаційно-комунікаційних мереж завдяки посиленню їх безпеки, надійності та стійкості функціонування у результаті міждержавної взаємодії та партнерства, мінімізації вторгнень у роботу інформаційно-комунікаційних мереж та своєчасного реагування на інциденти.

3. Розширення міжнародного співробітництва і сприяння законодавчому регулюванню питань ІБ шляхом повноправної участі й координації процесів розроблення відповідної законодавчої бази на міжнародному рівні.

4. Нарощування воєнної складової у вирішенні проблем щодо забезпечення ІБД, яке досягається задоволенням потреб збройних сил у безпечних інформаційно-комунікаційних мережах, оновленням формату військових союзів і розширенням напрямків співробітництва з партнерами для протидії загрозам та підвищення рівня ІБД.

5. Формування умов для стійкого розвитку мережі Інтернет шляхом створення ефективних структур управління, забезпечення його відкритості та використання інноваційних технологій, підтримки безпеки і стабільності, організації ефективної взаємодії фахівців у напрямку управління мережею Інтернет.

6. Розвиток потенціалу забезпечення ІБД завдяки відкритому доступу до навчальних матеріалів й інформаційних ресурсів для зацікавлених держав, допомозі у підготовці фахівців різного спрямування, сприянню щодо примноження технічних засобів для протидії загрозам.

7. Підтримка фундаментальних принципів свободи в мережі Інтернет, яка зводиться до створення дієвих і безпечних майданчиків об'єднання громадян та їх самовираження, взаємодії з громадянським суспільством з питань ІБД, спонукання міжнародної співпраці для реалізації захисту комерційної інформації.

Результати аналізу нормативно-правового забезпечення ІБД у США свідчать про існування стійких тенденцій розвитку СЗІБД і вироблення дієвих підходів до протидії загрозам у інформаційному просторі. Однак, на практиці існуючі законодавчі ініціативи не завжди є ефективними й іноді мають характер доктрини [41], [53], [55]. Така ситуація пояснюється постійним зростанням рівня сучасних загроз ІБД, зокрема у СІС, експоненціальним збільшенням значущості національного інформаційного простору для сталого розвитку держави.

Передові позиції у галузі забезпечення ІБД серед країн центральної Європи належить Естонії. В 2008 р. було затверджено Стратегію кібербезпеки Естонії на 2008 - 2013 рр., яка законодавчо закріпила напрямки реалізації заходів щодо забезпечення ІБД. До розроблення стратегії сумісно з урядом Естонії залучалися представники недержавних організацій, також враховувався міжнародний досвід і рекомендації ЄС та НАТО. Відповідно до цього документу, урядова політика в галузі кібербезпеки направлена на [41], [55]:

а) оцінювання вразливостей об'єктів критичної інфраструктури;

б) розроблення системи попередження кібератак;

в) розподіл повноважень між урядовими установами і організаціями у сфері управління кібербезпекою;

г) удосконалення нормативно-правового забезпечення;

д) сприяння міжнародному співробітництву;

е) підвищення ступеня поінформованості громадян про загрози кібербезпеці.

Стратегія визначає такі глобальні цілі у сфері ІБД:

1. Розроблення багаторівневої системи захисту об’єктів критичної інфраструктури, вироблення і впровадження заходів щодо забезпечення ІБ, вдосконалення сукупності організаційних дій.

2. Підвищення рівня знань громадян шляхом проведення практичних тренінгів, виконання наукових досліджень.

3. Покращення нормативно-правового регулювання питань ІБД, його реалізація і впровадження, розроблення законодавчих ініціатив на міжнародному рівні.

4. Посилення лідерських позицій Естонії у міжнародному співробітництві у сфері протидії загрозам ІБД.

Нині чинна стратегія кібернетичної безпеки Естонії на 2014 - 2017 рр. [59] зосереджена на питаннях захисту об’єктів критичної інфраструктури, кіберзлочинності та забезпеченні національної безпеки держави.

Стратегія кібербезпеки Великобританії [60] визначає одним з основних завдань стимуляцію ефективного використання інноваційних технологій у кіберпросторі для створення надійного і безпечного середовища розвитку суспільства та національної економіки. Для цього держава ініціює посилення співпраці між урядовим і приватним сектором, зокрема в розрізі обміну інформацією [41]. Особливого значення набувають потреби держави у розвитку національної галузі захисту інформаційно-комунікаційних мереж; підготовці висококваліфікованих фахівців з ІБ; розробленні та уніфікації стандартів, які встановлюють правила ведення бізнесу з використанням ресурсів мережі Інтернет; впровадженні заходів з попередження реалізації загроз і підвищенні рівня

компетентності громадян щодо ІБ; удосконаленні нормативно-правової бази регулювання сфери ІБД.

Особливої уваги потребує досвід Великобританії щодо нормативно-правового регулювання відносин користувачів мережі Інтернет. Поширення серед громадян інформації про існуючі загрози ІБД у мережі Інтернет виконується представниками відповідних державних установ і експертів з приватного сектору з використанням СІС. У випадку поширення контенту, який порушує чинне законодавство, хостинг-провайдер може бути притягнутий до відповідальності, а доступ інтернет-провайдера послуг до такого контенту лімітується [55]. Важливим механізмом контролю інформаційного простору мережі Інтернет є кодекс поведінки хостинг-провайдерів, який забезпечує процеси саморегуляції на ринку послуг.

Метою створення стратегії кібербезпеки Польщі [61], запропонованої Агентством внутрішньої безпеки і затвердженої урядом у 2013 р. є захист громадян, суб'єктів економічної діяльності, урядових установ від загроз ІБД. Першочергові завдання держави полягають у координації процесів реагування відповідних урядових організацій на факти реалізації загроз і створення системи обміну ресурсами та інформацією для протидії викликам ІБД. Стратегією передбачено розроблення законодавчих ініціатив у сфері ІБД, підвищення рівня освіченості громадян з питань безпеки, збільшення чисельності особового складу відомчих структур для реагування на загрози, впровадження заходів стримування появи загроз.

Таким чином, аналіз існуючих підходів до забезпечення ІБ провідних країн світу свідчить про активізацію робіт з розроблення і вдосконалення рамкових нормативно-правових документів, які визначають напрямки забезпечення національної безпеки у інформаційній сфері. Незважаючи на відмінність категоріального апарату, підходів до формування державної політики у галузі ІБД та її реалізації, спільним для всіх країн залишається усвідомлення високого рівня небезпеки сучасних загроз. Об'єднання зусиль міжнародного співтовариства для захисту глобального інформаційного простору завдяки удосконаленню

законодавчої бази, посиленню співпраці, обміну досвідом, підготовці фахівців дозволить підвищити рівень ІБД окремих держав зокрема [41], [62].

Особливо гостро проблема забезпечення ІБД в Україні постає в умовах гібридної війни з Російською Федерацією, у результаті якої сфера інформаційної діяльності перетворилася на арену інформаційного протиборства. Затверджена у 2017 р. Доктрина інформаційної безпеки України [63] відображає концепцію протидії цілеспрямованим агресивним загрозам національній безпеці в інформаційній сфері. Метою Доктрини є "уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни" [63]. Доктрина ґрунтується на дотриманні прав і свобод людини й громадянина; захисті життєво важливих інтересів особи, суспільства, держави; забезпеченні суверенітету і територіальної цілісності держави [63].

У документі наведено дефініції категорій "стратегічні комунікації", "урядові комунікації", "кризові комунікації", "стратегічний наратив", узгоджено компетенції виконавчих органів щодо забезпечення ІБД. Встановлено, що провідна роль у процесі реалізації Доктрини й координації взаємодії виконавчих органів належить Раді національної безпеки і оборони України (РНБОУ). Реалізація визначеної інформаційної політики держави покладена на Кабінет міністрів України (КМУ). Головним суб'єктом забезпечення ІБД виступає Міністерство інформаційної політики України (МІПУ), на яке покладаються завдання щодо моніторингу ЗМІ та національних ресурсів мережі Інтернет на предмет поширення інформації, що порушує законодавство. Також функції МІПУ зводяться до моніторингу загроз ІБД, визначення напрямків інформаційної політики, узгодження дій органів виконавчої влади, інформаційного супроводу поновлення контролю над тимчасово окупованими територіями тощо.

Слід зауважити, що відсутність дієвих засобів координації і забезпечення гнучкості процесів взаємодії відповідних державних структур негативно позначається на інформаційному суверенітеті України. У свою чергу, імплементація чинної Доктрини вимагає додаткового прийняття ряду нормативно-

правових документів, які забезпечать врегулювання процедур реалізації закріплених у ній положень на практиці [64], [65].

Зважаючи на провідне місце СІС в системі стратегічних комунікацій суспільства, сформульована у Доктрині потреба визначення інноваційних підходів до протидії комплексним загрозам ІБД вимагає побудови дієвої системи захисту національного інформаційного простору в СІС. Розроблення новітніх напрямків забезпечення ІБД у СІС повинне здійснюватися виходячи з аналізу існуючих наукових досліджень. Незважаючи на постійно зростаючу кількість публікацій, присвячених віртуальним спільнотам, проблема забезпечення ІБД у СІС залишається невирішеною. У свою чергу, з цією проблемою пов'язані питання щодо виявлення і оцінювання загроз життєво важливим інтересам особистості, суспільства та держави у СІС; розроблення нових підходів і комплексу заходів з протидії загрозам у СІС; розроблення цілісної методології побудови СЗІБД у СІС тощо [28], [66].

Публікації [28], [41], [67], [68] продемонстрували, що загрози у СІС носять комплексний характер, а їх кількість постійно збільшується. Встановлено, що загрози ІБД у СІС відрізняються за масштабністю, способом впливу на акторів, частотою повторюваності тощо [69], [70]. Тому сучасні загрози ІБД є складноформалізованими сутностями, характеризуються різноманітними ознаками прояву як в окремих, так і у різних видах СІС. Внаслідок відсутності узагальнених проявів загроз ІБД у СІС, розвитку технологій прихованого впливу на акторів, ускладнюються й процеси їх детектування. Тому виявлення і оцінювання загроз є проблемою на шляху побудови дієвої СЗІБД у СІС.

Поряд з тим, з праць [69], [71], [72] відомо, що СІС належать до класу складних нелінійних динамічних систем. Однією з властивостей таких соціотехнічних систем є перехід до хаотичної динаміки у результаті дії на них збурень. Отже, наслідком реалізації загроз ІБД у СІС може бути перехід віртуальних спільнот акторів до некерованого стану і непередбачуваність їх поведінки в реальному житті. Тому нині особливо гостро стоїть проблема

розроблення комплексу заходів для завчасної та ефективної протидії загрозам ІБД у СІС.

Забезпечення визначеного (заданого) стану ІБД у віртуальних спільнотах, відповідно до чинної Доктрини інформаційної безпеки України [63] та проекту Концепції інформаційної безпеки України [77], вимагає створення системи захисту інформаційного простору в СІС. Дослідження [50], [66], [73] показали, що система забезпечення ІБД представляє собою складову системи забезпечення національної безпеки держави з одного боку і складається з відомчих підсистем для вирішення окремих завдань з іншого. Встановлено, що в умовах зростання рівня загроз у державі відсутня науково обґрунтована методологія побудови СЗІБД у СІС. Аналіз показав, що існуючі засоби і відомчі підсистеми недостатньо забезпечені науковим інструментарієм виявлення загроз ІБД у СІС, а протидія здійснюється із затримкою [74]. Внаслідок недостатнього рівня захисту інформаційного простору СІС від загроз держава, її суспільство і окремі громадяни перетворилися на суб'єкти деструктивних зовнішніх та внутрішніх інформаційних впливів.

Таким чином, у результаті критичного аналізу теоретичної обґрунтованості відомих підходів до забезпечення ІБД встановлено, що:

- у світі існує стійка тенденція створення нормативно-правових документів, які визначають і регламентують базові принципи забезпечення безпеки національного інформаційного простору. Пріоритетними напрямками діяльності провідних держав світу у сфері ІБ є розроблення ефективних СЗІБД для створення безпечного середовища розвитку суспільства і сталого розвитку національної економіки;

- концептуальним документом, який закріплює засади формування інформаційної політики України під час гібридної війни з Російською Федерацією, є Доктрина інформаційної безпеки. Доктрина визначає механізми протидії інформаційному впливу агресора та спирається на дотримання прав і свобод людини й громадянина з одного боку та гарантування інформаційного суверенітету держави з іншого. У свою чергу, документ встановлює передумови для розроблення ефективних підходів до забезпечення ІБД у СІС, що є актуальним

теоретико-прикладним завданням в умовах глобалізації і необмеженого обігу інформації та потребує свого подальшого вирішення;

- встановлено, що сьогодні відсутні загальноприйняті підходи до реалізації задекларованих у Доктрині інформаційної безпеки України механізмів протидії зовнішнім і внутрішнім загрозам. Отже, невирішеними частинами загальної проблеми на шляху забезпечення ІБД у СІС є виявлення і оцінювання рівня загроз, розроблення комплексу заходів для завчасної та ефективної протидії, відсутність науково обґрунтованої методології побудови СЗІБД у СІС.

1.2. Поняття та види інформаційних впливів

Метою інформаційного впливу є активізація алгоритмів, відповідальних за порушення звичного режиму функціонування, тобто за виведення ІС за межі допустимого стану.

Джерело впливу може бути як зовнішнім по відношенню до системи, так і внутрішнім (рис. 1.1).

Причини зовнішніх впливів у разі цілеспрямованої інформаційної дії (у разі інформаційної війни) приховані в боротьбі конкуруючих ІС за загальні ресурси, що забезпечують системі допустимий режим для існування.

Причини внутрішніх впливів зобов’язані своїм існуванням появі усередині системи множини елементів, підструктур, для яких звичний режим функціонування став з огляду на ряд обставин неприпустимим.

Під допустимим режим функціонування розуміється таке функціонування ІС, яке забезпечене необхідними матеріальними ресурсами. Відповідно, неприпустимим режимом називається режим, знаходячись в якому система не забезпечена повною мірою необхідними для нормального функціонування матеріальними ресурсами.

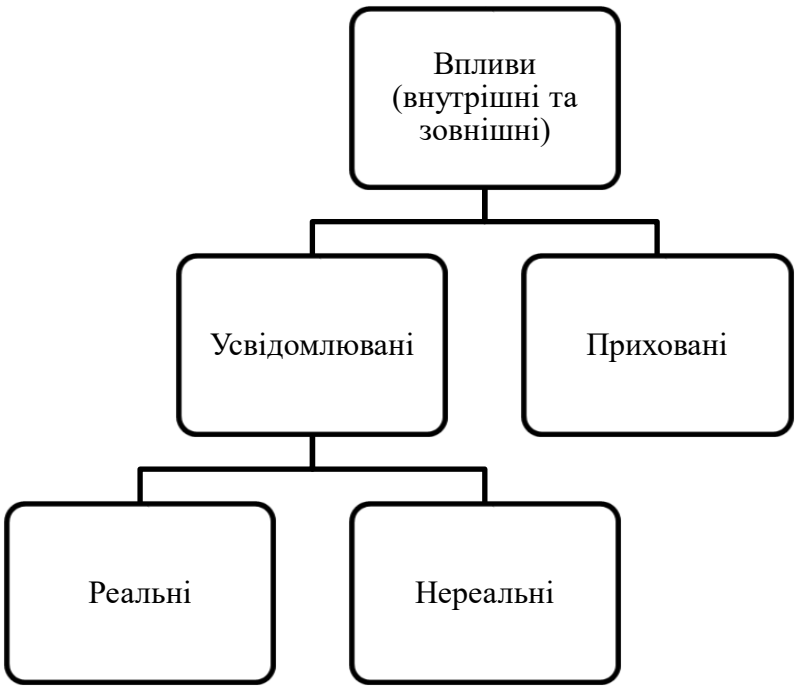

Рис. 1.1. Класифікація впливів

Таким чином, інформаційний вплив є вхідними даними, призначеними для активізації в ІС алгоритмів, відповідальних за порушення штатного режиму функціонування.

