

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ”

ЄВСЕЄВ С.П., ЗАКОВОРОТНИЙ О. Ю., МІЛОВ О.В., КУЧУК Г.А.,
ГАЛУЗА О.А., КОВАЛЬ М.В., ВОЙТКО О.В., ГРИЩУК Р.В.

МЕТОДОЛОГІЯ СИНТЕЗУ МОДЕЛЕЙ ІНТЕЛЕКТУАЛЬНИХ
СИСТЕМ УПРАВЛІННЯ ТА БЕЗПЕКИ ОБ’ЄКТІВ
КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Монографія

Харків. Вид. «Новий Світ-2000», 2024

М 54

УДК 004.056.5:004.912.4

Затверджено на засіданні вченої ради НТУ «ХПІ», протокол № 5 від 24.05.2024 р.

Рецензенти:

КОРЧЕНКО Олександр Григорович, перший проректор Державного університету телекомунікацій. Член-кореспондент НАН України, Лауреат державної премії України в галузі науки і техніки, Заслужений діяч науки і техніки України, д.т.н. професор

МІРНЕНКО Володимир Іванович – директор Департаменту військової освіти і науки Міністерства оборони України, доктор технічних наук, професор, заслужений працівник освіти України, полковник.

Євсєєв С.П. Методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури. Монографія/ С.П. Євсєєв, О.Ю. Заковоротний, О.В. Мілов, Г.А. Кучук, О.А. Галуза, М.В. Коваль, О.В. Войтко, Р.В. Грищук– Харків: Вид. «Новий Світ-2000», 2024. – 299 с. (Укр. мов.)

В монографії запропонована методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури, принципово різних за своїми властивостями забезпечується безперервність виконання основних функцій інтелектуальними системами управління об'єктів критичної інфраструктури при одночасному гарантованому (заданому) рівні захищеності таких систем, що має критично важливе значення для подальшого розвитку галузі інформаційної безпеки держави в інтересах підвищення рівня національної безпеки України, забезпечення безпеки громадян, захисту їх прав та свобод. Монографія призначена для студентів старших курсів, аспірантів, інженерів та наукових працівників, чия професійна діяльність пов'язана з розробкою та експлуатацією інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури.

© Національний технічний університет
“Харківський політехнічний інститут”

© Євсєєв С.П., Заковоротний О.Ю., Мілов О.В.,
Кучук Г.А., Галуза О.А., Коваль М.В., Войтко О.В.,
Грищук Р.В., 2024

ЗМІСТ

ВСТУП.....	6
ГЛАВА 1. ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ БАГАТОКОНТУРНИХ СИСТЕМ БЕЗПЕКИ.....	9
1.1. Об'єкти критичної інфраструктури: елементи, процедури, структура.....	9
1.2. Загрози безпеці об'єктам критичної інфраструктури. Класифікатор загроз як формальне подання типів та властивостей кіберзагроз.....	17
1.3. Концепція багатоконтурних систем безпеки об'єктів критичної інфраструктури.....	20
1.4. Система управління як система з критичною кіберінфраструктурою.....	24
1.5. Модель виявлення та пошуку об'єктів з критичною кіберінфраструктурою.....	28
Висновки за главою 1.....	32
ГЛАВА 2. МОДЕЛЮВАННЯ ДИНАМІКИ ПОВЕДІНКИ ОБ'ЄКТІВ СИСТЕМ БЕЗПЕКИ.....	34
2.1. Концепція моделювання поведінки взаємодіючих агентів систем безпеки.....	34
2.2. Модельний базис методології моделювання процесів поведінки антагоністичних агентів.....	38
2.3. Системно-динамічна модель поведінки антагоністичних агентів.....	43
2.4. Динамічні моделі безпеки на основі підходу Лотки-Вольтери...	46
2.5. Концепція побудови диференціально-ігрових розподілених систем інформаційної безпеки.....	50
2.6. Диференціально-ігрова модель розподіленої системи інформаційної безпеки.....	57
2.7. Диференціально-ігрова нетейлорівська модель.....	63
2.8. Синтез оптимальної поведінки в системі кіберзахист– кібератака.....	66
2.9. Багатокритерійна диференціально-ігрова модель процесу кібернападу на державні інформаційні ресурси об'єкта критичної інфраструктури.....	74

2.10. Ієрархічна диференціально-ігрова модель для задач оцінювання ефективності систем інформаційної безпеки.....	82
Висновки за главою 2.....	89
ГЛАВА 3. МЕХАНІЗМИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ПОСЛУГ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.....	92
3.1. Властивості постквантових алгоритмів забезпечення послуг безпеки об'єктів критичної інфраструктури.....	92
3.2. Забезпечення послуг безпеки об'єктів критичної інфраструктури на основі крипто-кодових конструкцій на <i>ЕС (МЕС)</i>	99
3.3. Забезпечення послуг безпеки об'єктів критичної інфраструктури на основі гібридних крипто-кодових конструкцій на збиткових кодах.....	102
Висновки за главою 3.....	105
ГЛАВА 4. ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ КЕРУВАННЯ ОБ'ЄКТАМИ ТА БАЗИ ЗНАНЬ НА ОСНОВІ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ.....	107
4.1. Архітектури та алгоритми функціонування безперервних нейронних мереж адаптивної резонансної теорії, здатних визначати декілька рішень.....	107
4.2. Стабільно-пластичні нейронні мережі Гемінга, Хебба та мережі на основі перцептрону здатні розпізнавати нову інформацію, донавчатися та визначати декілька рішень.....	117
4.3. Багатоспрямовані бази знань побудовані на моделях асоціативної пам'яті, що дозволяють донавчатися та визначати кілька рішень.....	144
Висновки за главою 4.....	163
ГЛАВА 5. МОДЕЛІ УПРАВЛІННЯ ТРАФІКОМ ІНТЕГРАЛЬНИХ ПОТОКІВ ДАНИХ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.....	164
5.1. Моделювання трафіку, створюваного інтегральними потоками даних.....	164

5.2. Модель процесу буферизації при управлінні трафіком інтегральних потоків даних.....	172
5.2.1. Сплайн-інтерполяція еластичного трафіку.....	172
5.2.2. Ітераційний метод оцінки адекватності моделі трафіку.....	175
5.3. Моделі інтелектуального управління трафіком інфокомунікаційних мереж об'єктів критичної інфраструктури.....	177
5.4. Конвергенція трафіку в мультисервісних мережах.....	182
5.5. Визначення характеристик викидів агрегованого трафіку.....	186
5.6. Фрактальна модель трафіку ІПД.....	194
5.6.1. Визначення фрактальної розмірності трафіку.....	194
5.6.2. Фрактальні властивості трафіку ІПД з повторними запитами.....	198
5.6.3. Фрактальна модель трафіку ІПД, що використовує властивість масштабної інваріантності.....	202
5.7. Модель процесу буферизації при управлінні трафіком інтегральних потоків даних.....	212
5.8. Моделі інтелектуального управління трафіком інфокомунікаційних мереж об'єктів критичної інфраструктури.....	217
Висновки за главою 5.....	226
ГЛАВА 6. ПРИКЛАДНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ.....	228
6.1. Диференціально-ігровий шаблон нормальної поведінки Web-сервера Житомирського військового інституту імені С. П. Корольова.....	228
6.2. Експериментальна верифікація диференціально-ігрових моделей критичної кіберінфраструктури на прикладі сайту Центральної виборчої комісії.....	241
6.3. Методологія синтезу диференціально-ігрових моделей та методів моделювання процесів кібернападу.....	255
6.4. Верифікація моделей постквантових алгоритмів у модифікації протоколу SSL/TLS.....	260
6.5. Методологія побудови багатоконтурних систем захисту об'єктів критичної інфраструктури.....	265
Висновки за главою 6.....	271
ВИСНОВКИ.....	275

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	278

ВСТУП

В умовах триваючої збройної агресії російської федерації проти України безпека людини, суспільства і держави суттєво залежать від надійного функціонування об'єктів критичної інфраструктури. Окрім фізичних впливів на такі об'єкти летальною зброєю російська федерація не полишає спроб разом зі своїми сателітами впливати нелетальними засобами – кіберзброєю на системи управління об'єктів критичної інфраструктури через кіберпростір та з кіберпростору. Враховуючи транскордонність кіберпростору та високий рівень інформатизації об'єктів критичної інфраструктури як в Україні, так і у світі, наприклад, об'єктів ядерної енергетики (Запорізька та Чорнобильська атомні станції) та об'єктів водопостачання (Каховська та Київська ГЕС), систем управління військами та зброєю (Єдиної автоматизованої системи управління (ЄАСУ) Збройними Силами (ЗС) України та її складових) тощо, ризики масштабуються не тільки на національний безпековий вимір, а й становлять загрозу для людства на глобальному рівні на досягну перспективу. Ситуація ускладнюється тим, що об'єкти критичної інфраструктури які функціонують в єдиному інформаційному просторі й підтримують широкий спектр сучасних інформаційних технологій, всупереч на колосальні зусилля задля протидії стороннім втручанням з кіберпростору та через кіберпростір й надалі залишаються вразливими до загроз нового типу.

Висока складність об'єктів та систем критичної інфраструктури, сучасних методів атак та захисту, потребують створення нових методів побудови відповідних систем управління та безпеки. Запропонована в монографії методологія синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури ґрунтується на принципово новому підході до побудови таких систем. В основу методології покладено принцип синергізму. Інтелектуалізація моделей та синергетичні ефекти, що виникають при їх синтезі дозволяють отримувати нові емерджентні властивості систем управління та безпеки об'єктів критичної інфраструктури. Зокрема на основі одержаних моделей відкрито ефект побудови N-контурних інтелектуальних систем управління та безпеки з наперед заданими показниками стійкості до загроз визначеного (квантового) або прогнозованого (постквантового) типу, залежно від приналежності об'єктів критичної інфраструктури. Розроблена методологія призначена для запобігання проявам несанкціонованого втручання в штатні режими функціонування об'єктів критичної інфраструктури та застосовується для прогнозування та запобігання

кризовим ситуаціям на об'єктах критичної інфраструктури унаслідок застосування кіберзброї недружніми до України державами або терористичними кіберугрупованнями. На основі розробленої методології синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури, принципово різних за своїми властивостями забезпечується безперервність виконання основних функцій інтелектуальними системами управління об'єктів критичної інфраструктури при одночасному гарантованому (заданому) рівні захищеності таких систем, що має критично важливе значення для подальшого розвитку галузі інформаційної безпеки держави в інтересах підвищення рівня національної безпеки України, забезпечення безпеки громадян, захисту їх прав та свобод.

Монографія складається з 6 глав. Перша глава присвячена теоретичним основам побудови багатоконтурних систем безпеки об'єктів критичної інфраструктури. Розглянуто особливості структури та функціонування таких об'єктів з точки зору забезпечення їх безпеки, обговорюються типи загроз та запроваджується їх формальна класифікація, описано загальну концепцію побудови багатоконтурних систем безпеки об'єктів критичної інфраструктури.

У другій главі обговорюються проблеми моделювання різноманітних процесів та об'єктів у системах безпеки. Зокрема, розглянуто динамічні моделі поведінки взаємодіючих та антагоністичних агентів, моделі безпеки на основі підходу Лотки-Вольтери, а також диференціально-ігрові моделі розподілених систем інформаційної безпеки.

Третя глава присвячена методам захисту інформаційних ресурсів об'єктів критичної інфраструктури. Обговорюються математичні моделі побудови несиметричних криптосистем на основі постквантових алгоритмів Мак-Еліса та Нідеррайтера, які дозволять забезпечити послуги безпеки в умовах постквантового періоду (появи повномасштабного квантового комп'ютера). Розглядаються різні конструкції алгеброгеометричних кодів, які можуть бути використано в програмно-апаратних (апаратних) засобах (застосунках) з низьким використанням енергомісткості, що дозволяє їх використання у будь-яких каналах зв'язку з урахуванням типу (міри секретності) інформаційних ресурсів.

Четверта глава присвячена інтелектуальним системам керування об'єктами та базами знань на основі штучних нейронних мереж. Обговорюються архітектури та алгоритми функціонування безперервних нейронних мереж, здатних визначати декілька рішень, стабільно-пластичні

нейронні мережі Хеммінга, Хебба та мережі на основі перцептрону, здатні розпізнавати нову інформацію та донавчатись. Розглянуті методи побудови баз знань на моделях нейромережевої асоціативної пам'яті, що дозволяють донавчатись та визначати кілька рішень.

У п'ятій главі розглядається проблема управління трафіком в інфокомунікаційних мережах об'єктів критичної інфраструктури. Обговорюється моделювання трафіку, створюваного інтегральними потоками даних, та процесу буферизації при управлінні таким трафіком. Також синтезована математична модель інтелектуального управління трафіком інфокомунікаційних мереж об'єктів критичної інфраструктури на комутаційних вузлах інфокомунікаційної мережі.

Шоста глава присвячена прикладним питанням побудови багатоконтурних систем захисту об'єктів критичної інфраструктури.

Монографія призначена для студентів старших курсів, аспірантів, інженерів та наукових працівників, чия професійна діяльність пов'язана з розробкою та експлуатацією інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури.