Відповідно до класифікації на рис. 1.1, зовнішні і внутрішні впливи поділяються на усвідомлювані системою (явні) і неусвідомлювані (приховані).

Явний вплив направлений на порушення штатного режиму функціонування системи. Крім того, явний вплив може бути реальним та нереальним. Проте, незалежно від того, як система сприймає вплив (або реальність), важливо, що якщо ІС здатна сприймати вхідні дані як вплив, то цей факт однозначно говорить про те, що даний вплив є явним.

Етапи обробки явного впливу:

1. Система приймає вхідні дані;

2. Система оцінює вхідні дані. Якщо вхідні дані є впливом, то перехід до п.3, інакше – до п.1;

3. Система оцінює реальність впливу. Якщо вплив реальний, то перехід до п.4, інакше – повернення до п.1.

4. Система оцінює свої можливості по організації захисту і величину власного збитку у разі програшу. Якщо втрати організації захисту оцінені меншою величиною (моральний, матеріальний збиток тощо), чим збиток від приведеного в дію впливу, то перехід до п.5, інакше – п.7.

5. Активізація алгоритмів, що реалізують способи інформаційного захисту. Якщо цього недостатньо, то активізація алгоритмів, відповідальних за пошук нових, нестардатних способів вирішення задачі.

6. Система оцінює результати інформаційного протиборства. У разі успіху перехід до п.1., інакше до п.7.

7. Виконання дій, відповідно до вимог інформаційного агресора. Якщо система залишається «функціонуючою», то перехід до п.1, отже, до тих пір, поки система «функціонує».

Як показано вище, явний вплив залишає системі шанс, дозволяє робити ходи у відповідь та припускає, що за ним прослідують певні дії, які завдають інформаційній системі збитку. Прихований вплив тому і називається прихованим, що він не фіксується системою захисту інформації об’єкту в режимі реального часу та не надає шансу.

Виходячи з аналізу впливу для захисту від зловмисника доцільно виконати наступні операції:

– поставити бар’єр між ІС та джерелом небезпеки;
– сховати ІС від небезпеки за недосяжні межі;
– знищити / ліквідувати джерело небезпеки;
– сховати або видозмінити ІС до невпізнання.

В даний час різним аспектам інформаційної боротьби (протиборства, дій, загрози війни) приділяється велика увага в ЗМІ та в наукових виданнях. Проведений аналіз дозволяє зробити висновок, що при спільності поглядів на інформаційну боротьбу існують різні підходи до визначення цілей, об’єктів дії, способів дії і засобів інформаційної боротьби [1, 2].

З погляду України джерелом інформаційних впливів, за їх походженням і внутрішній природі можна розділити на три категорії [1, 3, 4, 5].

До *першої категорії* відносяться джерела зовнішніх впливів:

– наявність інформаційних атак із зовні;

– зацікавленість у зміні інформаційних потоків як із зовні, так і внутрішніх;

– зацікавленість в ослабленні політичної, економічної і військової ролі України в регіоні, на континенті і в світі;

– підтримка і позитивне відношення до дій дестабілізуючих сил в Україні;

– зацікавленість в інформаційних ресурсах України, у встановленні контролю над її інформаційними ресурсами.

Друга категорія складає такі джерела:

– джерела, які утворюються об'єктивними зовнішніми умовами: діють або існують за межами України і не мають прямих ознак інформаційних впливів для України;

– стійке збільшення витрат на інформаційну боротьбу;

– внутрішня соціально-політична нестабільність.

До *третьої категорії* відносяться джерела внутрішнього походження, які так або інакше, впливають на рівень інформаційної небезпеки для України:

– незадовільний стан інформаційної безпеки;

– недостатнє фінансування з державного бюджету України на потреби інформаційної безпеки;

– прояв соціально-політичної і морально-психологічної кризи у відношенні до інформаційної боротьби.

Всі ці категорії впливу більшою чи меншою мірою діють на безпеку інформації в державі, а, отже, посилюють умови інформаційної боротьби.

Процес розробки теоретичних основ інформаційної боротьби і дій ускладнений тим, що до сьогоднішнього дня не існує однозначного визначення і всіма прийнятого поняття – «інформація». Закон України «Про інформацію» [6] визначає інформацію як документовані або такі, що публічно оповістили, відомості про події і явища, що відбуваються в суспільстві, державі і навколишньому середовищі. У той же час філософське визначення поняття «інформація» звучить, як система ідеальних (суб'єктивних) образів об'єктів, процесів і явищ

навколишнього світу в свідомості людини, а так само сукупність ознак, властивих матерії і формуючих ідеальних образів. Виходячи з наведених понять, можна зробити висновок, що вони не дозволяють розглядати «інформацію» як об’єкт впливу, що звужує сферу інформаційної боротьби і впливу.

Розглядаючи суб’єктно-об’єктні відносини, визначимо інформацію як об’єкт інформаційної боротьби, виділити області, в яких вона ведеться. Такий підхід забезпечує побудову системи загальних і приватних категорій інформаційної боротьби як виду боротьби, який характеризується властивими нею об’єктами і засобами дії, способами і формами їх застосування. Урахування загальних і окремих категорій інформаційної боротьби може бути подано у вигляді наступного підходу (рис. 1.2).

Розглянемо суть і зміст таких основних категорій інформаційної боротьби як інформація, інформаційні процеси, інформаційний ресурс. Детально зміст інформаційного впливу як основоположній категорії інформаційної боротьби було розглянуто в [2].

Поняття «інформація» є базовим для розуміння процесів, що протікають у ході інформаційної боротьби.

Обговорення проблеми інформації в сучасній науці ведеться в різних аспектах. З єдиного об'єкту пізнання – інформація – фахівці в різних областях знань вибирають «свій» аспект, який і є для них предметом пізнання. Так, фахівець в області теорії передачі інформації основну увагу приділяє кількісним характеристикам інформації, кодуванню, впливу шумів, перешкод тощо.

Об'єкт дослідження тут один – інформація. Але оскільки інформація вивчається різними галузями науки, що мають різні предмети, то і сама інформація представляється в різному «світлі», в ракурсі предмету тієї або іншої науки.

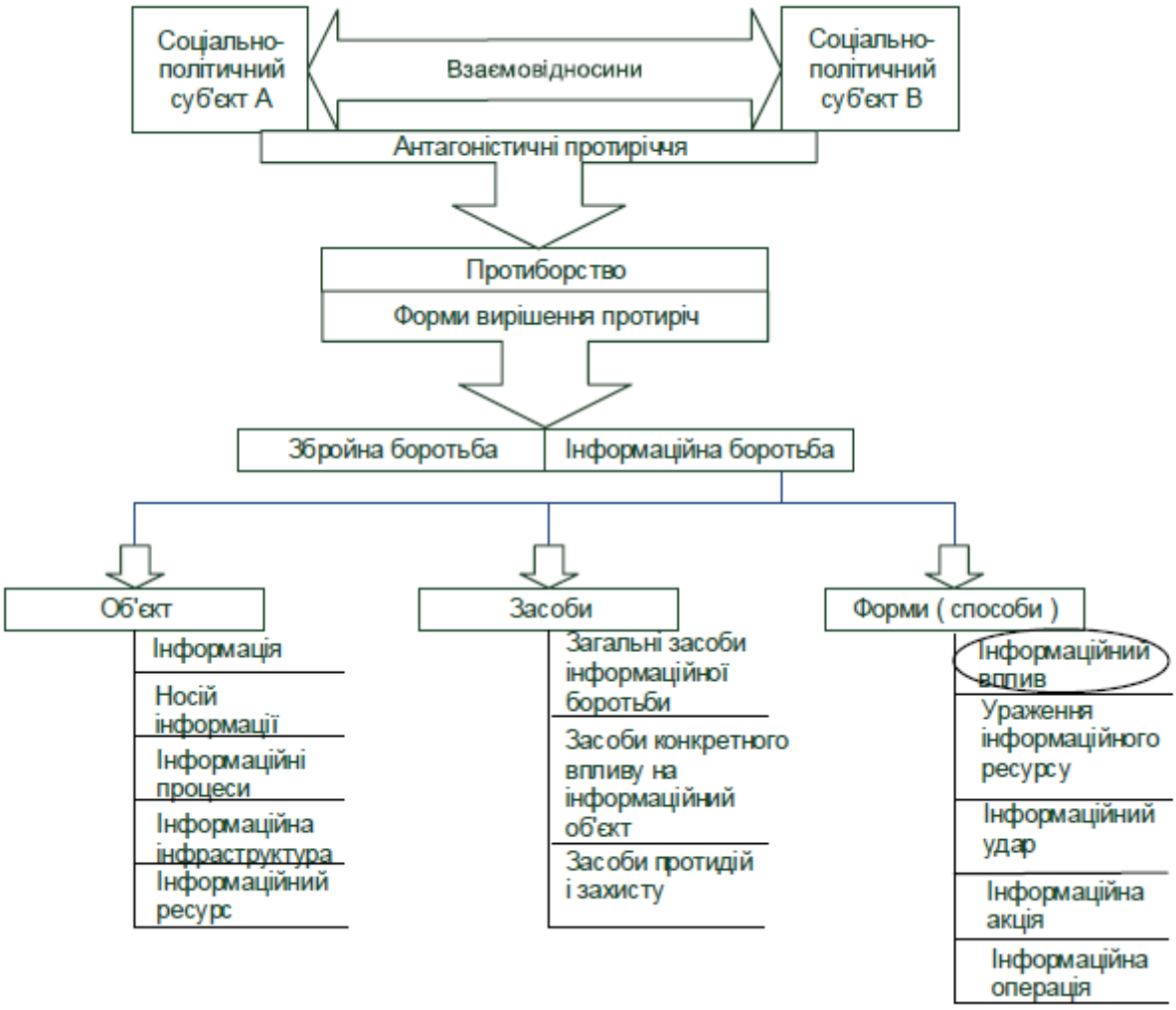

Рис. 1.2. Підхід до побудови загальних і окремих категорій інформаційної боротьби

Поняття інформації спочатку було пов'язане виключно з соціальною сферою, з комунікативною діяльністю людей. Цей висновок спирається на результат дослідження значень слова «інформація», яке вперше зародилося в латинській мові. У Російській імперії це слово вперше з'явилося в петровську епоху. Так, Н.А. Смірнов, вважає, що це слово перейшло у російську мову з польської «informacia», яка запозичила його у латинської. У той час слово інформація уживалося у сенсі «ідея, наука» [7].

Необхідно відзначити, що зараз поняття «інформація» в прямому розумінні – це сукупність образів і зв’язків між ними в рамках певної системи.

На підставі цього можна сформулювати друге непряме поняття терміну «інформація», яке свідчить, що інформація є множиною ознак, властивих об’єктам, процесам і явищам матеріального світу, які формують ідеальні (суб’єктивні) образи [2].

На підстав першого і другого непрямих понять інформації сформулюємо наступне визначення. Інформація є системою ідеальних (суб’єктивних) образів, об’єктів, процесів і явищ навколишнього світу в свідомості людини, а також множини ознак, властивих матерії і які формують ідеальні образи.

Запропоноване визначення в деякій мірі пояснюють ідеалістичний і матеріалістичний підходи до поняття «інформація», яка як множина образо утворюючих ознак є властивістю матерії і за своєю природою матеріальна, але як система ідеальних образів і зв’язків між ними – ідеальна за своїм змістом.

Саме таке розуміння інформації дозволяє визначити її джерела і носії, тобто виділити ті об’єкти, на які здійснюється дія в ході інформаційної війни (боротьби).

Носіями інформації енергетичні поля, потоки заряджених частинок, а також біохімічні процеси, комплекс яких об’єднаний загальною назвою «механізм електричної збудливості».

Джерелами інформації є самі об’єкти, процеси і (або) явища, що генерують (відображають, випромінюють) коливання і хвилі, а також випускають потоки заряджених частинок, і, звичайно, центральна нервова система (мозок) людини.

Визначення суті і природі інформації дозволяє зрозуміти природу і зміст інформаційних процесів, що є носіями інформації в часі і просторі. Зупинимося в першу чергу на елементарних інформаційних процесах, таких як отримання (сприйняття), переробка, передача і зберігання (накопичення) інформації, під якою розуміють [2]:

– отримання (сприйняття) – виокремлення розпізнаної інформації зі всієї різноманітності навколишнього світу;

– модифікація – зміна інформації, відповідно до раніше визначеного алгоритму. Мета модифікації інформації – отримання суб’єктивно нової інформації;

– передача – рух незмінної інформації в просторі і часі. При передачі інформації ознаки образів можуть змінюватися із збереженням смислового змісту;

– зберігання – передача інформації не в просторі, а в часі, тобто відворення образу (ознак) об'єкту в необхідний момент часу.

Сукупність елементарних інформаційних процесів утворюють такі їх види, як інформаційні ланцюги та інформаційні мережі.

У об'єктів натуральної неживої природи відображення здійснюється у вигляді віддзеркалення, а інформаційні процеси – зберігання внутрішньої різноманітності структури речовини.

Вищий рівень розвитку живих систем зумовив наявність у них всіх форм елементарних процесів: сприйняття, переробку, передачу і зберігання, а також деяких видів інформаційних процесів.

Високоорганізованій системі, якою є суспільство і сама людина, властиві всі форми і види інформаційних ресурсів.

В ієрархічній структурі матеріального світу техніка займає проміжне положення між неживою натуральною природою і суспільством і є частиною неживої штучної природи. Таке розташування обумовлене тим, що, розробляючи і створюючи різні технічні пристрої, людина перш за все прагнула удосконалювати свої технічні здібності і можливості по взаємодії з навколишнім світом.

Розглянемо зміст інформаційних процесів і поняття «інформаційний ресурс».

Інформаційним ресурсом є сукупність інформації та її носіїв, інформаційних технологій та інформаційної інфраструктури.

Отже, інформація має нерозривний зв'язок з джерелами інформації, які є початком відліку в реалізації інформаційних процесів.

Зміст інформаційної боротьби полягає у впливі цілеспрямованих інформаційних впливів на інформаційні ресурси. При цьому під інформаційним впливом слід розуміти процес або дію направлену на поразку або зменшення інформаційного ресурсу протиборчої сторони [1, 7].

На підставі сформульованого підходу до побудови загальних і приватних категорій інформаційної боротьби можна виділити напрями інформаційних

впливів і визначити їх суть. Встановлено [8, 9], що інформаційні впливи можуть бути навмисними і ненавмисними.

У ході інформаційної боротьби на інформаційний ресурс здійснюються навмисні інформаційні впливи, які по своєму характеру можуть бути активними і пасивними [8].

До активних відносяться такі інформаційні впливи, які призводять до зміни складу ознак, що визначають конкретний смисловий зміст, або порушення стійкості інформаційних процесів, а також до поразки зв'язків у системах образів.

При пасивних інформаційних впливах зміна складу ознак і порушення зв'язків у системі образів не відбувається.

Для реалізації дій в рамках виділених напрямів у ході інформаційної боротьби можна відзначити наступні види інформаційних впливів (рис. 1.4).

Рис. 1.3. Види інформаційних впливів

1.3. Аналіз сучасних методів моделювання інформаційних впливів

Розглянемо сучасні підходи до моделювання впливів на ІС – виділимо вхідні та вихідні дані кожного з критеріїв, основні операції, а також їх переваги та недоліки (табл. 1.1) [10].

Таблиця 1.1

Аналіз методів моделювання впливів на ІС

№	Назва	Вхідні дані	Вихідні дані	Основні операції	Переваги	Недоліки
1	Модель Мухіна-Волокіти	Статистична вибірка даних	Лічильник загроз впливу на інформацію	Експертні оцінки, теорія графів	Висока точність виявлення впливу	Потреба у статистичних даних, залежність від компетенції експертів
2	Модель Бела-Лападули та модель Біба	Множини об’єктів і суб’єктів, сторонні їх стани, запити	Рівень порушення цілісності	Теорія множин, булева алгебра	Простота реалізації, контроль цілісності	Врахування лише цілісності; можливість створення двосторонніх потоків інформації і як наслідок необхідне створення довірених потоків
3	Модель Хартсона (п’ятивимірна статична модель)	Ресурси системи та їх стани; користувачі та їх повноваження	Область безпеки системи	Декартів добуток множин	Можливість отримання кількісних оцінок	Абстрактна формалізація процесу нападу
4	Модель на основі нейронних оперет та ланцюгів Маркова	Статистичні дані для навчання нейромереж та задавання матриць	Виявлення вірусів, спаму та атак на WEB-сервери	Теорія нейронних мереж; теорія Маркова	Адаптивні виявлення нападу та захист інформації	Потреба у статистичному наборі даних для динамічного функціонування

№	Назва	Вхідні дані	Вихідні дані	Основні операції	Переваги	Недоліки
		ймовірностей переходів СЗІ				
5	Модель на основі мереж Петрі-Маркова	Інформаційні стани системи (більше 3-х)	Можливість реалізації загрози впливу на інформацію	Теорія мереж Петрі та теорія ланцюгів Маркова	Кількість оцінки з урахуванням часових параметрів	Складність розрахунків для практичної реалізації
6	Диференціально-ігрова однокритеріальна графова модель	Множина станів ІС	Оптимальна стратегія захисту інформації	Теорія графів, диференціально-ігрове моделювання	Дозволяє здійснити розподіл інформаційних ресурсів, що виділяють ви на захист інформації	Не відображає загальну динаміку впливу на інформацію
7	Диференціально-ігрові спектральні однокритеріальна графова модель	Множина станів ІС	Оптимальна стратегія та ціна гри (гарантований рівень захищеності)	Диференціально-ігрове моделювання	Низька обчислювальна складність, врахування нестаціонарності	Не точний покроковий процес впливу на інформацію
8	Диференціально-ігрова нетейлорівська модель	Інтенсивність потоку захисних і атакуючих дій	Траєкторія та ціна гри	Диференціальні перетворене нетейлорівського типу	Точний опис процесу нападу на інформацію	Висока обчислювальна складність, низький рівень науково-технічних досліджень
9	Гібридно диференціально-ігрова модель	Показники надійності та захищеності, ймовірності загроз, часові параметри	Оптимальний розподіл ресурсів захисту	Диференціально-ігрове моделювання	Врахування показника якісного функціонування СЗІ; висока точність навіть в умовах	Точність досягається лише в певному застосуванні (послідовно) математичних методів

№	Назва	Вхідні дані	Вихідні дані	Основні операції	Переваги	Недоліки
					невизначеності	
10	Непервна дискретна диференціально-ігрова модель	Скінчення множина станів системи	Оптимальний розподіл ресурсів захисту у режимі реального часу	Числово-аналітичне моделювання, диференціальні перетворення	Розширення діапазону моделювання впливу на інформацію; низька обчислювальна здатність	Не враховує усіх критеріїв (порівняно з багатокритеріальними моделями)
11	Багатокритеріальна диференціально-ігрова модель на основі інтегральної оптимальності	Стратегії протиборчих сторін, часові параметри	Оптимальні стратегії гравців, ціна гри (гарантований рівень захищеності)	Диференціально-ігрове моделювання; теорія підтримки прийняття рішень	Можливість захисту інформації в умовах конфлікту частинних критеріїв та несанкціонованого розподілу інформаційних ресурсів атакуючої сторони	Обмеження на частинні критерії якості
12	Багатокритеріальна диференціально-ігрова модель на основі нелінійної схеми компромісів	Інтенсивності потоків розподілу ресурсів протиборчих сторін, часові характеристики	Оптимальні стратегії протиборчих сторін	Диференціальні перетворене, теорія підтримки прийняття рішень	Простота реалізації, адаптивність до різних ситуацій	Значних недоліків не знайдено

Висновки до першого розділу:

Аналіз сучасних методів моделювання впливів на інформаційні системи дав можливість визначити найбільш ефективний підхід і використати його з метою оптимізації параметрів систем захисту.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ОЦІНКИ ЗАГРОЗ КІБЕРПРОСТОРУ

2.1. Узагальнена класифікація загроз

У загальному випадку під загрозою ІБ будемо розуміти дефініцію, сформульовану у підготовленому Проекті Концепції інформаційної безпеки України, а саме: “наявні та потенційно можливі явища і чинники, які створюють небезпеку життєво важливим інтересам людини і громадянина, суспільства та держави в інформаційній сфері” [15].

Закон України “Про основи національної безпеки України” визначає, що загрози національній безпеці України в інформаційній сфері зводяться до [16]:

- обмеження свободи слова і доступу до публічної інформації;
- поширення у ЗМІ культу насильства, жорстокості, порнографії;
- комп’ютерної злочинності та тероризму;
- розголошення інформації з обмеженим доступом;
- маніпулювання суспільною думкою.

Закон України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки” безпосередньо не визначає види загроз ІБД, але встановлює напрямки їх реалізації: “неповнота, невчасність та невірогідність інформації; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації” [17].

У Доктрині інформаційної безпеки України уточнено перелік актуальних загроз національним інтересам та національній безпеці України в інформаційній сфері в умовах збройної агресії Російської Федерації. Серед найважливіших загроз ІБД у документі виділено наступні [18]:

– спеціальні інформаційні операції з метою зниження обороноздатності держави, дестабілізації суспільно-політичної чи соціально-економічної ситуації, загострення міжетнічних та міжконфесійних конфліктів;

– спеціальні інформаційні операції проти України в інших державах;

– експансія та домінування держави-агресора в національному інформаційному просторі;

– низький рівень розвитку інформаційної інфраструктури держави;

– недостатня ефективність інформаційної політики держави, недосконалість нормативно-правового регулювання в інформаційній сфері, низький рівень медіа-культури;

– заклики до радикалізації суспільства тощо.

Запропонований експертною радою при Міністерстві інформаційної політики України (МІПУ) Проект Концепції інформаційної безпеки України [15] формулює засади функціонування СЗІБД. Даний документ, поряд з Доктриною, визначає множину загроз ІБД, які мали прояв у національному інформаційному просторі. Зазначені у Проекті Концепції загрози ІБД за сферою їх виникнення поділяються на комунікативні і технологічні (рис. 2.1).

Комунікативні загрози ІБД пов’язані з реалізацією потреб особи, суспільства і держави щодо створення, споживання, розповсюдження та розвитку національного стратегічного контенту. Технологічні загрози ІБД проявляються під час функціонування та забезпечення захисту кібернетичних, телекомунікаційних та інших автоматизованих систем, що формують матеріальну складову державного інформаційного простору [15].

Таким чином, в Україні, як і у всьому світі, прослідковується поступове збільшення кількості нових і доопрацьованих нормативно-правових документів у сфері ІБД, які закріплюють фундаментальні засади формування, захисту та сталого розвитку національного інформаційного простору. При цьому відмінність у способах визначення видів загроз ІБД пояснюється різними цілями систематизації та вибором ознак.

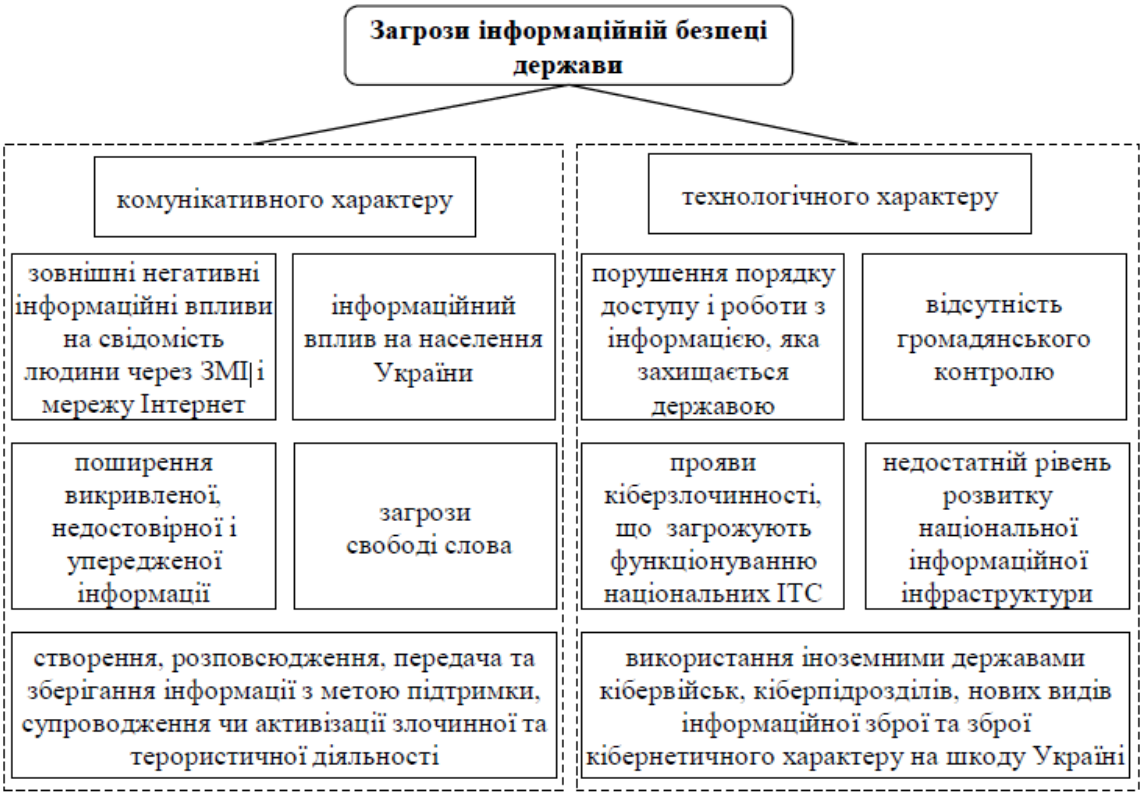

Рис. 2.1. Загрози ІБД відповідно до Проекту Концепції інформаційної безпеки України

Розглянемо існуючі наукові підходи до таксономії загроз ІБД з метою встановлення базових принципів і способів класифікації та їх подальшої адаптації для упорядкування загроз ІБД у ІС.

Професор В. А. Ліпкан у працях [19], [20] запропонував власний підхід до визначення загроз ІБД у розрізі загроз національній безпеці. Автор виділив групи класифікаційних ознак загроз ІБД, наведені на рис. 2.2.

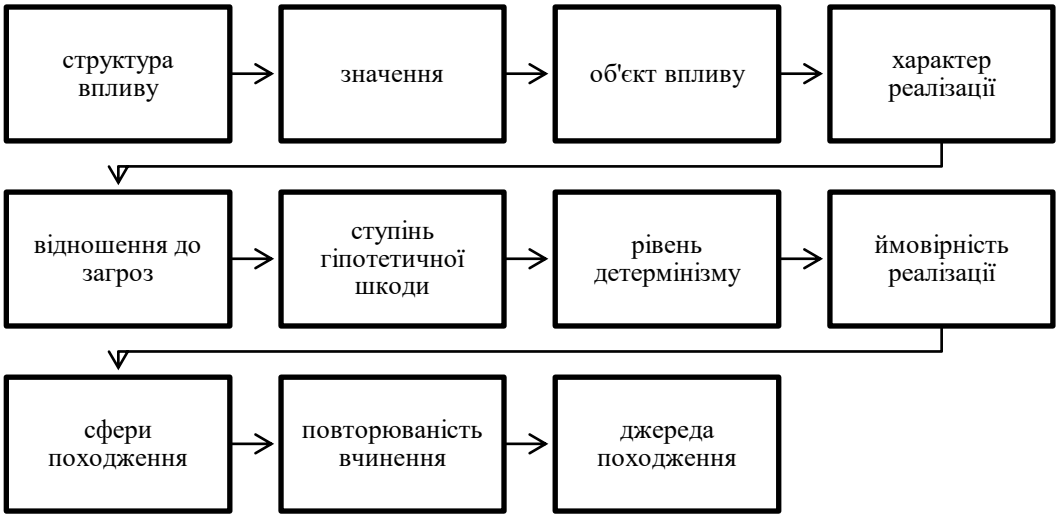

Рис. 2.2. Підхід до класифікації загроз ІБД професора В.А. Ліпкана

Перевагою такого підходу до класифікації є інтеграція з поняттями “інформаційна війна”, “інформаційне протиборство”, “інформаційний тероризм”, що є актуальним в умовах гібридної війни з Російською Федерацією. Однак, наведена систематизація не дозволяє однозначно ідентифікувати нові загрози ІБД, пов’язані з використанням новітніх інформаційних технологій для деструктивного впливу на акторів ІС.

Авторський колектив у складі В. Л. Бурячка, Р. В. Грищука та В. О. Хорошка у праці [21] сформулював підхід до класифікації загроз безпеці інформації у розрізі функціонування інформаційних систем (рис. 2.3).

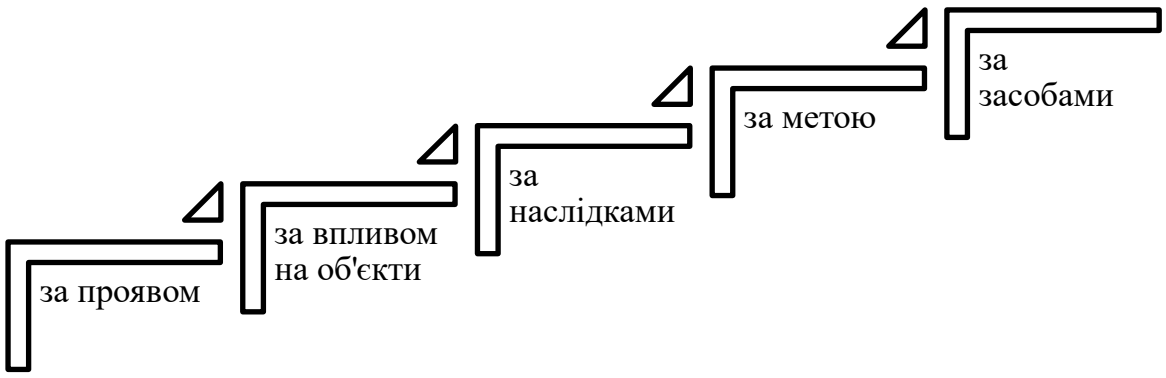

Рис. 2.3. Ознакова класифікація загроз безпеці інформації

Застосування такого підходу суттєво обмежує його використання для функціонування інформаційних систем завдяки акценту на технологічних схемах обробки інформації та врахуванню сучасних прийнятих концепцій архітектурної побудови інформаційних систем.

Серед вітчизняних вчених найбільш повна класифікація кібератак за ознаковим принципом належить професору О. Г. Корченку, яка може бути використана для забезпечення безпеки інформаційно-комунікаційних систем різного виду. До базових класифікаційних ознак кібератак автор відносить наведені на рис. 2.4 [22].

Розглянутий підхід до класифікації кібератак враховує їх технологічний характер, пов’язаний з особливостями функціонування інформаційно-комунікаційних систем і забезпеченням безпеки кібернетичного простору держави. Однак, така класифікація не може застосовуватися для опису загроз національним інтересам в інформаційному просторі.

Рис. 2.4. Класифікація кібератак за професором О. Г. Корченком

З огляду на особливості реалізації кібернетичних загроз та з урахуванням особливостей функціонування комп’ютерних систем (КС), розглянемо підхід, запропонований Грищуком Р. В. у монографії [13] (рис. 2.5).

Рис. 2.5. Класифікація кібернетичних загроз за Р. В. Грищуком

Перевагою такої класифікації (рис. 2.5) є врахування комплексного характеру загроз, що пояснюється використанням найбільш значущих для виявлення та інформаційної протидії ознак.