ГЛАВА 1.

ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ БАГАТОКОНТУРНИХ СИСТЕМ БЕЗПЕКИ

1.1. Об'єкти критичної інфраструктури: елементи, процедури, структура

Критична інфраструктура (CI – critical infrastructure) підтримує основні послуги, необхідні для функціонування складного сучасного суспільства. Серйозний збій в наданні таких послуг, як транспорт та енергетика, може зробити великі групи населення уразливими до нестачі продуктів харчування, електроенергії та палива, а також інших предметів першої необхідності. Залежність від своєчасних автоматизованих логістичних ланцюжків поставок також може погіршити наслідки. Об'єкти критичної інфраструктури формуються на основі об'єднання інформаційно-комунікаційних технологій комп'ютерних систем з елементами кіберпростору на основі технологій безпроводних мереж та мобільних Інтернет-технологій. Саме це поєднання дозволяє стверджувати, що такі системи відносяться до об'єктів критичної інфраструктури – сукупність взаємопов'язаних елементів, об'єднаних в єдине ціле, правильність функціонування та взаємодії яких значно впливає на кібернетичну безпеку держави протягом певного інтервалу часу.

До таких об'єктів також відносяться кіберфізичні та соціокіберфізичні системи на основі поєднання технологій кіберпростору та смарт технологій з бездротовими (мобільними) каналами зв'язку. На рис. 1.1 наведений взаємозв'язок структури об'єктів критичної інфраструктури, на прикладі організацій транспортного сектору.

Введемо такі дефініції:

Системи об'єктів критичної інфраструктури (ОКІ) – множина автоматизованих систем управління (диспетчеризації), які забезпечують взаємодію інформаційно-комунікаційних мереж (ІКС) ОКІ, Знищення / відмова у функціонуванні значно впливають на рівень інформаційної та / або кібербезпеки держави.

Інформаційні ресурси ОКІ (ІР) – інформаційні ресурси, що циркулюють в ІКС ОКІ модифікація і / або знищення яких може призвести до часткового або повного знищення ОКІ.

Конфіденційність (confidentiality) – захист ІР ОКІ від пасивних атак.

Конфіденційність системи ОКІ – властивість системи захисту інформації (СЗІ) ОКІ, яке забезпечує безпеку при передачі.

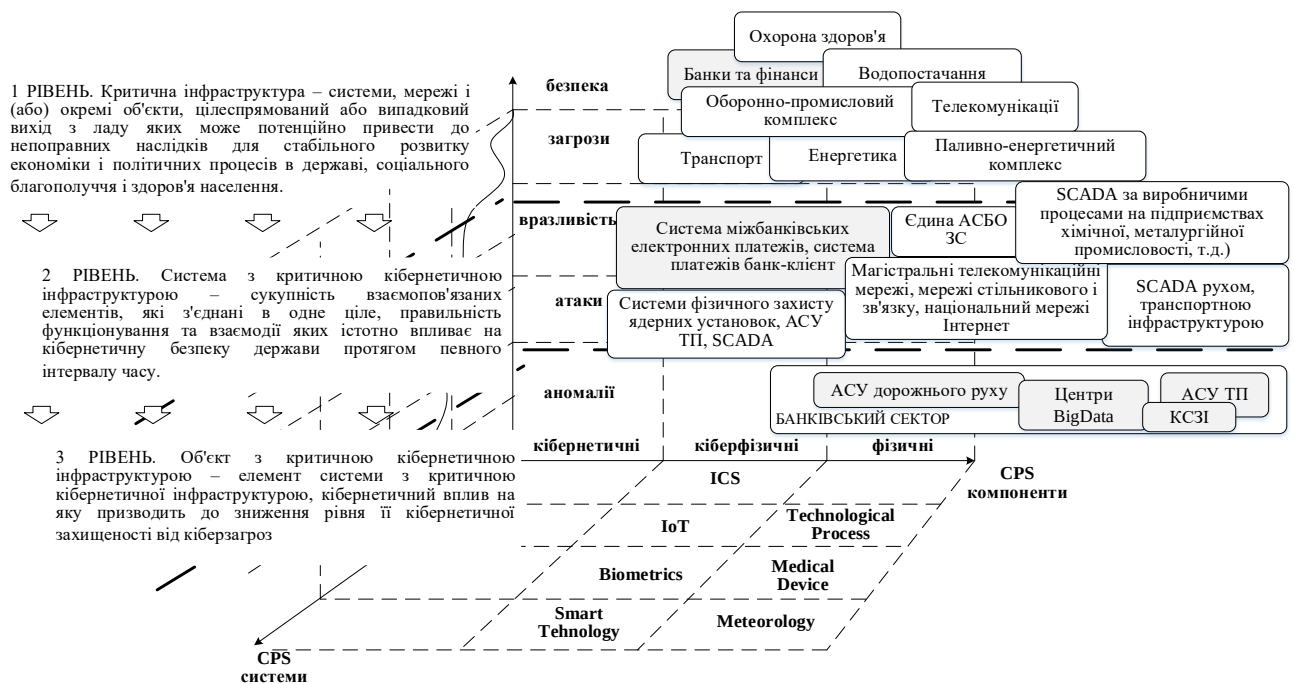


Рис.1.1. Схема взаємозв'язку структури об'єктів критичної інфраструктури на прикладі організацій транспортного сектору

Цілісність (integrity) – захист ІР ОКІ при зберіганні і / або модифікація ІР ОКІ тільки уповноваженим користувачем (процесом).

Цілісність системи ОКІ – властивість СЗІ ОКІ, яке забезпечує безпеку при зберіганні, та/або модифікацію ІР ОКІ тільки уповноваженим користувачем (процесом).

Доступність (availability) – доступ до ІР ОКІ уповноваженого користувача.

Доступність системи ОКІ – властивість СЗІ, яке забезпечує відповідний встановленої моделлю безпеки доступ до ІР без обмежень.

Автентичність (authenticity) – підтвердження достовірності ІР ОКІ. – властивість СЗІ, яке забезпечує справжність джерела інформації.

Структура системи кібербезпеки повинна здійснювати такі функції:

- збір та комплексування інформації про потенційні загрози та джерела їх реалізації;
- обробку та зберігання цієї інформації з прийнятними ступенями агрегації;
- автоматичну та (або) людино-машинну оцінку станів рівня захищеності та середовища функціонування бізнес-процесів з прогнозуванням появи нових типів загроз;
- автоматичний та (або) людино-машинний пошук рішень щодо вибору засобів протидії, що ініціюється оцінками станів об'єкта, що захищається,

та середовища його функціонування, а також несприятливими прогнозами тенденцій розвитку кіберзагроз;

- автоматичну та (або) людино-машинну оптимізацію з точки зору коштів, що витрачаються, і часу знайдених і рекомендованих рішень;
- людино-машинне прийняття рішень з можливостями виклику для аналізу як даних, що лежали в основі пошуку запропонованих рішень щодо протидії кібератакам, так і використовуваної логіки та математичних методів, на яких базувався пошук запропонованих рішень.

Передбачається, що органу управління відомо:

- не завжди певна множина параметрів $\{x\}$, що характеризують поточний стан об'єктів критичної інфраструктури та середовища протистояння;
- множина способів розбиття $\{x\}$ на класи станів $K=\{k_1, k_2, \dots, k_z\}$, які вимагають прийняття рішень;
- множина моделей пошуку рішень $\{M\}$;
- множина механізмів пошуку рішень на моделях – $\{\pi\}$.

При реалізації такої схеми динамічно формуються множини $\{k\}$ і $\{M\}$, з можливості дозволяють отримувати необхідні рішення в прийнятні терміни, проте характер рішень – якісний.

Забезпечення необхідного рівня кібербезпеки контуру бізнес-процесів розглядатимемо як людино-машинну діяльність з визначення станів об'єкта, що захищається, що вимагає прийняття рішень, пов'язаних з пошуком і вибором шляхом цілеспрямованої координації моделей поведінки всіх учасників кіберконфлікту, закладених у комп'ютер – M_1 та існуючої у ОІПР – M_2 . Таке модельне уявлення визначається накопиченими знаннями про методи та механізми забезпечення кібербезпеки, цілями та обмеженнями кожної із сторін, об'єктивних та суб'єктивних переваг щодо вибору шляхів досягнення цілей та оцінки ступеня їх застосування. Інтерактивність взаємодії людини з системою організується шляхом введення поняття людино-машинної ситуації, що вимагає прийняття рішень S_y та визначає це поняття множини атрибутів. Характер цієї діяльності, з одного боку, задається людиною шляхом управління процесами постановки завдання стеження за перебігом її вирішення. З іншого боку, система уточнює коректність поставлених завдань, пропонує альтернативні шляхи їх вирішення, використовуючи «знання та досвід» пошуку рішень, відображений у своїй моделі. Таким чином, людина та система взаємодіють як партнери, які узгоджують свої методи вирішення завдань забезпечення кібербезпеки необхідного рівня. Симбіоз буде оптимальним лише тоді, коли робота системи організується в режимі

«інтелектуального» порадника людини, здійснюючи рутинні функції автоматичного розпізнавання атак, а також пошуку засобів протидії на основі інформації, отриманої як від експертів, так і з використанням системних знань. Ці знання існують у системі у вигляді двох видів структурованих множин {обчислювальних та теоретико-множинних}, {діалогових та експертних (логіко-алгебраїчних та логіко-лінгвістичних)} моделей розпізнавання кібератаки та пошуку засобів протидії їй. Перший вид моделей визначений на ситуаціях, для яких може бути знайдений алгоритм, що пов'язує шукані параметри із заданими, і перебір варіантів не дуже великий. Другий тип моделей використовується для пошуку рішень, які сильно залежать від ситуацій і де пошук надзвичайно великий. Можна сказати, що обчислювальні та теоретико-множинні моделі є аналогами обчислювальних операцій при пошуку рішень, а діалогові та експертні – аналогами методів пошуку рішень.

Формальне уявлення моделі поведінки ОПР при оперативному прийнятті рішень задається виразом:

$$MI = \langle BT, DM, IT \rangle,$$

де

$BT = \langle L_{BT}, ACS, \Theta \rangle$ – теорія поведінки (модель знань системи);

$DM = \langle x_z, b_z, f_z, p_z \rangle$ – інформаційна модель даних, що описує систему;

$I = \langle UI_1, CI_2 \rangle$ – інтерпретація BT у DM .

Тут $L_{BT} = L_{KDL} \cup L_{DDL}$ – мова опису моделі поведінки, що є об'єднанням мов визначення знань і даних; ACS – аксіоми теорії; Θ – правила виведення тверджень у теорії; x_z, b_z – множина змінних та констант стану; f_z, p_z – множина функціональних і предикатних змінних стану; UI_1 – користувальницька інтерпретація елементів моделі знань системи, що задає експертно відповідність правила встановлення відповідності між синтаксичною структурою елементів мови L_{BT} та їх змістом у галузі кібербезпеки (семантика ОПР); CI_2 – машинна інтерпретація елементів, що задає експертно алгоритм встановлення відповідності між семантичною структурою елементів мови L_{BT} та їх істинністю в кожний момент пошуку рішень (прагматика області кібербезпеки).

Формальна модель поведінки учасника кіберконфлікту залежно від обмежень, що накладаються на правила виведення тверджень Θ , може бути описана засобами логіки предикатів першого порядку, продукційних та алгоритмічних систем. Справді, у логіці предикатів немає обмежень

застосування правил виведення. До будь-якого вже виведеного твердження підходить будь-яке правило виведення, якщо це твердження допускає його використання. У продукційних системах, що базуються також на логіці предикатів, є додаткові умови на застосування того чи іншого правила виведення. Ці умови можуть змінюватися у процесі функціонування продукційної системи залежно від отримання тієї чи іншої інформації у процесі виведення. У алгоритмічних системах послідовність застосування правил визначено однозначно. Як мову опису теорії управління застосовано мову логіки предикатів першого порядку та мову алгоритмів обробки інформації. Як правила виведення тверджень у теорії обрані правила виведення в логіці предикатів, їх модифікації в системі продукцій та алгоритмічні правила.