Зважаючи на різноманітність загроз національній безпеці в інформаційній сфері, доцільно використати фасетну систему класифікації за логічними ознаками, яка характеризується високою гнучкістю, можливістю необмеженого додавання числа фасетів і розбиття множини загроз за їх довільним сполученням. Встановлено такі основні ознаки класифікації загроз ІБД в ІС, які наведені на рис. 2.7 [14].

При аналізі класифікації інформаційних загроз, а також визначення інформаційної загрози, необхідно також мати визначення взаємно залежному з нею поняттю: атака. Атака, це наслідки загрози, що реалізована з встановленою (або невстановленою) ймовірністю. Отже, аналізуючи вище написане надамо визначення атаки на державні інформаційні ресурси. Атака на державні інформаційні ресурси – це дії щодо реалізації загрози державним інформаційним ресурсам, що сформовані на основі взаємодії джерела загрози через наявні фактори уразливості об’єкту інформаційної діяльності та такі, що приводять до різних видів збитків державі.

Дії щодо поширення в інформаційному просторі викривленої, недостовірної та упередженої інформації або негативні інформаційні впливи на суспільну

свідомість в ІП відносяться до порушення цілісності інформації. Однак, слід сказати, що фактично цілісність інформації не змінюється, а змінюється відношення до інформації. Тобто відбувається вплив на достовірність інформації.

В результаті ІДР підлягають інформаційному ризику. Зазвичай при дослідженні ризиків не надається увага оцінці якості інформації, за допомогою якої оцінюється ризик. Складові оцінки якості інформації наступні:

– достовірність інформації – міра наближеності інформації до першоджерела;

– об'єктивність інформації – міра віддзеркалення інформацією реальності;

– однозначність;

– порядок інформації – кількість передавальних ланок між першоджерелом і кінцевим користувачем;

– повнота інформації – віддзеркалення вичерпного характеру відповідності одержаних відомостей цілям збору;

– корельованість – ступінь відповідності інформації поставленому завданню;

– актуальність інформації (значущість) – важливість інформації;

– вартість інформації.

До факторів інформаційного ризику слід віднести:

– неповну або недостовірну інформацію у ЗМІ;

– надмірний обсяг і хаотичність інформації, яка циркулює в суспільстві;

– штучне або природне перекручування інформації в процесі її відбору для аналізу й використання у ході прийняття відповідальних державних рішень;

– технологічні помилки щодо введення, збереження й обробки даних в інформаційних системах.

Основними об'єктами інформаційних загроз в ІП:

– спільні інтереси великих мас громадян (соціальних груп або національних утворень, населення країни в цілому), які можна назвати груповими асоціаціями;

– культурні, духовні й моральні цінності, які сповідуються груповими асоціаціями.

2.2. Формалізація проблеми оптимізації систем захисту кіберпростору від інформаційних впливів

Приймаючи до уваги узагальнену модель процесу захисту інформації та її цільову функцію, можливо здійснити спробу знаходження оптимальних параметрів систем захисту – характеристик системи ТЗІ, наприклад, в розумінні максимальної шкоди. Яка попереджається, завдяки застосуванню системи захисту.

На рис. 2.6 умовно представлені інформаційні ресурси системи спеціального призначення (ССП), які потрібно захистити від природних та штучних впливів. Під природними впливами розуміються потоки будь-яких подій, які здатні тимчасово вивести ССП зі строю (збій, для якого характерно самоусунення) або на тривалий термін (збій, усунення якого потребує вторгнення персоналу), тобто потоки відмов. Причинами таких впливів можуть бути недостатня здатність первинних технічних засобів попередити дію таких впливів; недостатня надійність засобів ССП. Такі події впливають як безпосередньо на інформаційні ресурси ССП, так і на засоби технічного захисту цієї системи. При цьому стійкість ССП до природних впливів визначається такою її властивістю як надійність та забезпечується відповідними заходами (резервування, застосування елементів підвищеної надійності та ін.). для боротьби зі збоями, котрі призводять до порушення цілісності програмних засобів та інформації, що обробляється, можливо застосовувати засоби контролю й відновлення цілісності чи інші засоби відновлення ССП після збоїв.

Під штучними впливами розуміються ті події, котрі є результатом діяльності користувачів, як авторизованих, так і неавторизованих по відношенню до ресурсів ССП, що є, по якимось причинам, забороненим для даних користувачів. Такі впливи прийнято називати спробами несанкціонованого доступу (НСД), та вони можуть бути випадковими (в результаті помилки користувача) чи зловмисники, тобто спеціальними, з метою використання чи то ресурсів, чи то інформації ССП [11, 12].

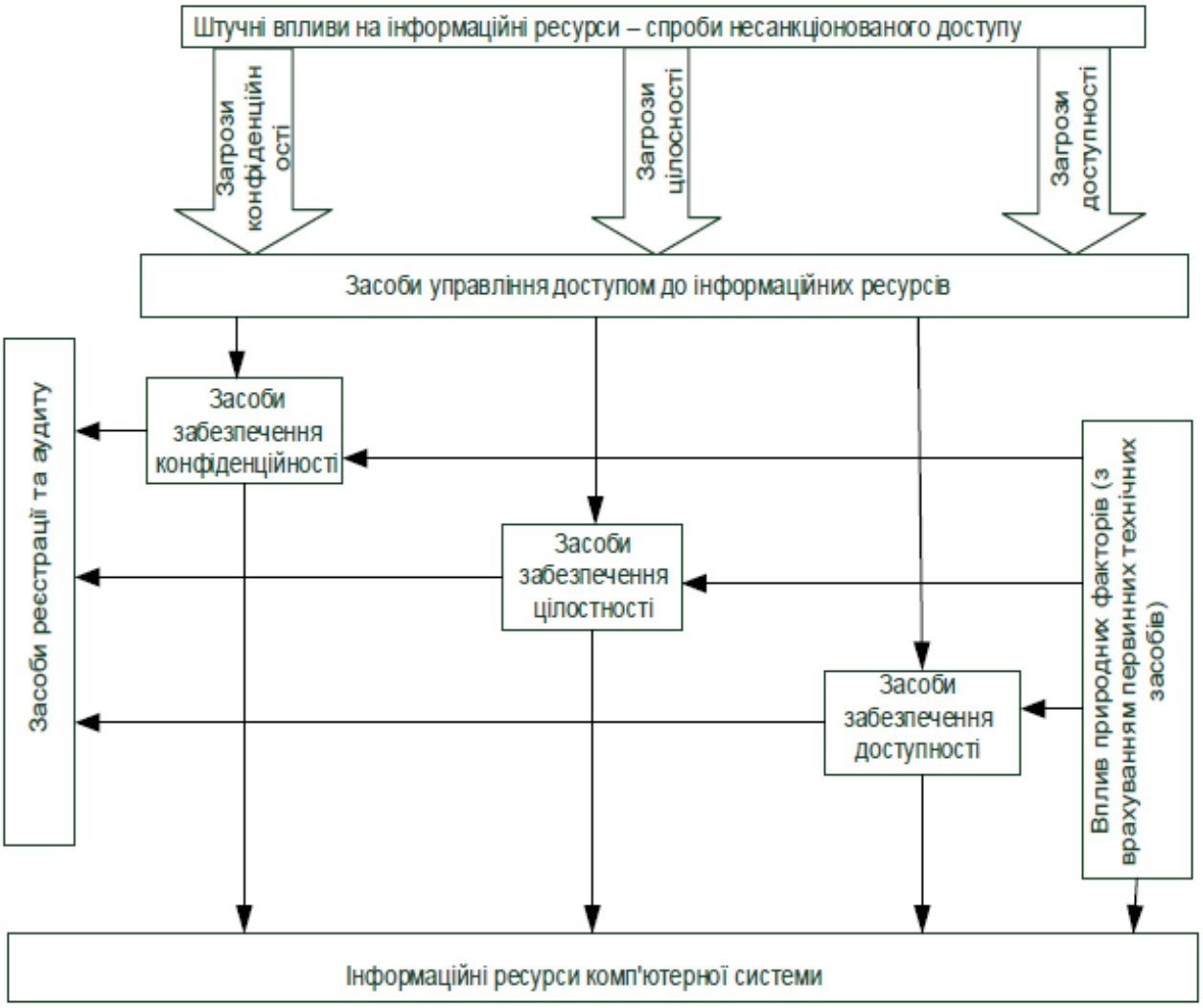

Рис. 2.6. Модель взаємодії засобів в процесі технічного захисту інформації

Спроби НСД можуть подіяти на ССП лише після подолання засобів управління доступом та відповідних засобів забезпечення тієї чи іншої функціональної послуги.

Таким чином, на інформаційні ресурси ССП можуть впливати як спроби несанкціонованого доступу, за умови подолання системи управління доступом, так і безпосередньо природні впливи [13, 14].

2.3. Метод оцінювання загроз інформації в кіберпросторі

Зважаючи на високі темпи розвитку інформаційних технологій загрози ІБД в ІП перетворилися на слабоформалізовані сутності, суттєво відрізняються між собою за ознаками і проявами у віртуальних спільнотах. Тому формування остаточних висновків про проведення в ІП інформаційних операцій можливе виключно за умови виявлення організаційних ознак загроз ІБД щодо використання суб'єктами ботів з подальшим детектуванням прихованих інформаційних впливів на систему в інформаційній системі. Після цього на основі інформаційної ентропії визначається інтегральний показник загрози ІБД для виявлення інформаційного впливу на користувачів і детектування маніпуляцій їх суспільною думкою.

Виявлення користувачів, які використовуються суб'єктами впливу для маніпулювання поведінкою аудиторії інформаційної системи, проводиться на основі побудови профілю інформаційної безпеки з подальшим віднесенням до визначеного класу загроз. Формування узагальненого висновку про рівень загрози ІБД у ІС створює передумови для підвищення ефективності заходів з інформаційної протидії. Тому метод оцінювання загроз ІБД у ІС є актуальним.

Аналіз останніх досліджень і публікацій [13], [15] показав відсутність загальноприйнятої методики оцінювання рівня загроз ІБД у ІС. Міжнародний досвід європейських країн [13], зокрема Латвії, Естонії, Німеччини, Італії, Польщі та інших продемонстрував, що провідна роль у виявленні та протидії загрозам ІБД належить об'єднаному центру передових технологій з кібероборони НАТО (NATO Cooperative Cyber Defence Centre of Excellence) із штаб-квартирою у Талліні (Естонія). Також у рамках проекту Академії електронного управління (eGA) Естонії використовується глобальний індекс National Cyber Security Index (NCSI), який оцінює готовність країн запобігти реалізації основних загроз та управляти інцидентами, злочинами і великомасштабними кризами. NCSI представляє собою інструмент для оцінки потенціалу інформаційної безпеки і заходів захисту інформаційного простору.

Індекс NCSI формується для окремих країн на основі таких даних:

а) загальний показник ІБ;

б) базові показники ІБ;

в) показники управління інцидентами і кризами;

г) показники міжнародного впливу.

Складність застосування індексу NCSI для вирішення проблеми оцінювання загроз ІБД у ІС полягає у відсутності докладної методології оцінювання у відкритому доступі, неможливості її окремого виділення і використання із сукупності інших інтегральних показників.

У загальному випадку для оцінювання загроз використовують дві групи методів: кількісні та якісні [15]. Суть кількісних методів зводиться до розрахунку показників ймовірності реалізації загроз на основі апріорної або апостеріорної інформації про їх прояви. Апостеріорні методи ґрунтуються на побудові гістограм розподілу проявів ознак загроз і частот їх реалізації, а група апріорних методів полягає в розрахунку статистичних характеристик процесів, які супроводжують реалізацію таких загроз. Недоліком такого підходу є обмеженість застосування для оцінювання загроз інформаційній безпеці держави у ІС, пов’язана зі складністю збору необхідного об’єму статистичних даних і формалізації ознак інформаційних акцій.

Якісне оцінювання рівня загроз ІБД ґрунтується на експертних методах [15] і зводиться до узагальнення та статистичної обробки думок кваліфікованих спеціалістів цієї галузі. Однак, застосування експертного оцінювання в задачах виявлення загроз суттєво обмежується необхідністю обробки великих масивів вхідних даних, низькою швидкодією процедури оцінювання, потребою підготовки великої кількості висококваліфікованих експертів, суб’єктивністю експертних оцінок тощо. Дослідження джерел і галузевих звітів [13], [15] свідчать про різке зростання кількості загроз ІБД у ІС, а поява протиріччя між рівнем сучасних загроз й науковим базисом їх оцінювання додатково актуалізує обраний напрямок наукових досліджень.

Ефективність виявлення загроз у ІС відповідною СЗІБД досягається завдяки врахуванню прояву ознак інформаційних операцій. Залежно від принципів багатокритерійної оптимізації виділяють наступні групи методів [16]:

1) оптимізації ієрархічної послідовності критеріїв якості;

2) визначення множини непокращуваних рішень;

3) на основі компромісу.

Серед недоліків перших двох груп методів слід відмітити складність визначення структури ієрархічної послідовності частинних критеріїв, суттєву обмеженість непокращуваних рішень областю компромісів тощо. У свою чергу, використання принципу справедливого компромісу, покладеного в основу третьої групи методів, забезпечує зниження якості за одними критеріями, яке не перевершує підвищення якості за іншими критеріями. Тому використання методів на основі компромісу для виявлення загроз у ІС є перспективним напрямком досліджень. Встановлено, що серед третьої групи методів нелінійна схема компромісів, запропонована професором А. М. Вороніним, забезпечує компроміс між частинними критеріями, а отримане рішення є оптимальним за Парето [16], [17]. Серед переваг даного методу виділяють обчислювальну простоту; унімодальність скалярної згортки, що забезпечує одно екстремальність задачі; адаптацію до умов прийняття рішення.

Отже, запропонований метод оцінювання загроз ІБД у ІС [18] ґрунтується на нелінійній схемі компромісів [17], [19] і зводиться до такого.

Етап 1. Розрахунок показника I_1 ознак інформаційних операцій у ІС. Метод [14] зводиться до пошуку дублікатів публікацій і коментарів у ІС, розрахунку показника читабельності текстового контенту та ведення діалогу з акторами, які є авторами такого контенту. Висновок про цілеспрямовану інформаційну операцію у ІС, направлену проти ІБ особистості, суспільства, держави з використанням спеціального програмного забезпечення формується на основі відповідного узагальненого показника 1 I , який приймає значення

$$I_1 = \begin{cases} 1, \text{якщо загроза існує;} \\ 0, \text{якщо загрози не існує.} \end{cases} \quad (2.1)$$

Етап 2. Визначення показника I_2 наявності інформаційного впливу на акторів у контенті ІС. Виявлення таких прихованих інформаційних впливів полягає в інтелектуальному пошуку текстового контенту ІС відповідно до заданого семантичного ядра за критерієм актуальності, критичності та рівня обговорення у суспільстві [22]. Відібраний контент підлягає семантичному аналізу на основі онтологій з використанням сигнатурного методу і методу виявлення аномалій. У результаті з використанням методу, описаного у п. 3.2, формується відповідний показник I_2

$$I_2 = \begin{cases} 1, \text{якщо загроза існує;} \\ 0, \text{якщо загрози не існує.} \end{cases} \quad (2.2)$$

Етап 3. Оцінювання прояву I_3 маніпуляцій суспільною думкою у ІС. Розрахунок показника I_3 проводиться відповідно до розробленого методу виявлення інформаційного впливу на користувачів у ІС [20]. Узагальнення частинних ознак маніпуляцій виконано на основі інтегрального показника інформаційної ентропії H_n контенту ІС, тобто встановлення рівня невизначеності щодо використання технологій прихованого впливу на акторів. Зростання величини інформаційної ентропії H_n характеризує зменшення невизначеності, тому для задачі оцінювання прояву ознак маніпуляцій суспільною думкою показник I_3 набуває значень

$$I_3 = 1 - H_n, H_n \in [0; 1] \quad (2.3)$$

Етап 4. Оцінювання профілю інформаційної безпеки актора I_4 . Розрахунок показника 4 І реалізований з використанням методу побудови профілів ІБ акторів [11]. Запропонований метод ґрунтується на технологіях інтелектуального аналізу даних, зокрема методах машинного навчання з учителем. Оцінка профілю інформаційної безпеки I_4 приймає значення у заданому діапазоні

$$I_4 \in [0;1] \tag{2.4}$$

Узагальнення загроз ІБД у ІС I_j , $j = \overline{1,4}$ та їх нормованих шкал оцінки подано в табл. 2.1.

Етап 5. Встановлення вагових коефіцієнтів α_j ознак загроз ІБД у ІС. Значення вагових коефіцієнтів встановлюються експертами на основі їх індивідуальних переваг і відповідають оперативній ситуації у ІС.

Вагові коефіцієнти ознак загроз ІБД у ІС визначаються на симплексі [19]

$$\alpha_j \in \Gamma_\alpha, \Gamma_\alpha = \left\{ \alpha_j \geq 0, \sum_{j=1}^{m} \alpha_j = 1 \right\}, j \in [1;m] \tag{2.5}$$

Таблиця 2.1

Шкала оцінювання загроз ІБ у ІС

Прояв загроз	Шкала оцінки	Якісний показник рівня загрози
Організаційні ознаки загроз I_1	0	Відсутня
	1	Існує
Загрози у змісті текстового контенту I_2	0	Відсутня
	1	Існує
Прояв маніпуляцій I_3	0,91-1,00	Дуже висока
	0,75-0,90	Висока
	0,50-0,74	Значна
	0,21-0,49	Низька
	0,00-0,20	Дуже низька
Оцінка профілю ІБ користувача I_4	0,70-1,00	Дуже високий
	0,50-0,70	Високий
	0,40-0,50	Значний
	0,20-0,40	Допустимий
	0,00-0,20	Низький

Етап 6. Скалярна згортка показників загроз І по нелінійній схемі компромісів. Багатокритерійна задача оцінки зводиться до моделі векторної оптимізації з різними ваговими коефіцієнтами ознак загроз ІБД у ІС [27].

$$I^* = \arg\min_{I \in M} \sum_{j=1}^{m} \alpha_j \left(1 - I_j\right)^{-1} \tag{2.6}$$

Для якісної оцінки загроз проводиться нормування скалярної згортки (2.6) до мінімального значення [12]

$$I = 1 - \frac{1}{I^*} \tag{2.7}$$

Отримане значення ставиться у відповідність якісній шкалі загроз (табл. 2.2), сформованій на основі оберненої нормованої фундаментальної шкали, запропонованої професором А. М. Вороніним [17].

Таблиця 2.2

Якісна шкала рівнів загроз

Рівень загрози	Інтервальні значення шкали оцінок
Існує	0,71-1,00
Вищий середнього	0,51-0,70
Нижчий середнього	0,31-0,50
Відсутній	0,00-0,30

У результаті моніторингу інформаційного простору ІС з метою оцінювання загроз ІБД відбирається текстовий контент і дані акторів, які його поширюють. Такий текстовий контент досліджується на предмет наявності ознак проведення інформаційної операції, деструктивного інформаційного впливу на акторів, маніпуляцій суспільною думкою. На основі відібраних акаунтів акторів у ІС проводиться оцінювання їх профілів ІБ.

Експерт після аналізу предметної області оцінює пріоритетність ознак загроз ІБД, на основі яких розраховуються значення вагових коефіцієнтів α_j . Сформований вектор ознак загроз I_j використовується для скалярної згортки по нелінійній схемі компромісів. На заключному етапі виконується перехід від числових значень I до якісної шкали оцінок рівня загроз ІБД у ІС. Отримані оцінки

використовуються для вироблення рекомендацій щодо переходу інформаційної системи до бажаного стану ІБ в ІП.

Отже, розглянутий метод оцінювання загроз ІБД у ІС, який опирається на нелінійну схему компромісів і забезпечує підвищення ступеня обґрунтованості управлінських рішень та ефективність заходів інформаційної протидії загрозам.

Висновки з другого розділу:

Досліджено класифікацію загроз ІС, яка реалізує віднесення виявлення об’єктів з множини небезпек до попередньо встановлених класів.

Досліджено метод оцінювання загроз ІБД у СІС, який ґрунтується на нелінійній схемі компромісів і відрізняється від відомих врахуванням ознак використання соціальних ботів для проведення інформаційних операцій, інформаційних впливів на акторів за змістом текстового контенту, інформаційно-психологічного впливу і профілів ІБ акторів у СІС. Завдяки узагальненому показнику рівня загроз ІБД метод дозволяє обґрунтувати вибір ефективних заходів з інформаційної протидії для нейтралізації виявлених загроз та забезпечення заданого рівня ІБД у СІС.

3 ОПТИМІЗАЦІЯ ЗАХИСТУ КІБЕРПРОСТОРУ ТА ВИЯВЛЕННЯ ОЗНАК ІНФОРМАЦІЙНИХ ВПЛИВІВ

3.1. Технології моделювання критеріїв оптимальності та обмеження загроз інформації

Для створення інформаційної системи та системи захисту інформації процедура аналізу ефективності та оптимальності рішень повинна містити обов'язкові етапи:

– визначення практичної потреби;

– вибір цілей та формування вимог до інформаційної системи, яка забезпечує досягнення поставлених цілей;

– визначення зовнішніх умов функціонування системи;

– визначення систем, з якими буде взаємодіяти створена система;

– вибір критеріїв оптимальності системи та побудова її математичних моделей;

– вибір та аналіз можливих способів вирішення поставлених задач;

– виявлення та дослідження ресурсів та правил на їх використання;

– розробка математичних моделей обмежень як функцій від керованих та некерованих змінних;

– порівняння аналогів, пошук та вибір оптимального рішення;

– аналіз адекватності та чуттєвості математичних моделей, критеріїв та обмежень до змін керованих змінних параметрів.

Сучасні СІС являють собою складні ієрархічні багаторівневі системи [22]. Основними характеристиками таких систем є вертикальна та горизонтальна декомпозиція на самостійні підсистеми, які мають свої цілі, критерії та органи керування, пріоритет прийняття рішень, залежність рішень, що приймаються на інших рівнях та в інших підсистемах, необхідність узгодження критеріїв та рішень,

координації виконання рішень та дій. Процес керування критеріями та рішеннями підсистем здійснюється в умовах невизначеності, яка обумовлена неповною інформацією про поведінку інших підсистем, а також про їхнє зовнішнє оточення [23].

При виборі критеріїв та обмежень в ієрархічних системах можливі наступні проблемні ситуації:

– одноріневий вибір критеріїв при наявності однієї мети;

– одноріневий багатоцільовий вибір критеріїв;

– багаторівневий вибір критеріїв при умові, що кожний рівень керується однією метою;

– багаторівневий багатоцільовий процес формування критеріїв.

Відповідно, побудова математичних моделей критеріїв ефективності та обмежень є ключовою проблемою в усіх задачах аналізу та синтезу, оптимізації систем, що розробляються, тому побудова процедур формалізації критеріїв та обмежень само по собі є важливою актуальною проблемою [24-26].

Тобто необхідні розробка та застосування системи правил для математичного моделювання критеріїв оптимальності та обмежень як певних функцій від керованих, так й некерованих змінних. Формалізація побудови математичних моделей дозволяє змістовно ставити та вирішувати задачі аналізу, синтезу та оптимізації систем за обраними критеріями та виявленим обмеженням. Некеровані змінні, як правило, відіграють роль параметрів родини рішень та визначають зазвичай ті чи інші умоаи функціонування та взаємодії систем та/або області існування та єдності оптимальних рішень.

Тому потрібно сформулювати систему правил, для чого використовуються три основних принципи:

1. Критерії ефективності повинні дозволяти оптимальне керування, тобто готувати та приймати оптимальні рішення.

2. Так як в задачах оптимізації обмеження відіграють роль критеріїв, то математичні моделі обмежень конструюють також й моделі критеріїв.

3. Будь-яка задача з обмеженнями може бути перетворена у послідовність задач без обмежень будується на необхідних та достовірних умовах існування екстремумів функцій та функціоналів. Вона дозволяє розробляти канонічні форми рівнянь оптимізації, як рівнянь балансу [27, 26], критеріїв оптимізації та обмежень, як інтегральних перетворень цих канонічних форм.

Розглянемо послідовно та детально запропоновану систему правил.

Правило оптимальності. Будь-яка безперервна двічі диференційована функція $OC(cv_1,\dots,cv_e)$ від e аргументів може бути критерієм оптимальності ОС цільової функції, а самі аргументи є керованими змінними cv, якщо для області існування ОС дотримуються необхідні та достатні умови існування екстремумів.

Правило обмеження. Будь-яка безперервна двічі диференційована функція $L(cv_1,\dots,cv_e)$ від e незалежних аргументів може бути обмеженням, а самі аргументи є керованими змінними, якщо для області існування L дотримуються необхідні та достатні умови існування екстремумів та задані обмеження у вигляді:

$$L_1(cv_1,\dots,cv_e) = L_1^*,\dots,L_\mu(cv_1,\dots,cv_e) = L_\mu^*; \qquad (3.1)$$

де μ - число обмежень.

Правило існування. Для того, щоб оптимальне рішення існувало та було єдиними, необхідно щоб число керованих змінних та число обмежень задовольняли умові:

$$e > \mu. \qquad (3.2)$$

Правило зведення. У випадках, коли обмеження (3.1) задані у вигляді нерівностей, оптимізація зводиться до відомих способів введення фіктивних допоміжних змінних. Якщо цільові функції та обмеження можуть мінятися місцями, то в задачах оптимізації повинна виконуватися необхідна умова (3.2).

Правило допоміжної функції. У задачах оптимізації з обмеженнями за критерій оптимізації використовується допоміжна функція Лагранжа виду:

$$AL(cv_1, \dots, cv_e) = OC(cv_1, \dots, cv_e) + (\lambda_1[L_1(cv_1, \dots, cv_e) - L_1^*] + \cdots + \lambda_\mu[L_\mu(cv_1, \dots, cv_e) - L_\mu^*]), \quad (3.3)$$

де λ_κ – допоміжні невизначені множники Лагранжа, $k = \overline{1, \mu}$.

Правило канонічності. Система з $e + \mu$ рівнянь оптимізації:

$$\begin{cases} \dfrac{\partial AL(cv_1, \lambda_1)}{\partial cv_1} = 0, \dots, \dfrac{\partial AL(cv_e, \lambda_e)}{\partial cv_e} = 0 \\ \dfrac{\partial AL(cv_1, \lambda_1)}{\partial cv_1} = 0, \dots, \dfrac{\partial AL(cv_\mu, \lambda_\mu)}{\partial cv_\mu} = 0, \end{cases} \quad (3.4)$$

може бути подана у канонічній формі виду

$$\begin{cases} \dfrac{\partial AL_1(cv_1, \lambda_1)}{\partial cv_1} = \dfrac{\partial AL_2(cv_1, \lambda_1)}{\partial cv_1}, \dots, \dfrac{\partial AL_1(cv_e, \lambda_e)}{\partial cv_e} = \dfrac{\partial AL_2(cv_e, \lambda_e)}{\partial cv_e} \\ L_1(cv_1, \dots, cv_e) = L_1^*, \dots, L_\mu(cv_1, \dots, cv_e) = L_\mu^*. \end{cases} \quad (3.5)$$

Таким чином систему (3.5) будемо називати першою канонічною формою представлення системи рівнянь оптимізації. Елементи обох частини рівнянь (3.5) будемо називати типовими елементами першої канонічної форми.

Правило критеріїв. Використання першої канонічної форми (3.5) системи рівнянь оптимізації дозволяє створювати критерії оптимізації у вигляді сепарабельних адитивних критеріїв:

$$OC(cv_1, \dots, cv_e) = \sum_{i=0}^{e} (\int \frac{\partial AL_1(cv_1, \dots, cv_e; \lambda_1, \dots, \lambda_\mu)}{\partial cv_i} \partial cv_i - \int \frac{\partial AL_2(cv_1, \dots, cv_e; \lambda_1, \dots, \lambda_\mu)}{\partial cv_i} \partial cv_i), \quad (3.6)$$

Сепарабельність $OC(cv_1, \dots, cv_e)$ означає, що всі недіагональні елементи матриці других часткових похідних цієї функції дорівнюють нулю.

Правило сепарабельного програмування. Сепарабельну форму та адитивність також зручно використовувати для обмежень виду (3.5):

$$OC_{1k}(cv_1) + \dots + OC_{ek}(cv_e) = OC_k^*; \tag{3.7}$$

Задачу оптимізації, у якій критерій оптимізації представлений у вигляді (3.6), а обмеження у вигляді (3.7), будемо називати задачею сепарабельного програмування. Якщо $OC(cv_1, \dots, cv_e)$ є випуклою функцією, а $L_k(cv_1, \dots, cv_e)$ – угнутою, існує рішення прямих задач сепарабельного програмування. Для зворотних задач функції $OC(cv_1, \dots, cv_e)$ та $L_k(cv_1, \dots, cv_e)$ повинні володіти протилежними властивостями. Властивості сепарабельності та адитивності дозволяють створювати ефективні обчислювальні алгоритми пошуку оптимальних рішень. Представлення критерію оптимізації у вигляді (3.6) називається другою канонічною формою постановки задачі оптимізації. У задачах оптимізації при побудові допоміжних функцій Лагранжа (3.3) критерій та одне з обмежень міняються місцями. При цьому змінюється і характер екстремуму, і вимоги випуклості та вгнутості цільових функцій та обмежень. Доданки суми будемо називати типовими елементами другої канонічної форми.

Запропонована система правил дозволяє створити загальну теорію математичного моделювання сепарабельних критеріїв оптимізації та обмежень. Вони засновані на виборі типових елементів канонічних форм (3.5), (3.6) та методах сепарабельного програмування. Параметри канонічних форм грають роль параметрів сімейтсва оптимальних рішень, їх зручно використовувати як параметри середовища (зовнішнього оточення) або як параметри, які характеризують взаємодію системи, що розглядається з іншими системами.

Для класифікації типових елементів першої канонічної форми (3.5) корисно використовувати методи аналітичної та диференційної геометрії, які володіють високою наочністю. У ролі типових елементів форм можуть бути обрані

алгебраїчні функції (поліноми) q-го порядку, показові, експоненціальні, тригонометричні, трансцендентні та інші.

Виходячи з цього, розглянемо випадок, коли *e=1, μ=0*. Це означає, що в ролі критерія оптимальності обирається функція однієї керуючої змінної, а обмеження відсутні. Припустимо, що перший типовий елемент $OC_1'(cv)$ є поліномом нульового порядку:

$$OC_1'(cv, a_{10}) = a_{10}, \tag{3.8}$$

а другий типовий елемент $OC_2'(cv, a_{21}, a_{20})$ є поліномом першого порядку:

$$OC_2'(cv, a_{20}) = a_{21}cv + a_{20}. \tag{3.9}$$

Покажемо вид канонічної форми (3.5) рівняння оптимізації, вид канонічної форми (3.6) критерія оптимальності. Побудуємо математичну модель критерія, тобто знайдемо оптимальне значення cv_{opt} керуючої змінної та екстремальне значення критерію. Дослідимо вид екстремума в залежності від параметрів a_{10}, a_{20}, a_{21} типових елементів форми (3.5).