Зв'язок моделі поведінки з проблемними ситуаціями і що виникають при їх появі завданнями пошуку рішень досягається шляхом урахування логічної послідовності етапів роботи ОПР при забезпеченні безпеки контуру бізнес-процесів та виділення множини процедур прийняття рішень, характерних для ОПР. Вказана множина процедур може бути представлена у вигляді наступної послідовності [1–3]:

процедура класифікації ситуацій:

$$\pi_1 = \langle S, J, K_p, K_s \rangle,$$

де S – ситуація, що задається деяким ставленням на множині елементів I ; J – множина експертних переваг щодо вибору правил класифікації, задане на множині $\{S \times K_s\}$; K_p – множина правил класифікації – вирішальних процедур; K_s – множина класів ситуацій, для яких існують моделі пошуку рішень;

процедура модельної класифікації дозволяє визначити множину моделей прийняття рішень, організуючи обчислення на яких можна знайти необхідні рішення щодо забезпечення необхідного рівня кібербезпеки:

$$\pi_2 = \langle S, K_s, Al, M_1 \rangle,$$

де Al – множина альтернатив вибору моделей пошуку рішень, вагові коефіцієнти яких залежать від S і K_s , може задаватися людиною в інтерактивному режимі роботи з системою; M_1 – множина моделей пошуку рішень;

процедура формування стратегій мети пошуку рішень дозволяє визначити множина локальних та (або) глобальних цілей системи кібербезпеки, які необхідно досягти за допомогою рішень, знайдених у даному класі ситуацій:

$$\pi_3 = \langle S, K_s, G, Cr, Str \rangle,$$

де G – множина поточних цілей, що стоять перед системою, що управляє; Cr – множина критеріїв досягнення цілей (і цілі, і критерії можуть змінюватись з часом); Str – множина стратегій мети пошуку рішень;

процедура пошуку цільових керуючих рішень дозволяє організовувати пошук рішень для кожної з проблемних ситуацій відповідно до цілей та критеріїв забезпечення безпеки контуру бізнес-процесів:

$$\pi_4 = \langle S, Str, M_1, RG \rangle,$$

де RG – множина цільових керуючих рішень, які можуть бути знайдені в моделі пошуку рішень (базі знань) M_1 , налаштованої на поточну ситуацію $s_i \in S$ при використанні стратегії Str_i . Ця процедура виконує дві функції – планувальника обчислювальної послідовності пошуку рішень та вирішувача. Перша функція полягає у формуванні вирішальної послідовності програм, друга - в організації виконання цих програм та отримання керуючих рекомендацій у конкретному обчислювальному середовищі;

процедура визначення можливих результатів реалізації рішень дозволяє задати досяжність локальних та (або) глобальних цілей управління при реалізації тих чи інших рішень щодо протидії кібератакам. Це виконується шляхом організації обчислень на моделі допустимої області прийняття рішень – M_{ODA} , визначення цієї галузі - O_{OD} , відповідно до цілей G та критеріїв – Cr , характерних для даного рівня прийняття рішень. Ця процедура задається:

$$\pi_5 = \langle S, RG, G, Cr, M_{ODA}, O_{OD}, RG_1 \rangle,$$

де RG_1 – множина тих управляючих рішень, які є задовільними наслідками, тобто. наслідками, при реалізації яких можуть бути досягнуті локальні та (або) глобальні цілі управління;

процедура обґрунтування рішень дозволяє оцінити якість рішень (їх оптимальність) шляхом організації обчислень на моделі визначення

оптимальної області прийняття рішень (M_{ODA}) для вибору області оптимальних керуючих рішень (O_{OD}) відповідно до цілей та критеріїв. Елемент кортежу RG_1 є множиною тих керуючих рішень, які задовольняють O_{OD} і можуть бути рекомендовані для реалізації. Ця процедура:

$$\pi_6 = \langle S, RG_1, G, Cr, M_{ODA}, O_{OD}, RG_2 \rangle;$$

процедура синтезу рішень дозволяє зменшити кількість одночасно рекомендованих рішень щодо протидії незалежно від того, скільки ситуацій одночасно аналізується системою. Крім того, процедура ранжує видані ОПР рішення як за інформацією, отриманою від процедур π_5, π_6 , так і користуючись безліччю переваг «звуження» множини RG . Ці переваги можуть задаватися експертно. Процедура задається у вигляді:

$$\pi_7 = \langle S, RG_2, O_{ACD}, O_{ODR}, R \rangle.$$

Інформація для ОПР після роботи цієї процедури видається як $\{\{S\} \Rightarrow \{R, O_{ACD}, O_{ODR}\}\}$. ОПР може пов'язати поточну ситуацію з необхідними рішеннями з урахуванням їхньої належності до O_{ACD} або O_{ODR} , задаючи RG_2 ;

процедура вибору рішень дозволяє організувати процес чоловіко-машинної взаємодії з метою прийняття одного рішення, яке підлягає реалізації. При цьому ОПР може вибрати один із рекомендованих системою засобів протидії або прийняти своє, відмінне від рекомендованих, RG , про що він повинен повідомити систему. Якщо $R_G \cap \bar{R} = 0$, то це рішення може бути реалізовано. Тут $\bar{R} = R_G \cap R_{G1} \cap R_{G2}$ – заборонена множина рішень. Формально ця процедура:

$$\pi_8 = \langle S, R, \bar{R}, R_G \rangle,$$

процедура оцінки результатів реалізації рішень дозволяє оцінювати ефективність прийнятих та реалізованих рішень з метою корекції (у режимі навчання або самонавчання) моделі знань системи та перекладу частини інформації виду $\{\langle \text{ситуація} \rangle \rightarrow \langle \text{рішення} \rangle\}$ із сфери системи прийняття рішень у сферу автоматичної реалізації рішення. Ця процедура:

$$\pi_9 = \langle S, R \cup RG, M_1, \pi_{13} \rangle,$$

де π_{13} – процедура навчання (самонавчання) системи та корекції її моделі знань M_1 ;

процедура трасування рішень дозволяє організувати стеження за логікою логічного виводу при пошуку рішень та використовуваному при цьому інформаційному базисі. Ця процедура повертає ОПР якість спостережуваності, тобто можливість встановлення будь-яких відносин на елементах процедур ухвалення рішень. Процедура трасування будується на основі модифікації впорядкованої послідовності π_1 - π_9 – процедур. Модифікація полягає у введенні у кожну процедуру π_i твердження про правильність отримання за її допомогою результатів. Формально ця процедура:

$$\pi_{10} = \langle \mu_1: \pi_1, \mu_2: \pi_2, \dots, \mu_9: \pi_9, Cor \rangle,$$

де $\mu_1, \mu_2, \dots, \mu_9$ – умови виконання (ствердження про правильність) процедур $\pi_1, \pi_2, \dots, \pi_9$ відповідно, записані у вигляді $\mu_i: \pi_i$. За допомогою елементів цього кортежу людина має можливість шляхом взаємодії із системою психологічно повірити у правильність знайдених рішень. Твердження, що належать Cor , визначають узгодженість логіки, закладеної основою моделей і процедур комп'ютера і ОПР, тобто. вони дозволяють системі повідомляти ОПР про те, що черговий цикл пошуку та прийняття рішень завершено;

процедура інформаційного діалогу організовує людине-машинну взаємодію ОПР із системою з метою отримання необхідної йому інформації. Ця процедура $\pi_{11} = \langle \pi_1, \pi_2, \pi_3, \pi_4 \rangle$, де $\pi_1, \pi_2, \pi_3, \pi_4$ – розглядаються процедури, в яких були зроблені наступні заміни: $R/R_0, M_1/M_A, C/C_D, G/G_D; R_D$ – множина запитів від ОПР; $M_A \in M_1$ – множина моделей пошуку відповіді з областей визначення запитів; Str_D – множина стратегій мети пошуку рішень, ранжованих за множиною M_A ; G_D – множина поточних цілей; R_0 – множина відповідей, що видаються ОПР при реакції системи на запит;

процедура визначення інформаційного базису для прийняття рішень здійснює зв'язок із системою збору інформації з метою організації обробки цієї інформації та запису її в інформаційну модель (базу даних) систем. Формально ця процедура:

$$\pi_{12} = \langle S, \pi_1, \pi_2, \pi_3, \pi_4, M_1, MD \rangle,$$

де MD – інформаційна модель, що зберігає поточний стан об'єкта.

процедура адаптації/навчання до зволяє організувати автоматизоване налаштування системи на область забезпечення кіберзахисту. Ця процедура:

$$\pi_{13} = \langle LL, E_K, E_D \rangle,$$

де LL – механізм корекції моделей баз знань та даних (засобів опису знань та даних), що дозволяє пов'язувати інформацію в її машинному поданні;

E_K, E_D – множина елементів рівня моделі знань та даних.

процедура автоматизованого проектування, або інакше, діалогова система автоматизованого проектування системи кібербезпеки. Для ОПР та системних аналітиків-проектувальників це процедура:

$$\pi_{14} = \langle S, L_{DKL}, L_{DML}, L_{DDL}, M_{Comp} \rangle,$$

де S – проектна ситуація з класу ситуацій людино-машинного проектування, що відображає предметно-орієнтовану постановку завдання побудови інформаційно-модельного базису; $L_{DKL}, L_{DML}, L_{DDL}$ мовні засоби опису елементів модельного базису знань та даних; M_{Comp} – машинне уявлення інформаційно-модельного базису.

1.2. Загрози безпеці об'єктам критичної інфраструктури. Класифікатор загроз як формальне подання типів та властивостей кіберзагроз

Аналіз оцінки тенденцій розвитку змішаних загроз (цільових атак) показав, що вектор загроз “клонує” попит цифровізації послуг та еволюційний розвиток як обчислювальної техніки, так і тенденцій розвитку технологій. В першу чергу, це стосується появи соціокіберфізичних систем, і їх спектром цифрових послуг, появи повномасштабних квантових комп'ютерів – в другу.

З урахуванням відкритості елементів систем ОКІ, використання кіберпростору, як основного “каналу” взаємозв'язків між елементами структури в умовах постквантового періоду такі системи схильні до цільових атак на основі комплексування загроз на окремі складові безпеки з урахуванням ознак гібридності та синергізму та можливості комплексування з методами соціальної інженерії. На рис. 1.2 наведено структурну схему моделі загроз.

Для визначення об'єктивності експертної оцінки та автоматизації розроблений веб-застосунок (<https://skl.sspu.sumy.ua/login>), який дозволяє

формувати експертну оцінку впливу загрози на послугу безпеки. Запропоновано визначити узгодженість димок експертів з різною мірою знань у галузі кібербезпеки та захисту інформації.

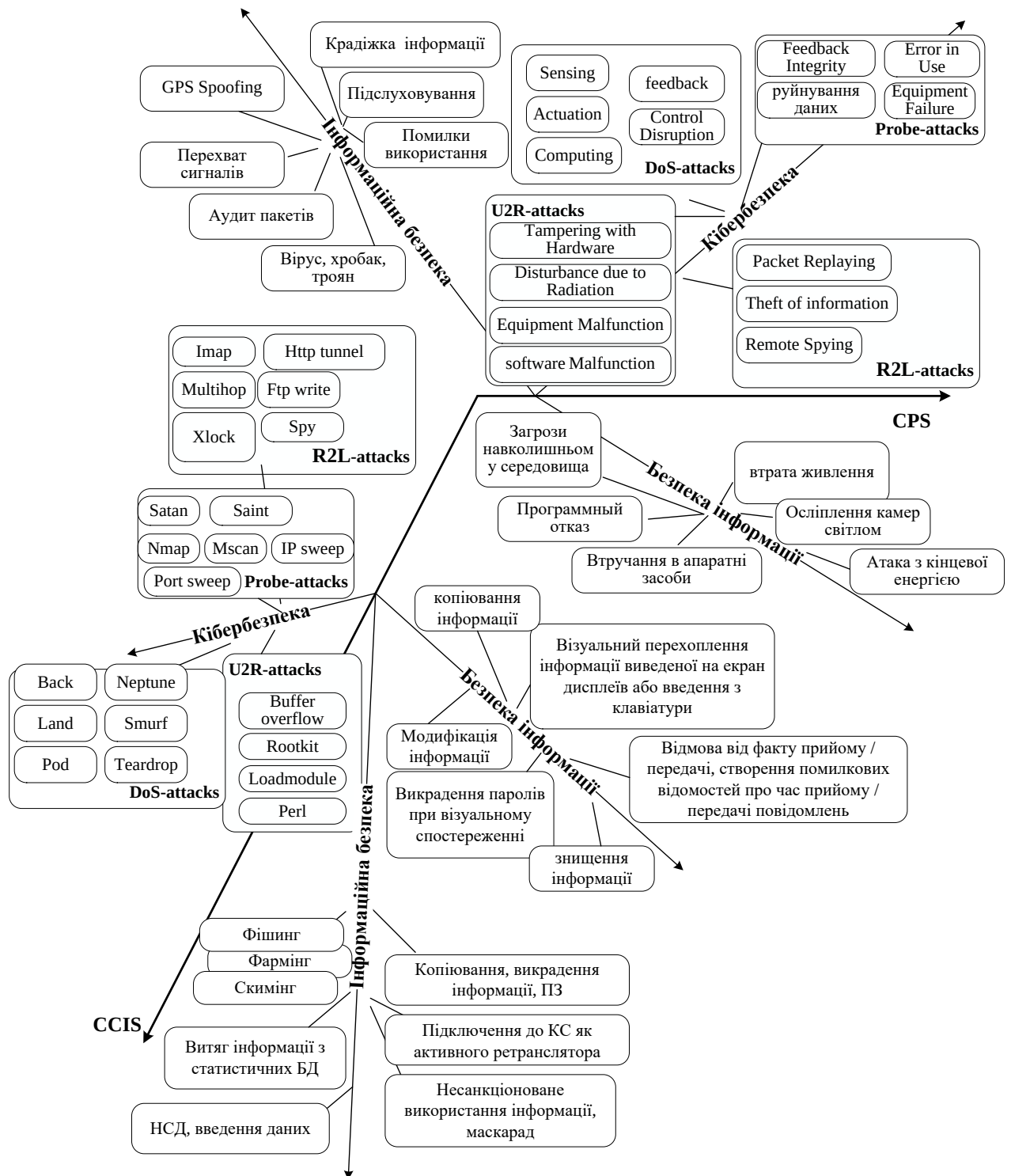


Рис. 1.2. Структурна схема синергетичної моделі загрози синтезу на SCADA

У табл.1.1 наведено основні характеристики бездротових мобільних та комп'ютерних мереж та послуги безпеки.