У відповідності з (3.5) рівняння оптимізації має вигляд:

$$a_{10} = a_{20} + a_{21}cv. \tag{3.10}$$

Розв’язуючи це рівняння відносно *x*, отримаємо оптимальне значення керуючої змінної

$$cv_{opt} = \frac{a_{10} - a_{20}}{a_{21}}. \tag{3.11}$$

За допомогою другої канонічної форми (3.6) визначимо математичну модель критерія:

$$OC(a_{10}, a_{20}, a_{21}, cv) = a_{10}cv + c_{11} - a_{20}cv - \frac{cv^2}{2} - c_{21} = \\ = -a_{21}\frac{cv^2}{2} - (a_{20} - a_{10})cv - (c_{21} - c_{11}). \quad (3.12)$$

З аналізу виразу (3.12) витікає, що друга канонічна форма (3.6) критерія є поліномом другого порядку, екстремуми якого визначають параметри першої канонічної форми (3.5). таким чином, якщо перша канонічна форма є лінійною і містить поєднання поліномів нульового та першого порядків, то друга канонічна форма (3.6) для критерія оптимальності є поліномом другого порідку. Отже, перші канонічні форми (3.12) породжують клас задач квадратичного програмування.

Лінійна апроксимація перших канонічних форм рівнянь оптимізації володіє відносно широкими можливостями для моделювання задач лінійного та нелінійного програмування. В цьому випадку лінійна канонічна форма включає чотири параметри: $a_{10}, a_{11}, a_{20}, a_{21}$ та дозволяє апроксимувати чимало класів критеріїв (середньоквадратичні критерії, критерії максимальної правдоподібності тощо) варіацією поєднань цих параметрів як морфологічних параметрів форми.

Визначимо екстремальні значення критерія оптимальності (3.12) при $cv = cv_{opt}$ (3.11). Підставимо значення cv_{opt} з (3.11) до (3.12) та отримаємо:

$$OC_{ext}(a_{10}, a_{11}, a_{21}, cv_{opt}) = -a_{21}\frac{(a_{10} - a_{20})^2}{2a_{21}^2} + \\ + \frac{(a_{10} - a_{20})^2}{a_{21}} - (c_{21} - c_{11}) = \frac{(a_{10} - a_{20})^2}{2a_{21}^2} - (c_{21} - c_{11}) \quad (3.13)$$

Для уточнення виду екстремуму виконаємо диференціювання ПФК за керованою *x*, отримаємо значення другої похідної критерію:

$$OC''(cv) = a_{21}. \quad (3.14)$$

Отже, значення параметру a_{21} ПКФ (3.5) визначає вид екстремуму. Якщо $a_{21} > 0$, тоді екстремум є мінімумом:

$$OC_{ext}(a_{10}, a_{11}, a_{21}, cv_{opt}) = OC_{min}(a_{10}, a_{11}, a_{21}, cv_{opt}). \quad (3.15)$$

Якщо $a_{21} < 0$, тоді екстремум є максимумом:

$$OC_{ext}(a_{10}, a_{11}, a_{21}, cv_{opt}) = OC_{max}(a_{10}, a_{11}, a_{21}, cv_{opt}). \quad (3.16)$$

Якщо $a_{21} = 0$ лінійна форма (3.5) першого порядку вироджується у канонічну форму нульового порядку (сингулярний порядок), квадратична форма критерія вироджується в лінійну форму

$$OC_0(a_{10}, a_{11}, a_{21} = 0, cv) = (a_{10} - a_{20})cv + c_{11} - c_{21}, \quad (3.17)$$

яка, як відомо з лінійного програмування, має екстремальні значення критерію лише на границях області існування cv.

Частіше за все такі границі задаються, виходячи з обмежень та вимог до допустимого значення критерію. Наприклад, якщо, як обмеження, задано необхідне значення OC_0^*, тоді значення cv_{opt} визначають з нерівності

$$(a_{10} - a_{20})cv + c_{11} - c_{21} \geq OC_0^*. \quad (3.18)$$

З рівняння (3.18) витікає, що

$$cv_{opt} \geq \frac{OC_0^* - c_{11} + c_{21}}{a_{10} - a_{20}}. \quad (3.19)$$

Таким чином, лінійну канонічну форму (3.5) зручно розглядати як деку перехідну форму, яка в граничному розумінні пов’язує між собою задачі лінійного та нелінійного програмування. Постійні інтегрування c_{11}, c_{12} можна розглядати як

деякі вільні параметри, значення яких обирають, виходячи з конкретного логічного розуміння та змісту задачі оптимізації.

Якщо ж, припустити, що за логічним змістом екстремум критерія оптимізації повинен бути мінімумом та мінімальне значення критерію повинно бути рівним нулю, тоді $c_{21} \geq 0$ та

$$c_{21} - c_{11} = \frac{(a_{10} - a_{20})^2}{2a_{21}}. \tag{3.19}$$

Система правил дозволяє ввести таку форму представлення системи рівнянь оптимізації (3.5), яка за допомогою її інтегрального перетворення (3.6) дозволяє синтезувати морфологічним методом сепарабельні адитивні критерії та обмеження у вигляді (3.6). тобто дозволяє оцінювати захищеність ІС з урахуванням дозволених границь гарантованого рівня захисту інформації.

3.2. Методика виявлення ознак інформаційного впливу в інформаційних системах

Попередні дослідження продемонстрували, що зміст текстового контенту у СІС може містити деструктивний інформаційний вплив на акторів у явному або прихованому вигляді [28 - 30]. Висока складність процедур аналізу змісту текстового контенту й особливо автоматичного аналізу, призводить до ускладнення процесу виявлення початку і самого факту інформаційного впливу в СІС. Тому розроблення ефективних алгоритмів функціонування СЗІБД для вирішення проблеми виявлення прихованих ознак загроз у СІС є актуальним теоретико-прикладним завданням.

Визначення 3.1. Під контентом у СІС будемо розуміти інформаційне наповнення віртуальних спільнот з метою зацікавлення акторів, вираження власної точки зору на події, поширення оперативної та корисної інформації тощо.

Разом з тим, контент, який ґенерується акторами віртуальних спільнот, може бути представлений текстовими, аудіо, відео, графічними та іншими типами даних. Дослідження співвідношення видів контенту в СІС показують, що найбільшу частку інформаційного простору займає текстовий тип даних [31]. В першу чергу, це пов’язано з високою швидкістю його споживання акторами віртуальних спільнот завдяки універсальності, відсутності залежності якості відображення від типу кінцевого пристрою користувача. Популярність текстового контенту визначається закладеною в його зміст ідеєю, яка, приймаючи різні форми, покликана донести до актора потрібні картини суспільних чи політичних подій.

Аналіз останніх досліджень і публікацій з напрямку [32–38] показав, що для обробки і аналізу текстового контенту використовуються методи статистичного й лінгвістичного аналізу. Перша група методів ґрунтується на аналізі змісту контенту за частотою слів, які в ньому використовуються. Спільним недоліком групи статистичних методів є неможливість врахування зв’язності текстового контенту і, як наслідок, його представлення у вигляді множини не пов’язаних між собою слів або Bag of Words [32], [33]. Для усунення цього недоліку використовують методи лінгвістичного аналізу, які включають такі рівні:

а) графематичний для виділення абзаців, речень і окремих слів;

б) морфологічний, який має на меті визначення морфологічних характеристик і словоформ вхідного контенту;

в) синтаксичний аналіз для встановлення синтаксичної залежності слів у реченні;

г) семантичний аналіз для змістовного розуміння текстового контенту.

Семантичний аналіз є складною процедурою, яка ґрунтується на використанні баз знань і тезаурусів для відображення зв’язку між окремими словами й словосполученнями [32]. Результатом семантичного аналізу є формалізоване подання текстового контенту, який досліджується, для подальшого

інтелектуального аналізу. До недоліків сучасних семантичних аналізаторів можна віднести високу вартість їх підтримки для кожної окремої мови, істотну обчислювальну складність, неоднозначність результатів функціонування [32], [34].

Проблема виявлення ознак інформаційних впливів за змістовними ознаками не обмежується лінгвістичним аналізом текстового контенту СІС. Детектування загроз СЗІБД в СІС належить, зокрема, до задач інформаційного пошуку [34]. Серед класичних методів інформаційного пошуку виділяють теоретико-множинні, алгебричні та ймовірнісні. Однак їх застосування для пошуку в СІС текстового контенту з деструктивним інформаційним впливом обмежується рядом недоліків [32]:

неможливістю ранжування результатів пошуку;

розрахунки пов’язані зі значними об’ємами даних;

низькою обчислювальною масштабованістю і необхідністю навчання системи.

Тому перспективним напрямком є використання моделей семантичного пошуку та аналізу, які враховують зміст текстового контенту. Встановлено, що в існуючих дослідженнях проблеми виявлення інформаційних впливів у СІС не використовується комплексний підхід, який би систематизував і узагальнив їх частинні прояви. Протиріччя між рівнем розвитку сучасних інформаційних технологій і науковим базисом автоматизованого виявлення загроз в СІС, відсутність дієвих методик змістовного аналізу текстового контенту СІС на предмет деструктивного інформаційного впливу додатково актуалізують обраний напрямок досліджень.

З праць [33], [39] відомо, що в загальному вигляді сучасні системи виявлення загроз як в текстовому контенті, так і в технічних системах, функціонують на основі таких базових методів:

а) сигнатурні, ідея яких полягає в ідентифікації загроз із використанням відомих значень їх параметрів;

б) виявлення аномалій на базі відхилень від еталонної моделі функціонування об’єкта досліджень.

Сигнатурні методи відрізняються високою ефективністю, а загроза, в свою чергу, описується у вигляді набору правил чи формальної моделі. Однак у разі відсутності моделі деякої загрози в системі, її ідентифікація стає неможливою. Детектування системою виявлення загроз аномальної поведінки об’єкта дослідження пов’язане з його навчанням еталонній поведінці, відхилення від якої вказує на появу загрози. В окремих випадках опис загрози може збігатися з еталонною поведінкою об’єкта, що істотно впливає на достовірність функціонування модуля виявлення загроз. Тому перспективним напрямком є розроблення таких методів виявлення загроз ІБД в СІС за змістовними ознаками, які забезпечать задану достовірність функціонування, виявлення відомих та нових загроз в явному або прихованому вигляді, реалізованість за умови обмеженого забезпечення ресурсами.

У результаті узагальнення відомих підходів до інформаційного пошуку і лінгвістичного аналізу контенту СІС розроблено метод виявлення інформаційних впливів на основі встановлення їх ознак у змісті текстового контенту, який зводиться до такого [40–42]. Структурна схема методу подана на рис. 3.1.

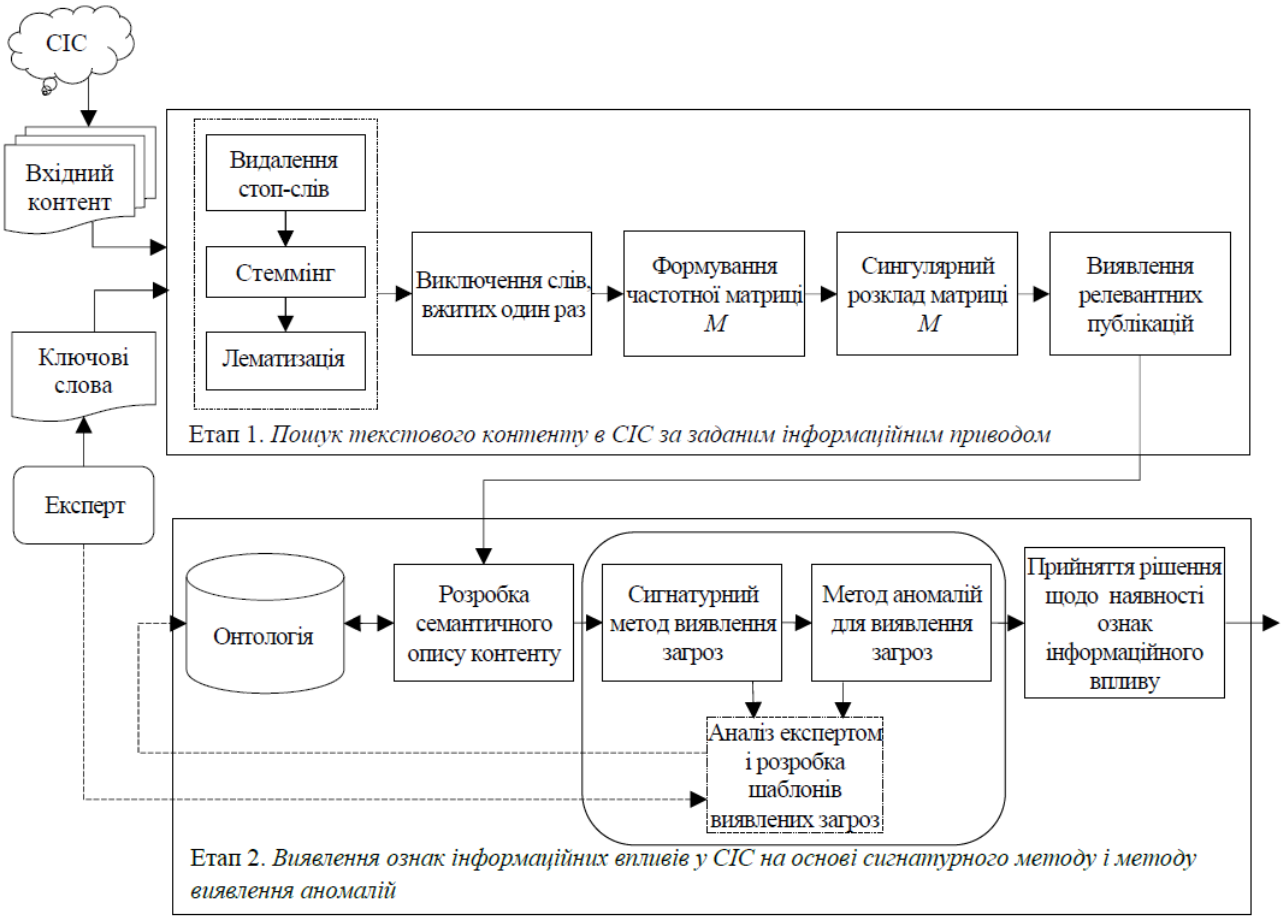

Рис. 3.1 - Узагальнена структурна схема методу виявлення інформаційних впливів у СІС

Етап 1. Пошук текстового контенту в СІС за заданим інформаційним приводом. На цьому етапі визначаються ключові слова $W = \langle w_i \rangle, i = \overline{1,n}$ для пошуку текстового контенту в СІС за критерієм актуальності, критичності та рівня обговорення у суспільстві його тематики.

У даному випадку поставлена задача зводиться до вибору методу інформаційного пошуку текстового контенту, який задовольняє вимогам релевантного пошуку природомовного тексту, ефективній обробці, зокрема, коротких публікацій. Тому пропонується скористатися методом латентно-семантичного індексування (LSI) (латентно-семантичного аналізу (LSA)) [34–36]. Особливостями LSI є пошук контенту в СІС на основі його змісту, а не щільності ключових слів, і пошук прихованих семантичних зв’язків між ключовими словами

й безпосередньо контентом. Суть методу LSI, адаптованого під задачі дослідження, наведена нижче [36].

Крок 1.1 методу полягає у попередній підготовці досліджуваного контенту СІС шляхом видалення стоп-слів, стеммінгу або лематизації слів. Стоп-слова зустрічаються у всьому контенті й не мають змістовного навантаження, наприклад, сполучники, частки, прийменники тощо. Стеммінг полягає у виділенні основи слова виключенням закінчень і суфіксів та є необов'язковим на великих наборах публікацій контенту СІС. Для випадку невеликих наборів публікацій доцільно скористатися алгоритмом Портера [43], який не вимагає морфологічних словників, а виділення основи слова реалізоване на основі визначених правил. Лематизація – це приведення слова до словникового виду.

Крок 1.2. Призначений для виключення з досліджуваного текстового контенту СІС слів, які вживаються тільки один раз. Даний крок не є обов'язковим, однак зменшує кількість подальших обчислень і, як наслідок, підвищує швидкодію.

Крок 1.3. Формування частотної матриці M ключових слів W , які індексуються. Рядками і цієї матриці є ключові слова W семантичного ядра, за яким виконується моніторинг текстового контенту СІС, а стовпцями j – публікації акторів чи віртуальних спільнот. Елементи матриці m_{ij} представляють собою частоту вживання деякого ключового слова w_i в j-й публікації.

Крок 1.4 полягає в сингулярному розкладанні початкової матриці M на три компоненти

$$M = U \times S \times V^T, \tag{3.20}$$

Де U і V^T – ортогональні матриці розмірністю $i \times k$ та $k \times j$відповідно;

S – діагональна матриця розмірністю $k \times k$;

k - кількість сингулярних значень матриці (прихованих тематик контенту), а її елементи впорядковані за спаданням.

На кроці 1.5 виділяють ті рядки матриці U і стовпці V^T , які відповідають найбільшим сингулярним числам k , а їх величина – ступеню прояву ключових слів у колекції публікацій в СІС.

У результаті виконання етапу 1 вдається одержати колекцію публікацій у СІС, які відповідають семантичному ядру пошукового запиту. Такі публікації підлягають подальшому семантичному аналізу на основі онтологій.

Етап 2. Виявлення ознак інформаційних впливів у СІС на основі сигнатурного методу і методу виявлення аномалій. Суть даного етапу полягає у виявленні загроз ІБД в СІС, які містяться в текстовому контенті, який ґенерується або поширюється віртуальними спільнотами, і мають на меті вплив на акторів, їх свободу вибору, дискредитацію органів влади тощо. Контент віртуальних спільнот, проіндексований і відібраний на попередньому етапі, підлягає семантичному аналізу на базі онтологій [44–48]. В роботі [44] визначено, що онтологія є експліцитною (явною) специфікацією опису множини об’єктів, які називають концептами, і зв’язків між ними – відношеннями. Зміст другого етапу методу полягає в наступному.

На кроці 2.1 складається онтологія функціонування віртуальної спільноти в СІС

$$Ont = \langle P_n, R_n \rangle, \tag{3.21}$$

де Ont – онтологія;

P_n – скінченна множина концептів;

R_n – скінченна множина відношень між концептами.

При цьому в онтології Ont (3.21) для автоматизації подальшого аналізу текстового контенту віртуальних спільнот виділяються [33]:

$P_s(p_n) \in P_n$ – підмножина концептів P_n, суміжних до деякого концепту p_n;

$P_{in}(r_n) \in R_n$ – підмножина відношень R_n, інцидентних до деякого концепту p_n;

$R_z(p_n) \in R_n$ - підмножина відношень R_n, вживання яких вказує на небезпеку для концепту p_n.

Крок 2.2 полягає у побудові семантичного опису текстового контенту, виявленого на першому етапі методу

$$Sem_t = \langle P_t, R_t \rangle, \tag{3.22}$$

Для забезпечення швидкодії функціонування методу доцільно застосовувати автоматичні засоби ґенерації онтологій. До такого класу програмних продуктів відносять *Protege, Ontology Learning Framework, LOGS, ABBYY Compreno* тощо [48]–[50].

Крок 2.3 зводиться до виявлення ознак загрози у попередньо проіндексованому на першому етапі методу текстовому контенті СІС. У формальному вигляді правила виявлення загроз інформаційній безпеці зводяться до такого [33]:

а) детектування на основі сигнатурного методу і семантичних ознак

$$\exists r_t(p_t): p_t \in P_n \wedge r_t \in R_z(p_n), \tag{3.23}$$

де $r_t(p_t)$ - деяке відношення з текстового контенту СІС, що аналізується;

$p_t \in P_n$ - концепт онтології *Ont* досліджуваної віртуальної спільноти;

$r_t \in R_z(p_n)$ - множина відношень, які вказують на небезпеку для деякого концепту p_n.

Суть виразу (3.23) полягає в наступному: для виявлення загрози ІБД у змісті текстового контенту віртуальної спільноти СІС необхідно виявити зв'язок між об’єктом публікації з його характеристиками у контенті та негативними ознаками для цього об’єкта внаслідок реалізації загрози;

б) виявлення суперечностей на основі методу аномалій шляхом співставлення семантичного опису проіндексованого текстового контенту і

семантичного шаблону загрози. При цьому встановлюється невідповідність фактів у контенті СІС, що проявляється як [33]:

– протиріччя понять в змісті контенту віртуальних спільнот – вживання концепту в конкретному відношенні не передбачене онтологією

$$\exists r_t(p_t): p_t \in P_n \wedge r_t \in R_n \wedge p_t \notin P_{in}(r_n), \quad (3.24)$$

Зміст виразу (3.24) полягає в такому: деякий концепт p_t текстового контенту СІС не може вживатися у конкретному відношенні $r_t(p_t)$.

– протиріччя відношень в контенті – вжите відношення між концептами не визначене онтологією

$$\forall p_t \in P_n \neg \exists r_n \in R_n: r_t = r_n. \quad (3.25)$$

Вираз (3.7) пояснюється наступним чином: множина відношень R_n онтології функціонування віртуальної спільноти, в які можуть вступати концепти $p_n \in P_n$, які пов'язані між собою відношеннями r_t , не містить цих відношень.

Крок 2.4 призначений для розгорнутого аналізу експертами проіндексованого текстового контенту на предмет наявності загроз. Даний крок необхідний, якщо контент СІС є релевантним семантичному ядру пошукового запиту до контенту СІС з етапу 1, однак на етапі 2 не виявлено суперечливих фрагментів такого контенту і онтології. Тоді ідентифіковані експертами небезпечні семантичні конструкції додаються до шаблонів загроз і використовуються в онтології. В результаті таких дій метод LSI забезпечує ефективне виявлення залежностей між лексичними одиницями в контенті СІС для наповнення онтологічних баз знань [49].

Обмеження 3.2. Вибір текстового контенту для досягнення мети дослідження проводиться відповідно до вимог критичності та значущості його тематики у розрізі ІБД.

Обмеження 3.3. Для побудови онтологій обираються предметні області, пов’язані із забезпеченням ІБД.

Розглянутий метод [41], [42] поєднує в собі сучасні підходи до обробки текстового контенту – семантичний і LSI. Така комбінація підходів реалізує взаємну компенсацію їх недоліків: полісемії, омонімії та інших видів лінгвістичних неоднозначностей для LSI; виявлення латентних залежностей між концептами для семантичного аналізу. Перспективним є використання запропонованого методу для функціонування СЗІБД в СІС, зокрема для підвищення ефективності виявлення прихованих ознак загроз в інформаційному середовищі віртуальних спільнот. Окреме місце в забезпеченні функціонування методу належить експертам і співробітникам спеціальних підрозділів, перед якими стоїть завдання виявлення деструктивних інформаційних впливів у попередньо проіндексованому й відібраному контенті СІС. На основі таких ідентифікованих впливів створюються семантичні шаблони загроз і додаються до онтологічних БЗ.

3.3. Оптимізація етапів методології захисту кіберпростору від інформаційних впливів

На заключному етапі досліджень на основі розглянутого методологічного інструментарію та з урахуванням вимог нормативних документів досліджено методологію побудови СЗІБД у ІС, яка забезпечує ефективність і дієвість протидії зовнішнім і внутрішнім загрозам [21]. Реалізація методології зводиться до виконання ряду етапів і подана у вигляді структурної схеми на рис. 3.5.

Етап 1. Моніторинг текстового контенту в ІС. На першому етапі експертом з ІБД на основі проведеного аналізу інформаційного простору визначається найбільш актуальна тематика, яка є значущою для суспільства, обговорюється і поширюється у ІС.

Етап 2. Виявлення і оцінювання загроз ІБД у ІС. З цією метою на базі розглянутих методологічних засад виявлення загроз у ІС виконують наступні кроки:

1) виявлення ознак інформаційних операцій, спрямованих проти ІБД;

2) виявлення прихованих ознак загроз ІБД;

3) виявлення інформаційного впливу на користувачів ІС;

4) оцінювання профілів ІБ ІС;

5) розрахунок інтегральної оцінки загроз у ІС.

Етап 3. Прийняття рішення щодо заходів з інформаційної протидії виявленим загрозам ІБД у ІС є завершальним етапом методології. На основі розрахованого на попередньому етапі значення інтегральної оцінки загроз ІБД у ІС виконується вибір заходів з протидії.

Якщо рівень загрози визначено як “відсутня”, то використання ресурсів СЗІБД у ІС не проводиться. У випадку виявлення загрози рівня “нижча середнього”, тоді продовжуються дії системи з моніторингу інформаційного простору віртуальних спільнот відповідно до першого етапу.

Якщо рівень загрози ІБД у ІС набуває значення “існує”, то додатково до заходів з моніторингу інформаційного простору сервісів для реалізації керованого переходу інформаційної системи до заданого стану ІБ використовується концепція синергетичного управління взаємодією користувачів. При цьому експерт з ІБ обирає параметр взаємодії користувачів, який потребує коригування, та модель синергетичного управління для прихованого управління процесами соціальної комунікації з метою переходу до заданого стану ІБД. У свою чергу, СЗІБД у ІС формує рішення щодо протидії загрозам залежно від їх особливостей, завантаженості ресурсів системи тощо.

Реалізація методології побудови СЗІБД у СІС, з урахуванням концептуальних основ і методів, дозволяє підвищити рівень ІБД в умовах інтеграції національного сегменту в загальносвітовий інформаційний простір. Застосування методології при побудові СЗІБД у ІС дозволяє врахувати різні прояви загроз ІБД при одночасному зростанні їх кількості й забезпечує завчасне виявлення їх ознак

та створює передумови для організації ефективної інформаційної протидії. Таким чином, методологічні засади побудови СЗІБД у ІС забезпечують досягнення поставленої мети.

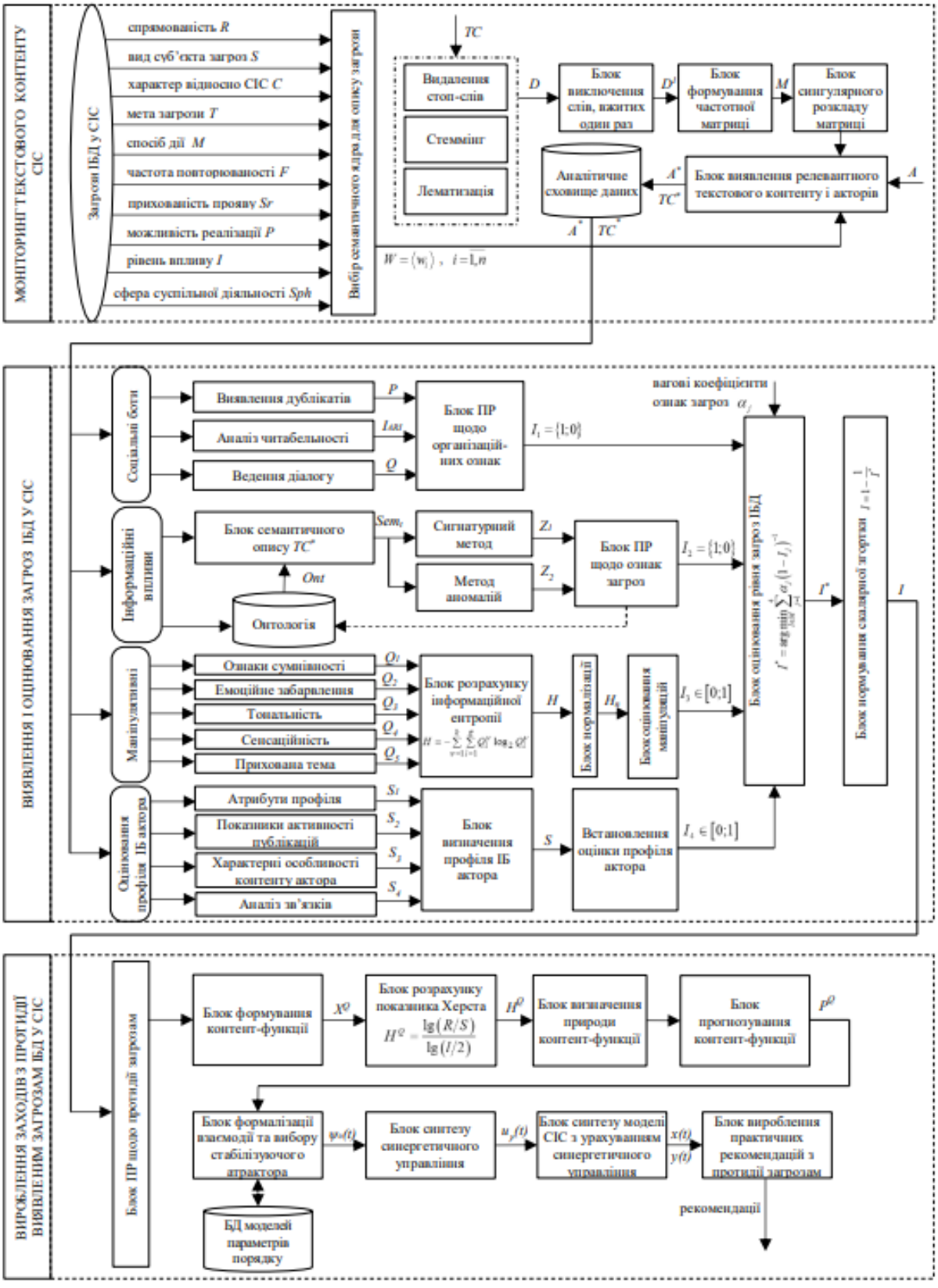

Рисунок 3.2 – Схема методології побудови системи забезпечення ІБД у СІС

Висновки з третього розділу:

Запропоновано систему правил щодо моделювання критеріїв оптимальності, які, за рахунок синтезу морфологічним методом сепарабельних адитивних критеріїв та обмежень, дозволяють розвязувати задачі аналізу, синтезу та оптимізації систем за обраними критеріями та виділеними обмеженнями, а також оцінювати рівень захищеності інформаційних систем з урахуванням дозволених границь гарантованого рівня захисту інформації.

Представлено методологію виявлення інформаційно впливу на користувачів віртуальних спільнот у СІС, в основу якого покладено дерево рішень, що призначене для визначення зв'язків між ознаками маніпуляцій в текстовому контенті, який поширюється у СІС. Це дозволяє визначати інформаційну ентропію у вигляді інтегрального показника загрози ІБД для планування та проведення у подальшому на основі одержаних результатів заходів інформаційної протидії.

Обґрунтовано вимоги до СЗІБД у СІС як дієвого механізму реалізації державної інформаційної політики для злагодженого задоволення інтересів людини, суспільства і держави в інформаційній сфері. Сформульовано мету і завдання функціонування СЗІБД у СІС, визначено суб'єкти забезпечення ІБД відповідно до Доктрини інформаційної безпеки України. Встановлено, що перспективним напрямком забезпечення суверенітету держави у інформаційній сфері є залучення громадських організацій до діяльності державних органів, які представляють собою суб'єкти ІБД.

ВИСНОВКИ

1. Проведений аналіз сучасних методів моделювання інформаційних впливів дав можливість визначити найбільш ефективний підхід і використати його з метою оптимізації параметрів систем захисту.

2. Досліджено класифікацію загроз кіберпростору, яка реалізує віднесення виявлених об’єктів з множини небезпек до попередньо встановлених класів. Використання фасетного підходу до класифікації загроз забезпечує можливість подальшого її розширення для врахування їх нових видів і проявів. Однозначна формалізація загрози в кіберпросторі у вигляді кортежу дозволяє в подальшому розробити дієві методи їх виявлення, оцінювання і протидії, прогнозування впливу на процеси взаємодії акторів та ІБД в цілому.

3. Досліджено метод оцінювання загроз кіберпростору, який ґрунтується на нелінійній схемі компромісів і відрізняється від відомих врахуванням ознак використання соціальних ботів для проведення інформаційних операцій, інформаційних впливів в ІС. Завдяки узагальненому показнику рівня загроз метод дозволяє обґрунтувати вибір ефективних заходів з інформаційної протидії для нейтралізації виявлених загроз та забезпечення заданого рівня.