Таблиця 1.1

Порівняльні характеристики бездротових та мобільних Інтернет-технологій

Технологія	Забезпечення послуг безпеки					Ступінь секретності інформації (β_i)				
	C	I	A	A _ц	B	1,0	0,75	0,5	0,25	0,01
<i>LTE (4G), LTE (5G)</i>	–	–	+	–/+	–/+	–	–	–	–	–
<i>IEEE 802.11 ac (Wi-Fi 5)</i>	–	–	+	–/+	–/+	–	–	–	–	–
<i>IEEE 802.11ax, Wi-Fi 6+KNX</i>	–/+	–/+	+	–/+	–/+	–	–	–	+	+
<i>IEEE 802.16+KNX</i>	–/+	–/+	+	–/+	–/+	–	–	–	+	+
<i>IEEE 802.16m (WiMAX2)</i>	–/+	–/+	+	–/+	–/+	–	–	–	+	+
<i>IEEE 802.15.1 Bluetooth 5+KNX</i>	–/+	–/+	+	–/+	–/+	–	–	–	+	+
<i>IEEE 802.15.4+KNX</i>	–/+	–/+	+	–/+	–/+	–	–	–	+	+

Аналіз табл. 1.1 показує, що в умовах появи повномасштабного квантового комп'ютера послуги у внутрішньому контурі безпеки ставляться під сумнів через квантові алгоритми злому симетричних і несиметричних алгоритмів. Крім цього, у мобільних технологіях на основі протоколу DEA забезпечуються лише послуги 3A (авторизація, ідентифікація, автентифікація).

У сучасних умовах гібридності та синергізму кібератак це дозволяє безперешкодно отримувати несанкціонований доступ як у внутрішній, так і зовнішній контури безпеки та практично реалізовувати цільові атаки на ОКІ. Також застосування класичних (симетричних) криптосистем на основі блокових та поточкових шифрів (які використовуються у стандарті KNX) не забезпечують послуги конфіденційності та цілісності у повному обсязі.

Аналіз оцінки тенденцій розвитку змішаних загроз (цільових атак) показав, що вектор загроз “клонує” попит цифровізації послуг та еволюційний розвиток як обчислювальної техніки, так і тенденцій розвитку технологій. В першу чергу, це стосується появи соціокіберфізичних систем, і їх спектром цифрових послуг, появи повномасштабних квантових комп'ютерів – в другу. Таким чином, пропонується загальний підхід універсалізації побудови класифікаторів загроз ОКІ, який враховує не тільки напрям цільових атак, а також визначає критичні точки інфраструктури ОКІ, можливості загроз комплексувати з методами соціальної інженерії.

Крім того запропонований веб-застосунок, враховує всі складові класифікатору загроз, який наведений на рис. 1.3.

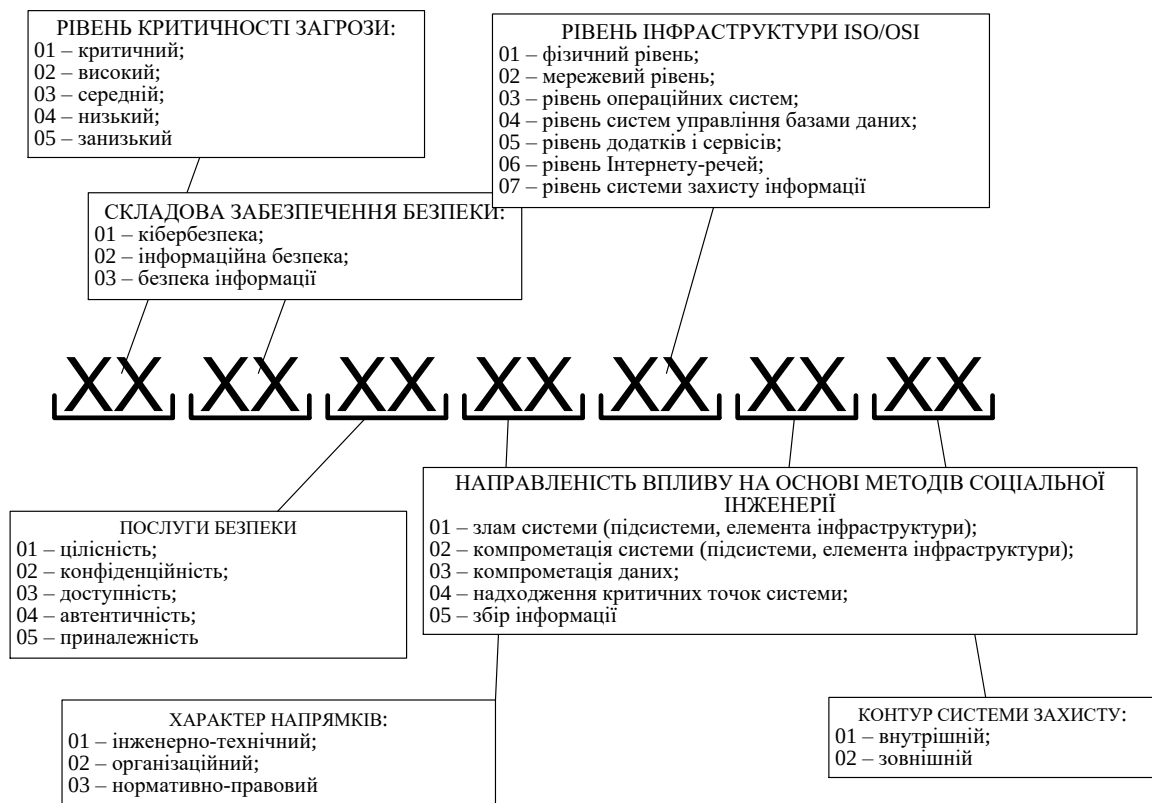


Рис. 1.3. Класифікатор загроз соціокіберфізичних систем

Запропонований класифікатор загроз соціокіберфізичних систем дозволяє враховувати ознаки синергізму та гібридності цільових (змішаних) атак, можливість їх комплексування з методами соціальної інженерії.

Такий підхід дозволяє формувати вимоги та будувати многоконтурні системи захисту інформації з урахуванням платформеності (структури) соціокіберфізичних систем.

1.3. Концепція синтезу моделей різних типів та призначення

Для формування многоконтурної системи захисту інформації запропонований наступний математичний апарат побудови многоконтурних систем безпеки, в якому враховані ознаки синергізму та гібридністю змішаних та цільових атак на кожну з платформ соціокіберфізичних систем (на внутрішній та зовнішній контури).

– *загрози внутрішнього контуру з урахуванням гібридності та синергізму загроз для 1 платформи – соціальні мережі:*

$$\begin{aligned}
Q_{\text{hybrid } C, I, A, Au, Af \text{ synerg}_{1\text{platform}}}^{SCS \text{ ISL}} &= \left(Q_{\text{synerg}_{1\text{platform}}}^{SCS \text{ ISL } C} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \\
&\cap \left(Q_{\text{synerg}_{1\text{platform}}}^{SCS \text{ ISL } I} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{1\text{platform}}}^{SCS \text{ ISL } A} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \\
&\cap \left(Q_{\text{synerg}_{1\text{platform}}}^{SCS \text{ ISL } Au} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{1\text{platform}}}^{SCS \text{ ISL } Inv} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right), \quad (1.1)
\end{aligned}$$

де $Q_{\text{synerg}_{1\text{platform}}}^{SCS \text{ ISL } i}$ – синергія загроз на відповідну послугу безпеки; α_i – ваговий коефіцієнт можливості реалізації загрози на основі методів соціальної інженерії, $i \in \{0,25; 0,5; 0,75; 1,0\}$, де 0,25 – ймовірність використання загрози на основі методів соціальної інженерії 1 раз на рік (низький рівень); 0,5 – ймовірність використання загрози на основі методів соціальної інженерії 1 раз на місяць (середній рівень); 0,75 – ймовірність використання загрози на основі методів соціальної інженерії 1 разів на тиждень (високий рівень), 1,0 – ймовірність використання загрози на основі методів соціальної інженерії 1 раз на день (критичний рівень).

– загрози внутрішнього контуру з урахуванням гібридності та синергізму загроз для 2 платформи – кіберпростір:

$$\begin{aligned}
Q_{\text{hybrid } C, I, A, Au, Af \text{ synerg}_{2\text{platform}}}^{SCS \text{ ISL}} &= \left(W_{\text{synerg}_{2\text{platform}}}^{SCS \text{ ISL } C} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \\
&\cap \left(Q_{\text{synerg}_{2\text{platform}}}^{SCS \text{ ISL } I} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{2\text{platform}}}^{SCS \text{ ISL } A} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \\
&\cap \left(Q_{\text{synerg}_{2\text{platform}}}^{SCS \text{ ISL } Au} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{2\text{platform}}}^{SCS \text{ ISL } Inv} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right), \quad (1.2)
\end{aligned}$$

– загрози внутрішнього контуру з урахуванням гібридності та синергізму загроз для 3 платформи – кіберфізичні системи:

$$\begin{aligned}
Q_{\text{hybrid } C, I, A, Au, Af \text{ synerg}_{3\text{platform}}}^{SCS \text{ ISL}} &= \left(Q_{\text{synerg}_{3\text{platform}}}^{SCS \text{ ISL } C} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \\
&\cap \left(Q_{\text{synerg}_{3\text{platform}}}^{SCS \text{ ISL } I} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{3\text{platform}}}^{SCS \text{ ISL } A} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \\
&\cap \left(Q_{\text{synerg}_{3\text{platform}}}^{SCS \text{ ISL } Au} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{3\text{platform}}}^{SCS \text{ ISL } Inv} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right), \quad (1.3)
\end{aligned}$$

Загальна оцінка загроз на внутрішній контур за всіма платформами складає:

$$Q_{ISL}^{SCS} = W_{\text{hybrid } C, I, A, Au, Af \text{ synerg}_{1\text{platform}}}^{SCS \text{ ISL}} \cup Q_{\text{hybrid } C, I, A, Au, Af \text{ synerg}_{2\text{platform}}}^{SCS \text{ ISL}} \cup Q_{\text{hybrid } C, I, A, Au, Af \text{ synerg}_{3\text{platform}}}^{SCS \text{ ISL}} \cdot \quad (1.4)$$

Загрози на зовнішній контур по кожній з платформ визначаються:

– загрози зовнішнього контуру з урахуванням гібридності та синергізму для 1 платформи – соціальні мережі:

$$Q_{\text{hybrid } C, I, A, Au, Af \text{ synerg}_{1\text{platform}}}^{SCS \text{ ESL}} = \left(Q_{\text{synerg}_{1\text{platform}}}^{SCS \text{ ESL } C} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{1\text{platform}}}^{SS \text{ ESL}} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right)^I \cap \left(Q_{\text{synerg}_{1\text{platform}}}^{SCS \text{ ESL}} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right)^I \cap \left(Q_{\text{synerg}_{1\text{platform}}}^{SCS \text{ ESL } A} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{1\text{platform}}}^{SCS \text{ ESL } Au} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{1\text{platform}}}^{SCS \text{ ESL } Inv} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right), \quad (1.5)$$

– загрози зовнішнього контуру з урахуванням гібридності та синергізму для 2 платформи – кіберпростір:

$$Q_{\text{hybrid } C, I, A, Au, Af \text{ synerg}_{2\text{platform}}}^{SCS \text{ ESL}} = \left(Q_{\text{synerg}_{2\text{platform}}}^{SCS \text{ ESL } C} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{2\text{platform}}}^{SCS \text{ ESL } I} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{2\text{platform}}}^{SCS \text{ ESL } A} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{2\text{platform}}}^{SCS \text{ ESL } Au} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{2\text{platform}}}^{SCS \text{ ESL } Inv} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right), \quad (1.6)$$

– загрози зовнішнього контуру з урахуванням гібридності та синергізму для 3 платформи – кіберфізичні системи:

$$Q_{\text{hybrid } C, I, A, Au, Af \text{ synerg}_{3\text{platform}}}^{SCS \text{ ESL}} = \left(Q_{\text{synerg}_{3\text{platform}}}^{SCS \text{ ESL } C} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{3\text{platform}}}^{SCS \text{ ESL } I} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{3\text{platform}}}^{SCS \text{ ESL } A} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{3\text{platform}}}^{SCS \text{ ESL } Au} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right) \cap \left(Q_{\text{synerg}_{3\text{platform}}}^{SCS \text{ ESL } Inv} \cup \sum_{i=1}^5 S_i^{\text{sthreats}} \times \alpha_i \right), \quad (1.7)$$

Загальна оцінка загроз на зовнішній контур за всіма платформами складає:

$$Q_{ESL}^{SCS} = Q_{\text{hybrid } C, I, A, Au, Af \text{ synerg}_{1\text{platform}}}^{SCS \text{ ESL}} \cup \bigcup Q_{\text{hybrid } C, I, A, Au, Af \text{ synerg}_{2\text{platform}}}^{SCS \text{ ESL}} \cup Q_{\text{hybrid } C, I, A, Au, Af \text{ synerg}_{3\text{platform}}}^{SCS \text{ ESL}} \quad (1.8)$$

Загальна оцінка загроз на многоконтурну систему захисту інформації визначається:

$$Q_{\text{final}}^{CPSS} = Q_{ISL}^{CPSS} \cup Q_{ESL}^{CPSS}. \quad (1.9)$$

На основі запропонованого підходу щодо оцінки потокового стану захищеності елементів системи (інфраструктури) пропонується наступна методика оцінки захищеності соціокіберфізичних систем:

1 етап. Формування експертних оцінок загроз, їх вплив на послуги безпеки, можливість ознак синергізму та гібридності, а також комплексування з методами соціальної інженерії. Визначення впливу загрози на рівень інфраструктури (моделі ISO/OSI). При цьому формується матриця вагових коефіцієнтів $S_{\text{stheats}}^* = \|S_{\text{stheats}_{ij}}\|$, де i – послуги безпеки, j – відповідна загроза, $j \in \overline{1 \dots N}$.