4. Запропоновано систему правил щодо моделювання критеріїв оптимальності, які, за рахунок синтезу морфологічним методом сепарабельних адитивних критеріїв та обмежень, дозволяють розв’язувати задачі аналізу, синтезу та оптимізації систем за обраними критеріями та виділеними обмеженнями, а також оцінювати рівень захищеності інформаційних систем з урахуванням дозволених границь гарантованого рівня захисту інформації.

5. Запропоновано методику виявлення інформаційно впливу, в основу якого покладено дерево рішень, що призначене для визначення зв’язків між ознаками маніпуляцій в текстовому контенті, який поширюється в кіберпросторі. Це дозволяє визначати інформаційну ентропію у вигляді інтегрального показника

загрози для планування та проведення у подальшому на основі одержаних результатів заходів інформаційної протидії.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Буравльов М.М. Глобалізація: проблеми безпеки / Буравльов Є.П. – К.: Ін-т проблем нац.. безпеки, 2007 – 160 с.

2. Ковтун И.А. Виды информационных воздействий / Ковтун И.А., Мухан В.И., Набока Ю.И. // Вопросы защиты информации, 2001, №1 (52). – С. 2-7.

3. Голубенко О.Л. Політика інформаційної безпеки / Голубенко О.Л., Хорошко В.О., Петров О.С., Головань С.М., Яремчук Ю.Є. – Луганськ: Вид. СНУ ім. В. Даля, 2009. – 300 с.

4. Захаров А.И. Информационные системы: оценка рисков / А.И. Захаров // Information Security (Информационная безопасность) – 2005. - №6 – С. 18-19.

5. Петренко С.А. Политика информационной безопасности / Петренко С.А., Курбатов В.А. – М.: Компания Ай Ти, 2006. – 400 с.

6. Волобуев С.В. О систематизации выявления и анализа каналов утечки. Прямые и косвенные носители информации / Волобуев С.В. // Вопросы защиты информации, №1, 2000. – С. 26-37.

7. Николаев Ю.А. Оборонная достаточность: критерии и методы оценки / Николаев Ю.А. // Военная мысль, 1992, №4-5. – С.47-52.

8. Габобич А.Г. Методика оцінки рівня безпеки інформації / Габобич А.Г., Горобець А.Ю., Хорошко В.О. // Вісник НУ «Львівська політехніка», №551, Автоматика, вимірювання та керування, 2006. – С. 48-53.

9. Хорошко В.А. Виды информационных воздействий / Хорошко В.А., Чередниченко В.С. // Захист інформації, Спец. Випуск, 2007. – С. 6-8.

10. Мухин В.Е. Комплексная система мониторинга безопасности на основе анализа целей субьектов компьтерных систем и сетей / В.Е. Мухин, А.Н. Волокита // Управляющие системы и машины. – К.: УСиМ, 2006. – №5. – С. 85-92.

11. Сірченко Г.А. Алгоритм визначення показників для оцінки надійності систем спеціального призначення / Г.А. Сірченко, В.О. хорошко, Ю.Є. Хохлачова // Інформаційна безпека. – 2013. - №1(9). – С. 142-147.

12. Biskup J. Security in Computing Systems: Challenges, Approaches and Solutions: monograph / J. Biskup. – Berlin: Springer, 2009. – 694 p.

13. Стратегія управління інформаційною безпекою / В.І. Андрєєв, В.Д. Козюра, Л.М. Скачек, В.О. Хорошко. – К.: ДУІКТ, 2007. – 272 с.

14. Управление надежностью. Анализ риска технологических систем: ГОСТ Р 51901 – 2002. – Введ. 2003.09.01. – М.: ИПК «Издательство стандартов», 2002. – 21 с.

15. Міністерство інформаційної політики України. (2015, Черв. 5). Проект Концепції інформаційної безпеки України. [Електронний ресурс]. Доступно: http://mip.gov.ua/documents/30.html. Дата звернення: Лист. 07, 2017.

16. Верховна Рада України. (2003, Черв. 19). Закон України № 964-15, Про основи національної безпеки України. [Електронний ресурс]. Доступно: http://zakon2.rada.gov.ua/laws/show/964-15. Дата звернення: Лист. 07, 2017.

17. Верховна Рада України. (2007, Січ. 09). Закон України №537-16, Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки. [Електронний ресурс]. Доступно: http://zakon4.rada.gov.ua/laws/show/537-16.

18. Офіційне представництво Президента України. (2017, Лют. 25). Указ Президента України №47/2017, Доктрина інформаційної безпеки України. [Електронний ресурс]. Доступно: http://www.president.gov.ua/documents/472017-21374.

19. В. А. Ліпкан, Ю. Є. Максименко, та В. М. Желіховський, Інформаційна безпека України в умовах євроінтеграції, К.: КНТ, 2006.

20. В. А. Ліпкан, Національна безпека України: нормативно-правові аспекти забезпечення, К.: Текст, 2003.

21. В. Л. Бурячок, Р. В. Грищук, та В. О. Хорошко, Політика інформаційної безпеки, К.: ПВП “Задруга”, 2015.

22. Вунш Г. Теория систем / Вунш Г. – М.: Сов. Радио, 1978. – 288 с.

23. Тиснина Е.О. Абсолютная устойчивость положения равновесия системы поддержки принятия решений в системе защиты информации / Тиснина Е.О., Хорошко В.А. // Сучасний захист інформації, №4, 2010. – С. 74-79.

24. Игнатов В.А. Аксиоматическая теория математического моделирования критериев оптимальности и ограничений / Игнатов В.А., Минаев Ю.Н., Гузий Н.Н. // Захист інформації №4, 2005. – С. 46-56.

25. Мухин В.Е. Комплексная система мониторинга безопасности на основе анализа целей субьектов компьютерных систем и сетей / В.Е. Мухин, А.Н. Волокита // Управляющие системы и машины. – К.: УСиМ, 2006. - №5. – С. 85-92.

26. Хохлачова Ю.Є. Моделювання критеріїв оптимальності та обмежень для захисту інформаційних систем / Ю.Є. Хохлачова // Захист інформації. – 2012. - №4(57). – С. 106-109.

27. Хоменюк В.В. Элементы теории многоцелевой оптимизации / Хоменюк В.В. – М.: Наука, 1983. – 343 с.

28. В. А. Ліпкан, “Сутність гібридної війни проти України”, Імперативи розвитку цивілізації, № 2, с. 13–16, 2015.

29. В. М. Панченко, та В. І. Полевий, “Методика виявлення ознак інформаційного впливу в засобах масової інформації”, Інформаційна безпека людини, суспільства, держави, № 3(7), с. 70–77, 2011.

30. Р. В. Грищук, та Ю. Г. Даник, Основи кібернетичної безпеки. Монографія, Житомир: ЖНАЕУ, 2016.

31. “Какие бывают типы контента и как с ними работать для реализации успешной стратегии контент-маркетинга”, Alphaland.in Интернет Маркетинг. [Электронный ресурс]. Доступно: http://alphaland.in/kakie-by-vayut-tipy-kontenta-i-kak-s-nimi/. Дата обращения: Ноя. 22, 2017.

32. С. В. Лапшин, “Методы повышения показателей качества фильтрации DLP-систем на основе предметно-ориентированной морфологической модели естественного языка”, дисс. канд. техн. наук, Санкт-Петербургский нац. иссл. ун-т информационных технологий, механики и оптики, Санкт-Петербург, 2014.

33. С. В. Чернишук, “Методика виявлення кібернетичних загроз у природномовних текстах”, Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем, вип. 8, с. 112–121, 2013.

34. Chr. D. Manning, P. Raghavan, and H. Schütze, Introduction to Information Retrieval, Cambridge University Press, 2008.

35. “Латентно-семантический анализ”, Habrahabr.ru, 2015. [Электронный ресурс]. Доступно: https://habrahabr.ru/post/110078/. Дата доступа: Ноя. 17, 2017.

36. S. Deerwester, S. T. Dumais, G. W. Furnas, T. K. Landauer, and R. Harshman, “Indexing by latent semantic analysis”, Journal of the American Society for Information Science, 41(6), pp. 391–407, 1990.

37. І. В. Замаруєва, В. Б. Толубко, Л. О. Литвиненко, та О. Ю. Ніколаєвський, “Модель лінгвістичної бази даних в системах автоматичної обробки природномовної текстової інформації”, Інформатика та математичні методи в моделюванні, т. 3, № 1, с. 75–81, 2013.

38. С. В. Лєнков, І. В. Замаруєва, І. В. Пампуха, та Л. В. Охрамович, “Модель представлення знань для багатомовної системи машинного перекладу”, Сучасна спеціальна техніка, № 2(37), с. 14–20, 2014.

39. Р. В. Грищук, Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень: монографія, Житомир: Рута, 2010.

40. К. В. Молодецька-Гринчук, “Метод виявлення ознак інформаційних впливів у соціальних інтернет-сервісах за змістовними ознаками”, Радіоелектроніка, інформатика, управління, № 2(41), с. 117–126, 2017.

41. К. В. Молодецька-Гринчук, “Семантичний аналіз текстового контенту для виявлення інформаційних впливів на акторів у соціальних інтернет-сервісах”, на Міжнар. наук.-практ. конф. Проблеми і перспективи розвитку ІТ-індустрії, Харків, 2017, с. 58.

42. К. В. Молодецька-Гринчук, “Виявлення інформаційних впливів у соціальних інтернет-сервісах на основі інтелектуального аналізу текстового контенту”, на ІІІ Міжнар. наук.-практ. конф. Актуальні питання забезпечення кібербезпеки та захисту інформації, Київ, 2017, с. 121–122.

43. “Стеммер Портера для русского языка”, Algorithmist.ru. [Электронный ресурс]. Доступно: http://www.algorithmist.ru/2010/12/porter-stemmer-russian.html. Дата обращения: Ноя. 22, 2017.

44. T. R. Gruber, “A Translation Approach to Portable Ontology Specifications”, Knowledge Acquisition, 5(2), pp. 199–220, 1993.

45. B. Wielinga et al., “Framework and Formalism for Expressing Ontologies”, ESPRIT Project 8145 KACTUS, Free University of Amsterdam Deliverable, DO1b.1, 1994.

46. Y. Kalfoglou, and M. Schorlemmer, “Ontology mapping: The state of the art”, The Knowledge Engineering Review, 18(1), pp. 1–31, 2003.

47. M. Priya, and K. Aswani, “A survey of state of the art of Ontology construction and merging using formal concept analysis”, Indian Journal of Science and Technology, 8(24), 2015.

48. Я. Р. Василюк, В. М. Теслюк, та А. Я. Зелінський, “Аналіз моделей, методів, принципів і засобів для побудови онтологій області мікроелектромеханічних систем”, Наук. вісн. Нац. лісотехнічного ун-ту України, вип. 21.12, с. 322–330, 2011.

49. О. О. Марченко, “Порівняння методів онтологічного семантичного аналізу та алгоритмів латентного семантичного аналізу”, Вісн. Київського нац. ун-ту ім. Т. Шевченка. Сер. фіз.-мат. науки, 2, с. 169–174, 2012.

50. В. А. Ліпкан, І. М. Сопілко, та В. О. Кір’ян, Правові засади розвитку інформаційного суспільства в Україні, К.: ФОП О. С. Ліпкан, 2015.

51. В. К. Конах, Національний інформаційний простір України: проблеми формування та державного регулювання: аналіт. доп., К.: НІСД, 2014.

52. К. В. Молодецька, “Соціальні інтернет-сервіси як суб’єкт інформаційного простору держави”, на VIII Міжнар. наук.-техн. конф. Інформаційно-комп’ютерні технології, Житомир, 2016, с. 43–44.

53. О. Бусол, “Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України”, Nbuviap.gov.ua. [Електронний ресурс]. Доступно: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=

2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350. Дата звернення: Лист. 10, 2017.

54. О. В. Олійник, “Інформаційна безпека США”, Боротьба з організованою злочинністю і корупцією (теорія і практика), вип. 1, с. 280–288, 2012.

55. В. М. Петрик, М. М. Присяжнюк, та Д. С. Мельник, Забезпечення інформаційної безпеки держави, К.: ДПУ “Книжкова палата України”, 2015.

56. International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. The WHITE HOUSE. [Online]. Available: http://www.whitehouse.gov/sites/default/files/rss_viewer/ international_strategy_for_ cyberspace.pdf. Accessed: Nov. 10, 2017.

57. О. Зернецька, “UA Foreign Affairs: Еволюція стратегій кібербезпеки США”, Uaforeignaffairs.com, 2017. [Електронний ресурс]. Доступно: http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/evoljucija-strategii-kiberbezpeki-ssha-1/. Дата звернення: Лист. 10, 2017.

58. О. Бусол, “Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України”, Nbuviap.gov.ua. [Електронний ресурс]. Доступно: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350. Дата звернення: Лист. 10, 2017.

59. Cyber Security Strategy. [Online]. Available: https://www.enisa.europa.eu/ topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_ Strategy.pdf. Accessed: Nov. 10, 2017.

60. The UK Cyber Security Strategy. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/UK_ NCSS.pdf. Accessed: Nov. 10, 2017.

61. Cyberspace protection policy of the Republic of Poland. [Online]. Available: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy _of_PO_NCSS.pdf. Accessed: Nov. 10, 2017.

62. О. Ю. Запорожець, “Політика європейського союзу в сфері інформаційної безпеки”, Актуальні проблеми міжнародних відносин, вип. 87, ч. 2, с. 36–45, 2009.

63. Офіційне представництво Президента України. (2017, Лют. 25). Указ Президента України №47/2017, Доктрина інформаційної безпеки України. [Електронний ресурс]. Доступно: http://www.president.gov.ua/documents/472017-21374.

64. Н. Тарасенко, “Доктрина інформаційної безпеки України в оцінках експертів”, Резонанс, № 18, с. 3–14, 2017.

65. Т. Попова, “Що означає “Доктрина інформаційної безпеки України”?”, 2017. [Електронний ресурс]. Доступно: http://www.radiosvoboda.org/a/ 28337376.html. Дата звернення: Лист. 10, 2017.

66. В. М. Богуш, та О. К. Юдін, Інформаційна безпека держави, Київ: МК-Прес, 2005.

67. О. Золотар, та І. Трубін, “Класифікація загроз інформаційної безпеки”, Інформація і право, № 3(9), с. 105–112, 2013.

68. А. Пелещишин, та Р. Гумінський, “Загрози інформаційної безпеки держави в соціальних мережах”, Наука і техніка Повітряних Сил Збройних Сил України, №2, с. 192–199, 2013.

69. В. Сазанов, “Социальные сети : Анализ – Технологии – Перспективы. Обзор”, Сайт Лаборатории СВМ. [Электронный ресурс]. Доступно: http://ntl-cbm.narod.ru/CBM-NET/net_rew.doc. Дата обращения: Ноя. 08, 2017.

70. Міністерство інформаційної політики України. (2015, Черв. 5). Проект Концепції інформаційної безпеки України. [Електронний ресурс]. Доступно: http://mip.gov.ua/documents/30.html.

71. В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, та С. В. Толюпа, Інформаційна та кібербезпека: соціотехнічний аспект, Ред. В. Б. Толубко, Київ: ДУТ, 2015.

72. C. Barrett, S. Eubank, and M. Marathe, “Modeling and simulation of large biological, information and socio-technical systems: an interaction based approach”, in Interactive Computation, Berlin: Springer Berlin Heidelberg, 2006, pp. 353–392.

73. Ю. Радковець, О. Левченко, та О. Косогов, “Погляди на створення системи інформаційної безпеки України та її Збройних Сил”, Наука і оборона, № 1, с. 38–42, 2014.

74. Я. Малик, “Інформаційна безпека України: стан та перспективи розвитку”, Ефективність державного управління, вип. 44, с. 13–20, 2015.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (ПРЕЗЕНТАЦІЯ)