2 етап. Формування матриці відповідності між інформаційними ресурсами та послугами безпеки: $S_{\text{inf}}^* = \|S_{\text{inf}_{il}}\|$, де i – послуги безпеки, l – інформаційний ресурс, $l \in \overline{1 \dots L}$. При заповненні матриці враховується необхідність надання відповідної послуги безпеки (1 – послуга потрібна, 0 – послуга не потрібна).

3 етап. Формування залежності між інформаційними ресурсами та рівнями інфраструктури (моделі ISO/OSI), де циркулює та/або зберігається інформація: $S_{\text{ISO}}^* = \|S_{\text{ISO}_{kl}}\|$, де k – наявність і тип зв'язку, елемент інфраструктури (рівень) де зберігається інформація, l – інформаційний ресурс, $l \in \overline{1 \dots L}$.

4 етап. Формування залежності загроз та інформаційних ресурсів (оцінка критичності інфраструктури): $S_{\text{inf/stheats}}^* = \|S_{\text{inf}_{lj}}\|$, де l – інформаційний

ресурс, $l \in \overline{\forall 1 \dots L}$, j – відповідна загроза, $j \in \overline{\forall 1 \dots N}$. Етап дозволяє визначити критичність несанкціонованого доступу до того чи іншого інформаційного ресурсу

5 етап. Формування залежності загроз та елементів інфраструктури (рівень моделі ISO/OSI):

$S_{\text{streats}/\text{ISO}}^* = \|S_{\text{streats}/\text{ISO}_{kj}}\|$, де k – наявність і тип зв'язку, елемент інфраструктури (рівень) де зберігається інформація, j – відповідна загроза, $j \in \overline{\forall 1 \dots N}$. Етап дозволяє визначити критичні точки у інфраструктурі та заздалегідь визначити превентивні заходи безпеки.

6 етап. Формування оцінки захищеності соціокіберфізичної системи на основі аналізу 2 та 3 етапів (знаходження зв'язку між інформаційними ресурсами, елементами інфраструктури (критичними точками несанкціонованого доступу/витоку інформації) та послугами безпеки.

7 етап. Формування оцінки можливостей діючої системи захисту інформації протистояти загрозам:

$S_{\text{streats}/\text{protection system}}^* = \|S_{\text{streats}/\text{protection system}_{qj}}\|$, де q – наявність механізму протидії загрозі, j – відповідна загроза, $j \in \overline{\forall 1 \dots N}$.

8 етап. Формування оцінки регуляторів та законодавчих актів.

9 етап. Формування оцінки потокового стану системи безпеки. При цьому враховуються результати етапів 7–9.

Таким чином запропонована методика дозволяє враховувати відповідні критерії класифікатора загроз соціокіберфізичних систем, потоковий стан системи захисту та виконання керівництвом (в першу чергу) вимог міжнародних регуляторів, та законодавчих актів держави.

1.4. Система управління як система з критичною кіберінфраструктурою

Виходячи з тих міркувань, що система управління незалежно від її цільового призначення та природи походження, виступає базовою основою будь-якої кіберсистеми, то сукупність усіх кіберсистем які існують у живій і неживій природі та зав'язків між ними в загальному вигляді можна подати моделлю неорієнтованого графа (рис. 1.4).

Рис. 1.5. Графова модель ланцюгової реакції при взаємодії кіберсистем в умовах кібервпливу на об'єкти з критичною кіберінфраструктурою

Зважаючи на виняткову цінність з позиції безпеки процесів управління в системі управління або системах управління, стає зрозуміло, що кіберсистеми з критичною кіберінфраструктурою виступають ключовим елементом у забезпеченні їх кібербезпеки. Таким чином, об'єкти з критичною кіберінфраструктурою мають власну мережеву архітектуру, яку в подальшому називатимемо критичною [55, 56]. Вирішення проблеми забезпечення кібербезпеки систем з критичною кіберінфраструктурою неминуче пов'язано з виявленням власне таких систем, їх обліком та аудитом, що ґрунтується на відповідній методології [59, 83, 99]. Особливе місце в системі критичної інфраструктури будь-якої держави світу (табл. 1.2), у т.ч. й України займає кіберінфраструктура, ефективний захист якої виступає необхідним елементом забезпечення їх національної безпеки. Кіберінфраструктура охоплює множина елементів (підсистем) критичної інфраструктури держави [57, 67–74, 76]. Разом з тим до сьогодні й досі в світі немає єдиного усталеного тлумачення згаданої категорії [94].

Таблиця 1.2

Порівняльна таблиця критичних інфраструктур на прикладі деяких провідних держав світу

ДЕРЖАВА СЕКТОР КРИТИЧНОЇ ІНФРАСТРУКТУРИ	Велика сімка						Австрія	Австрія	Нідерланди	Нова Зеландія	Норвегія	Польща	Фінляндія	Швеція
	США	Японія	Німеччина	Велика Британія	Франція	Італія	Канада							
Банки та фінанси														
Водопостачання														
Дамби														
Енергетика														
Комунальні мережі														
Національні символи														
Небезпечні матеріали (Х, Б, Р, Я)														
Оборонно-промисловий комплекс														
Органи виконавчої влади														
Органи судової влади														
Охорона здоров'я														
Паливно-енергетичний комплекс														
Поштові служби														
Сільське господарство														
Система управління повітряним рухом														
Служби охорони громадського порядку														
Служби екстр. допомоги та реагування на НС														
Телекомунікації														

Таким чином, з аналізу критичних інфраструктур на прикладі держав, перелік яких подано у табл. 1.2, встановлено: найбільш вразливими критичними інфраструктурами є об'єкти, що належать до банківської та фінансової сфер, енергетики та телекомунікацій [58]. Тому Україні в умовах триваючої збройної агресії слід зосередити зусилля на покращенні питань кіберзахисту саме тих об'єктів, які належать до згаданого вище сектору.

На прикладі інформаційних, комунікаційних та інформаційно-комунікаційних систем покажемо принцип формування в Україні об'єктів з критичною кіберінфраструктурою. В основу згаданого принципу покладемо ознаковий підхід [92], що ґрунтується на таких основних критеріях як: категорія інформації управління, що циркулює в кіберсистемі (відкрита або з інформація з обмеженим доступом); призначення кіберсистеми; прогнозований рівень втрат у різі стороннього кібервпливу на систему; прогнозований рівень настання суспільно-небезпечних наслідків. Відповідно до визначеної системи критеріїв до об'єктів з критичною кіберінфраструктурою окрім зазначених вище секторів доцільно віднести інформаційно-комунікаційні системи органів державної влади, підприємств,

установ, організацій, сторонній кібервплив деструктивного характеру на які може призвести до настання суспільно небезпечних наслідків для національної безпеки держави [85, 86]. Нині в державі розроблено низку нормативно-правових документів, що надають особливого статусу об'єктам, які за світовою практикою віднесені до критичної інфраструктури. При цьому актуальними залишаються питання ефективного управління ресурсами на запобігання, реагування та ліквідацію надзвичайних ситуацій, що можуть бути утворені загрозами для таких об'єктів [75, 77]. Зв'язок кіберсистем з підсекторами критичної інфраструктури України на прикладі інформаційних, комунікаційних та інформаційно-комунікаційних систем можна подати схематично у вигляді рис. 1.6 [89].



Рис. 1.6. Зв'язок кіберсистем з підсекторами критичної інфраструктури України

Таким чином, головним завданням в галузі кібербезпеки об'єктів критичної інфраструктури України має стати запобігання проявам кібервпливів на системи з критичною кіберінфраструктурою, зниження вразливості держави від таких впливів та мінімізація збитків і часу на їх відновлення.

1.5. Модель виявлення та пошуку об'єктів з критичною кіберінфраструктурою

Одним зі стримуючих чинників, який до сьогодні не дозволяв системно досліджувати критичну кіберінфраструктуру держави був недолік, пов'язаний з неможливістю повного охоплення всіх взаємозв'язків і взаємозалежностей між її системами та об'єктами на основі існуючих моделей [100].

Для побудови адекватних моделей наявної у державі критичної кіберінфраструктури, управління нею та її захисту мають розроблятися спеціалізовані системи імітаційного моделювання, які б поєднували дані геопросторової інформації та багатовимірний (просторово-часовий) ефект.

У сучасних засобах імітаційного моделювання критичної інфраструктури досить поширеним є застосування методу Барлоу для визначення горизонтальної зв'язності елементів з ваговими коефіцієнтами, метод Вардена – для виявлення вертикальної взаємозалежності та ін. Інтегроване застосування цих методів дозволяє розробити математичні моделі для дослідження об'єктів будь-якого масштабу (секторів інфраструктури, міст, держав, регіонів) з метою виявлення їх уразливих об'єктів (центрів тяжіння за Клаузевіцом) та прийняття відповідних рішень щодо їх захисту.

В основу моделі виявлення та пошуку об'єктів з критичною кіберінфраструктурою пропонується покласти теорію графів. Вершини графу можуть відноситися до двох великих груп – джерел і споживачів. При цьому одна вершина може виконувати одночасно обидві функції (рис. 1.7).

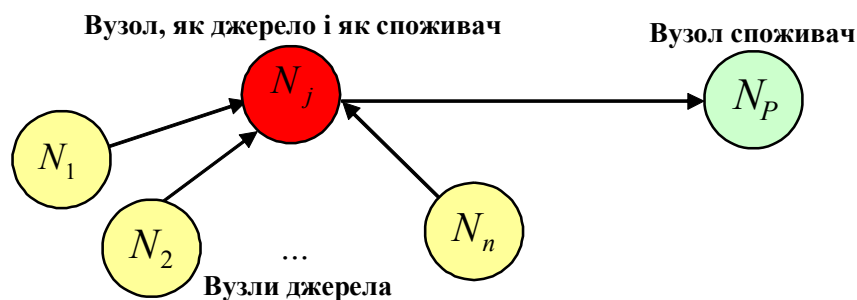


Рис. 1.7. Граф функціонально взаємозв'язної мережі

На графі видно, що працездатність об'єкту споживача N_p залежить від рівня працездатності об'єкту джерела N_j і одночасно від рівня його забезпеченості вже як споживача. При цьому рівень працездатності може бути виражений через критерій корисності (цінності) об'єкту, пропускну здатність або інші показники.

У подальшому міра взаємозалежності об'єктів з критичною кібернетичною інфраструктурою поданою у вигляді графа, трансформується в матрицю зв'язності. Як приклад, можна використовувати матрицю зв'язності для п'яти секторів, визначених як критичні для кібернетичної інфраструктури. Це таких як: органи державного управління, енергетичний, транспортний та ІТ- сектор, екстрені служби.

Після побудови графа і формування матриці зв'язності критичної кіберінфраструктури виникає необхідність математичного опису усієї складності взаємозалежності її об'єктів. Для цього різні сектори інфраструктури можна зобразити у вигляді графів, в яких вершини – це об'єкти, а ребра – зв'язки між ними.

Математичний опис міри зв'язності об'єктів критичної інфраструктури необхідний для здійснення пошуку ланцюгів відмов в усіх взаємозв'язаних секторах і прогнозування відмов N -го покоління. Такі ланцюги, що потенційно з'являються у результаті множинних взаємозалежностей різної природи, утворюють дуги між секторами інфраструктури або їх об'єктами.

Після математичного опису взаємозалежності об'єктів критичної кіберінфраструктури ведеться пошук найуразливіших з них, дія на які може завдати найбільшої шкоди усій інфраструктурі. При цьому вирішується ряд завдань, загальна кількість яких може варіюватися залежно від цілей дослідження і системи, що аналізується.

Пошуком ключових об'єктів, вплив на які може завдати найбільшої шкоди, дослідження критичної кібернетичної інфраструктури не обмежується. Це лише перший етап, після якого слід провести оцінку уразливості виявлених «центрів тяжіння»² за допомогою інженерного методу побудови дерева відмов, яке трансформується у дерево подій, що дозволяє визначити можливі уразливості інфраструктури, а також їх варіації. Дерево відмов є бінарним деревом з усіма можливими логічними подіями для кожної потенційної відмови. Саме дерева відмов і подій дозволяють сформулювати і розробити можливі заходи щодо захисту або впливу на критично важливі і уразливі об'єкти інфраструктури. Результатом формування дерева події є список уразливостей, який використовується у якості початкових даних для розрахунку (із застосуванням законів булевої алгебри) ймовірності їх виникнення, а також формування гістограми ймовірності відмов.

На наступному етапі розробляються алгоритми оцінювання ризиків, зміст яких полягає у визначенні ресурсів, необхідних для забезпечення безпеки (впливу) найбільш важливих з виявлених об'єктів з критичною кібернетичною інфраструктурою. При цьому однією з головних умов залишається дотримання критерію «вартість – ефективність», а ключова проблема полягає у тому, щоб правильно вибрати способи і засоби для організації захисту або дії. У загальному процес виявлення та пошуку об'єктів з критичною кібернетичною інфраструктурою передбачає реалізацію декількох покрокових процедур [60, 79, 98].

На першому кроці доцільно реалізувати процедуру всебічного аналізу об'єкта на предмет «критичності». Базовий алгоритм для визначення належності об'єкта й віднесення його до категорії об'єктів з критичною кіберінфраструктурою можна подати у вигляді блок-схеми (рис. 1.8).

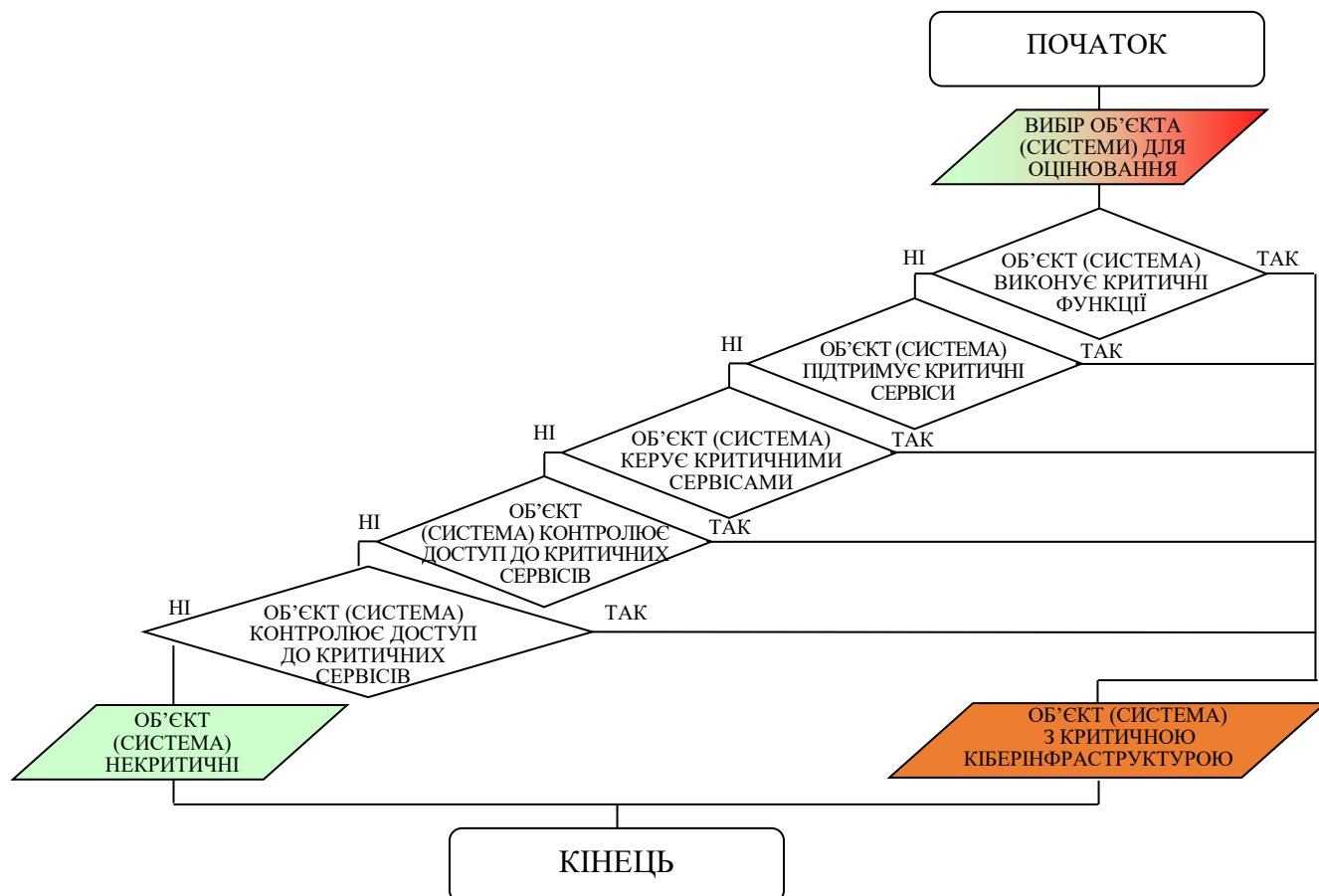


Рис. 1.8. Алгоритм визначення належності об'єкта (системи) до критичної інфраструктури

У разі віднесення об'єкта до класу об'єктів з критичною кіберінфраструктурою на другому кроці слід організувати процес категоріювання відповідних об'єктів за ступенем їх важливості. Виходячи з аналізу розробленого алгоритму (див. рис. 1.8) об'єкти з критичною кіберінфраструктурою доцільно розподілити за рівнями їх важливості і віднести до однієї з трьох категорій (табл. 1.3): життєво-важливі; вкрай важливі; важливі.

Відмінною рисою розробленого алгоритму (див. рис. 1.8) та таблиці (табл. 1.3) категоріювання від відомих є можливість формулювання на їх основі кількісних показників кіберуразливості об'єктів з критичною кіберінфраструктурою, оскільки переважна більшість наукових досліджень у цій сфері не дозволяли реалізувати подібні функції.

Третій крок передбачає вироблення процедур захисту об'єкта з критичною кіберінфраструктурою. Процедура захисту визначених об'єктів є однією з найбільш важливих з питань забезпечення кібербезпеки.

Таблиця 1.3

Категоріювання об'єктів з критичною кіберінфраструктурою

РІВЕНЬ ВАЖЛИВОСТІ	КАТЕГОРІЯ ВАЖЛИВОСТІ	КАТЕГОРІЯ ОБ'ЄКТА
I	Життєво-важливі	☐ АЕС; ☐ ГЕС (більше 2 ГВт); ☐ гідротехнічні споруди; ☐ об'єкти зберігання стратегічних запасів нафти і газу; ☐ шкідливі хімічні і нафтохімічні виробництва; ☐ склади зберігання ядерних матеріалів і боєприпасів.
II	Вкрай важливі	☐ системи енергозабезпечення (більше 2 ГВт); ☐ метрополітен; ☐ лінії водопостачання; ☐ підземні каналізаційні системи; ☐ магістральні трубопроводи (більше 100 млрд. куб. м.).
III	Важливі	☐ морські порти (для морських держав); ☐ очисні споруди; ☐ магістральні споруди; ☐ великі аеропорти; ☐ великі центри зв'язку; ☐ магістральні трубопроводи.

Захист виявлених об'єктів з критичною кіберінфраструктурою включає проведення заходів, які повинні забезпечити їх збереження у разі різних впливів природного або техногенного характеру.

Ефективний захист повинен передбачати розроблення необхідної законодавчої бази, фінансових вкладень, створення необхідних органів управління і підпорядкування їм надзвичайних служб, оснащення необхідними апаратними і програмними засобами.

При цьому створення системи кібербезпеки в інтересах захисту об'єктів з критичною кіберінфраструктурою обов'язково має здійснюватися з врахуванням національних особливостей, традицій і основ державного устрою.

Четвертим кроком має бути розроблена система управління захистом виявленого об'єкта з критичною кіберінфраструктурою. В основу має бути

покладений принцип відкритої архітектури та метод ієрархій, що забезпечить її формування у вигляді багаторівневої складної системи, що має єдиний координаційний орган управління.

Висновки за главою 1

На основі проведеного аналізу запропоновано нове формальне подання та класифікацію процесів системи безпеки. Були отримані наступні результати: виявлено загальні характеристики процесів системи безпеки, сформовані інформаційний і модельний базиси системи безпеки, що дозволило представити підхід до класифікації та формальному поданню процедур, реалізованих в системах безпеки. Представлений підхід до класифікації та формальному опису процедур, реалізованих в системі безпеки, дозволяє формалізувати підхід до аналізу і подальшого синтезу необхідного процедурного базису при проектуванні і реінжинірингу систем безпеки, у вигляді більш зрозумілою особі, що приймає рішення. Таким чином збільшується ефективність управління механізмами захисту контуру бізнес-процесів.

Вперше з системних позицій обґрунтовано належність системи управління об'єктів критичної інфраструктури держави до систем з критичною кіберінфраструктурою, оскільки більшість з них в процесі свого функціонування пов'язані з роботою інформаційно-комунікаційних систем. Розроблена графова модель взаємодії таких систем дозволила зробити висновок про наявність ланцюгових реакцій в системах управління критичної інфраструктури, що суттєво підвищує вимоги до систем безпеки об'єктів критичної інфраструктури. Вивчення світового досвіду дозволило запропонувати найбільш вразливі сектори об'єктів критичної інфраструктури України, що було згодом підтверджено практикою, якої набула Україна в ході відбиття збройної агресії, у т.ч. й в кіберпросторі.

Запропонована графова модель виявлення та пошуку об'єктів з критичною кіберінфраструктурою дозволяє на практиці виявляти найслабкішу ланку безпеки в контурі управління об'єктом критичної інфраструктури, чим суттєво загострити вимоги до створюваних систем безпеки таких об'єктів. Показано, що такі системи повинні мати розподілену структуру. Тому з метою практичної реалізації розподілених систем інформаційної безпеки об'єктів критичної інфраструктури запропоновано відповідну концепцію. Розроблена концепція ґрунтується на моделях напівмарковських процесів для постановки

задач дослідження динаміки протікання процесів кібернападу у ході інформаційного конфлікту в системі інформаційної безпеки об'єкта критичної інфраструктури під час кібератаки. Концепція узагальнює розроблені в роботі диференціально-ігрові моделі й розвиває відповідні політики безпеки на новий клас систем захисту об'єктів критичної інфраструктури. Базисом концепції є авторський метод диференціально-ігрового моделювання процесів кібернападу, що забезпечує збереження точності вихідних моделей при моделюванні відповідних процесів у реальному масштабі часу.

ГЛАВА 2.

МОДЕЛЮВАННЯ ДІНАМІКИ ПОВЕДІНКИ ОБ'ЄКТІВ СИСТЕМ БЕЗПЕКИ

2.1. Концепція моделювання поведінки взаємодіючих агентів систем безпеки

Базисом запропонованої концепції моделювання поведінки взаємодіючих агентів є трирівнева структура моделювання суб'єктів та бізнес-процесів контурів функціонування організації та системи безпеки [28, 35]. На відміну від існуючих методологій моделювання, побудованих на моделюванні аспектів здійснення кібератак, запропонована базується на моделюванні поведінки антагоністичних агентів [39]. Концепція може застосовуватися для прогнозування можливої поведінки нападаючої сторони, обґрунтування вибору засобів протидії на системному рівні кіберзагрозам та розрахунку необхідної суми інвестицій у кібербезпеку з відповідним розподілом на напрямках та часу інвестування [36]. Визначимо наступні дефініції:

Дефініція 1. Критичні бізнес-процеси – процеси, неналежні організації яких або недотримання вимог до їх виконання можуть представляти фактичну або потенційну небезпеку для забезпечення якості послуги.

Дефініція 2. Контур бізнес-процесів організації – сукупність інформаційних ресурсів та зв'язаних з ними бізнес-процесами, виконання яких в заданій послідовності призводить до досягнення мети організації

$$S^{BC} = \left\{ \langle S^{BP_1}, IR^{BP_1}, T^{BP_1} \rangle, \dots, \langle S^{BP_n}, IR^{BP_n}, T^{BP_n} \rangle \right\}$$

де S^{BP} – контур бізнес-процесів як множина бізнес-процесів, кожен з яких представляє собою:

S^{BP_i} – i -й бізнес процес. заданий структурою зв'язків окремих бізнес-операцій, які виконуються в певній послідовності;

IR^{BP_i} – сукупність інформаційних ресурсів i -го бізнес-процесу;

T^{BP_i} – сукупність загроз, що діють на i -й бізнес-процес.

Дефініція 3. Контур бізнес процесів системи безпеки – сукупність бізнес процесів та необхідних для них ресурсів, виконання яких забезпечує нормальне функціонування контуру бізнес-процесів організації:

$$S^{BP} = \left\{ \langle S^{BP_1}, Rs^{BP_1}, T^{BP_1} \rangle, \dots, \langle S^{BP_m}, Rs^{BP_m}, T^{BP_m} \rangle \right\}$$

де S^{BP} – контур бізнес-процесів системи безпеки як множина бізнес-процесів, кожен з яких представляє собою:

S^{BSi} – i -й бізнес-процес, заданий структурою зв'язків окремих бізнес-операцій, які виконуються в певній послідовності в системі безпеки;

IR^{BSi} – сукупність інформаційних ресурсів, що захищаються i -м бізнес-процесом системи безпеки;

Tr^{BSi} – сукупність загроз, захист від яких забезпечує i -й бізнес-процес системи безпеки.

Формування методології моделювання поведінки агентів контуру бізнес-процесів (БП) системи безпеки складається з наступних етапів:

Етап 1. Аналіз контурів БП та можливих атак на них

$$S^{BC} = \left\{ \langle S^{BP_1}, IR^{BP_1}, Tr^{BP_1} \rangle, \dots, \langle S^{BP_n}, IR^{BP_n}, Tr^{BP_n} \rangle \right\}$$

Етап 2. Розробка моделей рівня індивідуальних агентів системи безпеки

$$M_A = \{M_A^{DM}, M_A^L\}$$

Етап 3. Розробка моделей рівня групи агентів системи безпеки

$$M_G = \{M_G^B, M_G^L\}$$

Етап 4. Розробка моделей загальносистемного рівня

$$M_G = \{M_G^C, M_G^{SO}\}$$

Етап 5. Розробка методів визначення найбільш ймовірних загроз та оцінки їх вартісних показників

$$Tr_l = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A$$

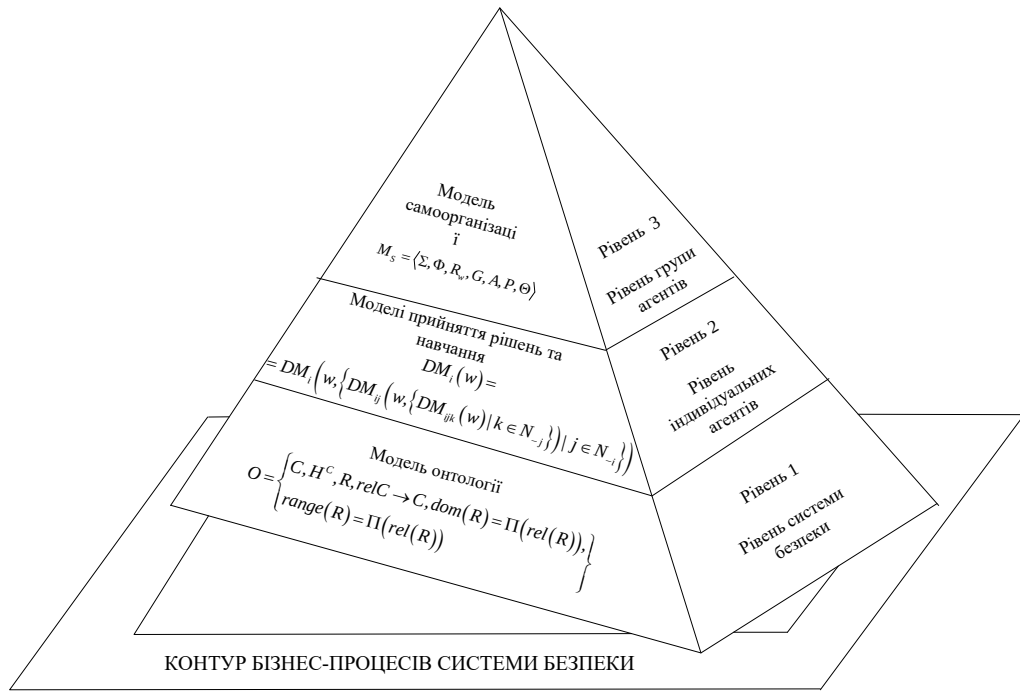


Рис. 2.1. Концепція моделювання поведінки агентів систем безпеки
Контур БП СБ поєднує БП: управління безпекою, забезпечення безпеки, реалізації, планування, перевірки, удосконалення.

На *першому рівні Концепції* використовується запропонована онтологічна модель, як носій знань про конфліктно-коопераційні взаємодії агентів системи безпеки. Формалізована модель онтології пропонується у вигляді:

$$O = \{C, H^C, R, rel C \rightarrow C, dom(R) = \Pi(rel(R)), range(R) = \Pi(rel(R))\}.$$

де C – множина, елементи якої називаються поняттями;

$H^C: H^C$ – ієрархія концепцій, при $H^C \subseteq C \times C$;

R – множина, елементи якої називаються відносинами, C та R не перетинаються;

$rel: R \rightarrow C \times C$ – функція, яка співвідносить концепції не таксономічно;

$dom: R \rightarrow C$ – функція, з $dom(R) := \Pi_1(rel(R))$ задає предметну область R , а $R \rightarrow C$ з $range(R): \Pi_2(rel(R))$ задає його діапазон. Для $rel(R) = (C_1, C_2)$ записуємо $R(C_1, C_2)$;

A^O – набір аксіом онтології, виражений на відповідній логічній мові.

Аналіз класифікатора існуючих загроз дозволив сформулювати відношення гібридності та синергетичності загроз залежно від їх типу та спрямованості [49]. У класифікатор загроз введено платформу вартісних

показників атак, що дозволяє оцінювати загрози з економічної ефективності їх використання та протидії їм. Запропонована шкала вимірювання вартості збитків для експертного оцінювання у вигляді: *{незначна, низька, середня, висока, дуже висока}*. Позначимо: i поточний номер загрози ($\{i\}_1^N$), k – поточний номер експерта, який виконував оцінку ($\{k\}_1^K$). Середнє значення оцінки вартості збитків експертами за всіма загрозами для певно контуру бізнес-процесів в може бути записане:

$$P_k^A = \frac{1}{KM} \sum_{j=1}^M \sum_{i=1}^K \alpha_j p_{ijk}^A; C_k^A = \frac{1}{KM} \sum_{j=1}^M \sum_{i=1}^K \alpha_j c_{ijk}^A,$$

$$P_k^D = \frac{1}{KM} \sum_{j=1}^M \sum_{i=1}^K \alpha_j p_{ijk}^D; P_k^D = \frac{1}{KM} \sum_{j=1}^M \sum_{i=1}^K \alpha_j p_{ijk}^D,$$

де K – кількість експертів, M – кількість бізнес-операцій, на які може бути спрямована загроза, α_j – коефіцієнт критичності бізнес-процесу, до якого належить відповідна бізнес-операція.

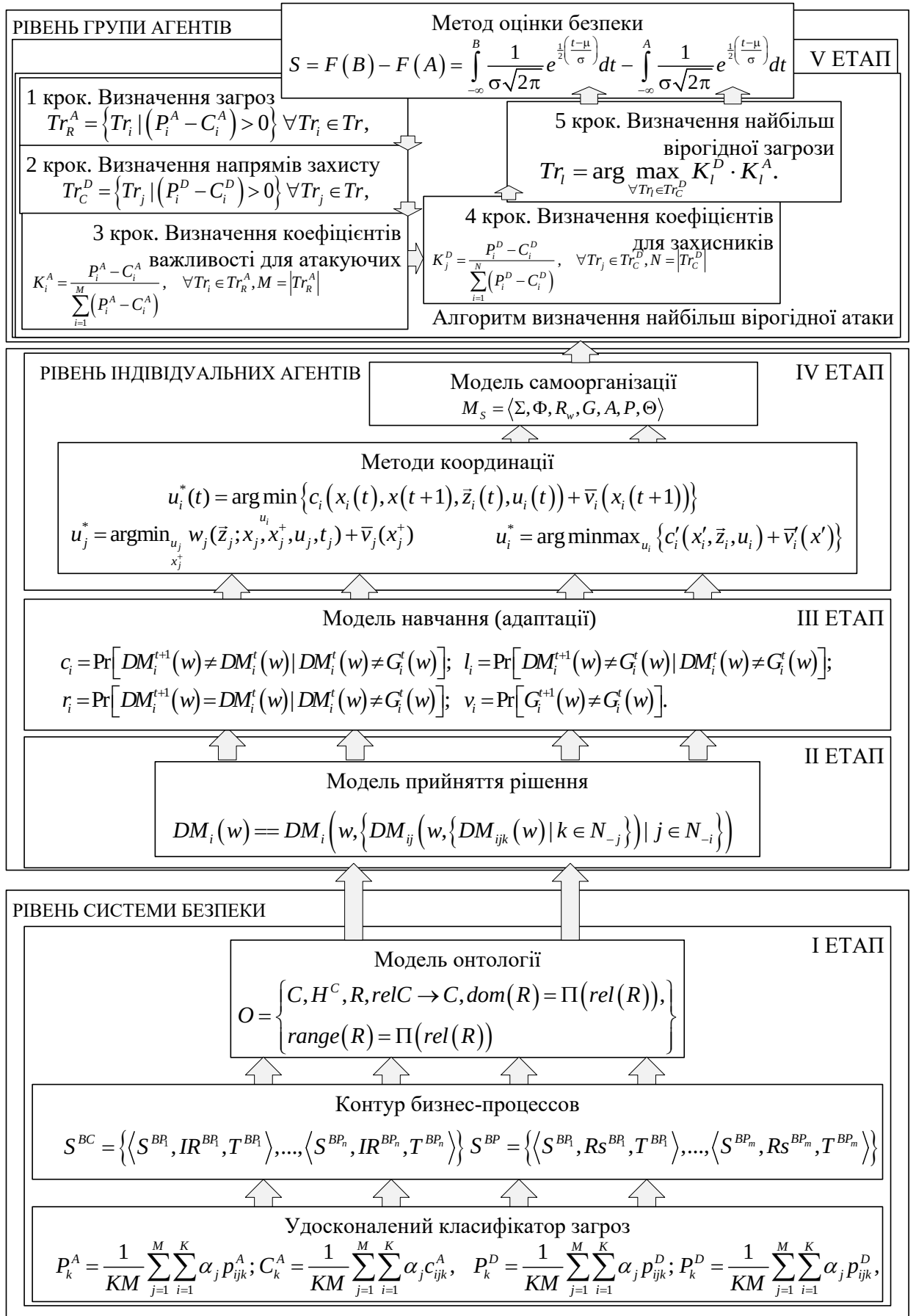


Рис. 2.2. Методологія моделювання процесів поведінки антагоністичних агентів в системах безпеки

На *другому рівні Концепції* розглядаються питання поведінки окремих суб'єктів системи безпеки та будуються моделі їх поведінки, а саме моделі прийняття рішень (M_R^{DM}) та моделі навчання (M_R^L): $M_R = \{M_R^{DM}, M_R^L\}$.

На *третьому рівні Концепції* моделі попереднього рівня використовуються для побудови моделей групової поведінки. А саме моделей координації, адаптації та самоорганізації: $M_G = \{M_G^C, M_G^A, M_G^{SO}\}$.

Реалізація концепції моделювання поведінки взаємодіючих агентів систем безпеки дозволяє побудувати методології моделювання процесів поведінки антагоністичних агентів, яка у загальному структурованому вигляді наведена на рис. 2.2 [3, 4].

Модельне наповнення методології доцільно розглядати у хронологічній послідовності її розробки, яке реалізується як послідовність 5 етапів. Опис моделей та їх прив'язка до відповідних етапів [10, 17] наведена у наступному розділі.

2.2. Модельний базис методології моделювання процесів поведінки антагоністичних агентів

На *1 етапі* запропонована Концепція моделювання поведінки агентів систем безпеки, яка реалізується на трьох рівнях (рівень системи безпеки, рівень індивідуальних агентів, рівень групи агентів, на рис. 2.1) та спрямована на гарантоване забезпечення безпеки бізнес-процесів організації, що дозволяє створити контур бізнес-процесів системи безпеки.

Побудований комплекс моделей дозволяє зробити економічно обґрунтований розподіл обмежених коштів на захист інформаційних ресурсів контуру бізнес-процесів [22].

На *2 етапі* запропонована базова модель прийняття рішення окремим агентом (рис. 2.3). Модель реалізує процес прийняття рішення на двох стадіях (ідентифікація загрози (ТІ) та вибір засобів протидії (RC)), кожна з яких передбачає узгодження сформованої оцінки з оцінками інших ОПР системи безпеки [6].

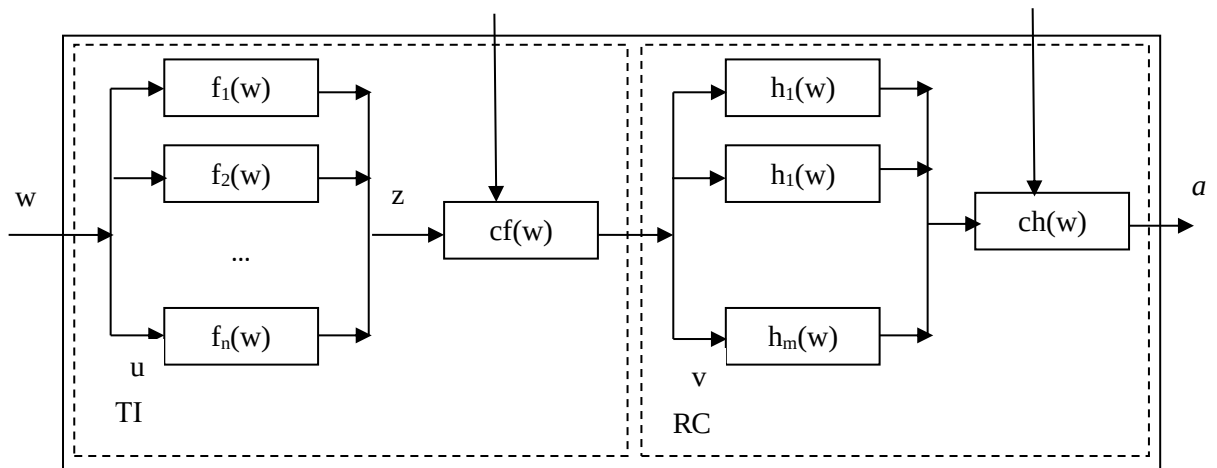


Рис. 2.3. Базова модель прийняття рішення окремим агентом

На рис. 2.3 прийнято такі позначення: w – кібероточення системи безпеки; $f_i(w)$ – i -й алгоритм ідентифікації загрози по отриманих даних w ; u – змінна вибору алгоритму ідентифікації загрози; z – змінна, що визначає загрозу (результат ідентифікації); $h_j(z)$ – j -й алгоритм вибору засобів протидії ідентифікованій загрозі; v – змінна, що визначає засіб протидії; a – реалізація засобів протидії сторони захисту.

Модель групового рівня дозволяє реалізовувати моделі 2-го рівня методології (координації, адаптації та самоорганізації) [50, 51].

Відповідні множини та функції окремого агента наведені на рис. 2.4.

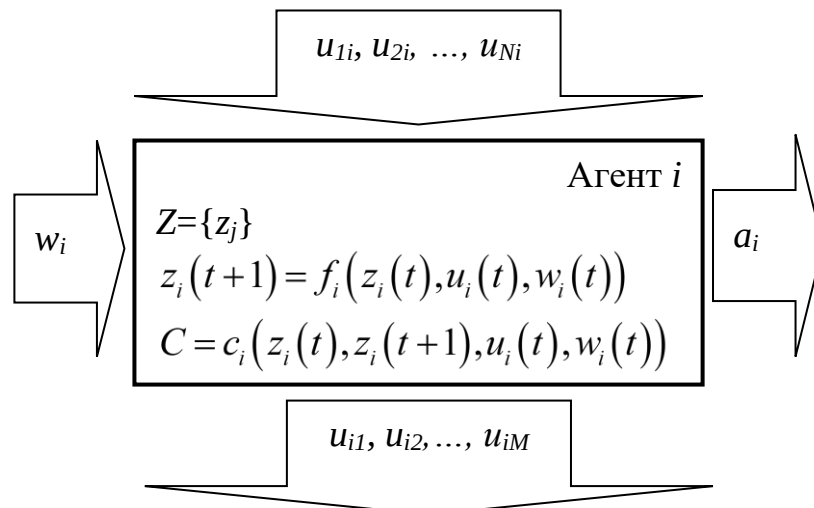


Рис. 2.4. Модифікація моделі окремого агента

На рис. 2.4. прийнято такі позначення: $W=\{w_i\}$ – множина станів простору протистояння (інформація про кібератаки); $A = \{a_i\}$ – множина дій, що може здійснити агент; $Z=\{z_j\}$ – множина станів, в яких може перебувати

агент; $z_i(t+1) = f_i(z_i(t), u_i(t), w_i(t))$ – функція переходів; $u_{ij}(t) = g_{ij}(z_i(t))$ – функція агрегування; $C = c_i(z_i(t), z_i(t+1), u_i(t), w_i(t))$ – функція локальних витрат; $a_i(t) = h_i(z_i(t), u_{ji}(t))$ – локальна функція виходу.

На 4 етапі запропоновані методи координації поведінки агентів контуру бізнес-процесів системи безпеки різняться в залежності від рівня рефлексивності окремого агента і можуть застосовувати різні стратегії координації в групах агентів системи безпеки [21]:

Метод координації без комунікації. Агент нічого не знає поза своєї локальної моделі: $u_i^*(t) = \arg \min_{u_i} \{c_i(x_i(t), x(t+1), \bar{z}_i(t), u_i(t)) + \bar{v}_i(x_i(t+1))\}$.

Метод координації з прогнозом. Агент прогнозує наступні взаємодії, що генеруються: $u_j^* = \arg \min_{u_j} w_j(\bar{z}_j; x_j, x_j^+, u_j, t_j) + \bar{v}_j(x_j^+)$.

Метод координації для обмеженого горизонту. Вибір найкращої загальної взаємодії для періоду T : $u_i^* = \arg \min_{u_i} \max_{x_i'} \{c'_i(x'_i, \bar{z}_i, u_i) + \bar{v}'_i(x'_i)\}$.

Метод координації з абстракцією. Кожний агент має спрощену модель середовища:

$$u_i^* = \arg \min_{u_i} \max_{\substack{\tilde{z}_{ij} \\ \tilde{z}_{ji}}} w_i(\tilde{z}_i; x_i, x_i^+, \tilde{u}_i, T) + \bar{v}_i(x_i^+) + \sum_{i \in R^+} p_{ji}(\tilde{z}_{ji}) + \sum_{j \in R^-} r_{ij}(\tilde{z}_{ij}),$$

де R^+ – верхній перетин; R^- – нижній перетин.

Моделі координації у групах агентів безпеки враховують характеристики агентів, зокрема рівень рефлексивності.

Для групового рівня поведінки агентів додається характеристика координації дій агентів та спосіб її розрахунку:

$$\begin{aligned} G_c^n = & \sum_{i=1}^{u^n} p_i^n g_c^{n_i}(p(x^n)) + \alpha_i^n H(p_i^n) + H(z^n, z^{no}) + \\ & + g_c^{A^n}(p(z^n, z^{on})) + g_c^{B^n}(\bar{z}^n, v^{on}) + \sum_{j=1}^{v^n} p_j^n g_c^{nU^{n+j}}(p(\bar{z}^n | \bar{v}^n = j)) + \alpha_j^{nU^{n+j}} H(p_j^n) + \\ & + H(y^n) + H(z^n) + H(\bar{z}^n) + T_{z^n}(\tilde{x} : z^{on}) + T_{\bar{z}^n}(\tilde{x}^n, z^{on} : v^{on}) \end{aligned}$$

де X_i – локальний простір станів; Y_i – простір виходів; U_i – локальний простір рішень U_i ; $z_{1i}, \dots, z_{Ni}$ – вхідні множини впливів; $z_{i1}, \dots, z_{iN}$ – вихідні множини

впливів; $x_i(t+1)=f_i(x_i(t),z_{1i}(t),...,z_{Ni}(t),u_i(t))=f_i(x_i(t),z_i(t),u_i(t))$ – динаміка локального домену; $y_i(t)=h_i(x_i(t),z_i(t))$ – локальна функція виходу; $z_{ij}(t)=g_{ij}(x_i(t))$, $j=1,...,N$ – функція агрегування; $c_i(x_i(t), x_i(t+1),z_i,u_i)$ – локальна функція витрат.

На 5 етапі запропонований алгоритм оцінювання економічної ефективності загрози та протидії їй складається з наступних кроків [5, 38, 40]:

1-й крок. Визначаються ті загрози, ефект від реалізації яких перевищує витрати на їх проведення:

$$Tr_R^A = \{Tr_i \mid (P_i^A - C_i^A) > 0\} \forall Tr_i \in Tr,$$

де Tr_R^A – множина потенційних загроз, реалізація яких ефективна для атакуючого; Tr_i – загроза i -му інформаційному ресурсу; P_i^A – оцінка вартості успішності реалізації атаки на i -й ресурс бізнес-процесу з боку атакуючого; C_i^A – вартість проведення атаки на i -й ресурс бізнес-процесу з боку атакуючого.

2-й крок. Аналогічно визначаються напрямки захисту, які забезпечують більший ефект, ніж витрати на їх забезпечення:

$$Tr_C^D = \{Tr_j \mid (P_j^D - C_j^D) > 0\} \forall Tr_j \in Tr,$$

де Tr_C^D – множина загроз, проти яких доцільно з точки зору вартості вибудовувати захист; P_j^D – оцінка вартості втрати j -го інформаційного ресурсу для сторони захисту; C_j^D – вартість захисту j -го інформаційного ресурсу для стороною захисту;

3-й крок. Визначення коефіцієнтів важливості для атакуючих визначаються як частки виграшу від загальної суми виграшу, яка може бути отримана потенційно при реалізації всього комплексу загроз для нападників [30]:

$$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^M (P_i^A - C_i^A)}, \quad \forall Tr_i \in Tr_R^A, M = |Tr_R^A|$$

де K_i^A – рейтинговий коефіцієнт (важливості) реалізації загрози i -му інформаційному ресурсу; M – потужність (кількість елементів) множини відібраних потенційно ефективних загроз для атакуючої сторони.

4-й крок. Визначення коефіцієнтів для захисників визначаються як частки виграшу від загальної суми виграшу, яка може бути отримана потенційно при реалізації всього комплексу захисних заходів:

$$K_j^D = \frac{P_i^D - C_i^D}{\sum_{i=1}^N (P_i^D - C_i^D)}, \quad \forall Tr_j \in Tr_C^D, N = |Tr_C^D|$$

де K_j^D – рейтинговий коефіцієнт (важливості) вибудовування захисту j -го інформаційного ресурсу.

5-й крок. Визначення найбільш вірогідної загрози, яка може бути реалізована. Вибирається та з них, для якої множення коефіцієнтів важливості атакуючого і нападника виявляється максимальним [14]:

$$Tr_l = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A.$$

Рівень безпеки оцінюється в відносних одиницях: 1 – відповідає максимальному рівню безпеки, що забезпечується системою безпеки, 0 – система безпеки не забезпечує захист ні по одному з ресурсів.

Визначення ймовірності реалізації загрози при граничних можливостях захисту A і граничних можливостях нападу B буде визначатися різницею $F(B) - F(A)$, де A – граничний рівень можливостей сторони захисту, B – граничний рівень можливостей реалізації атаки боку нападу, $F(x)$ – щільність ймовірності випадкової величини x .

Рівень безпеки визначатимемо як частку тих ресурсів, які захищені від кібератак. Легко бачити, що ця величина може бути обчислена в такий спосіб:

$$S = F(B) - F(A) = \int_{-\infty}^B \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt - \int_{-\infty}^A \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{1}{2}\left(\frac{t-\mu}{\sigma}\right)^2} dt.$$

Графічне подання поточного рівня безпеки при зміні можливостей сторін кіберконфлікту (відносні величини), наведені на рис. 2.5.

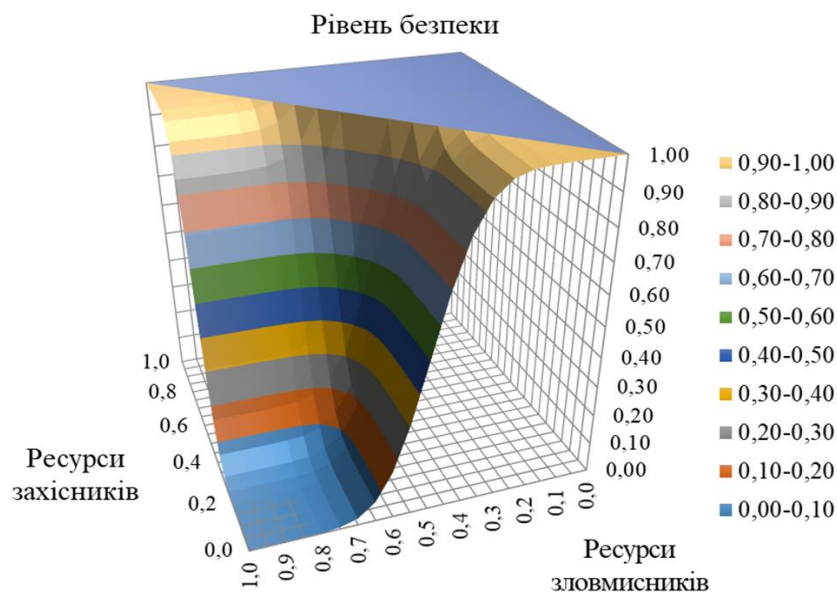


Рис. 2.5. Поточний рівень безпеки при зміні стратегій сторін кіберконфлікту

Для формального опису сценаріїв поведінки агентів в умовах кіберконфлікту [19, 20] може бути застосована контекстно-вільна граматика у вигляді Бекуса-Наура форми.

Синтез сценарію зводиться до побудови формальної грамматики на певній множині термінальних і нетермінальних символів. Синтаксису логіки висловлювань відповідає контекстно-вільна граматика, яка описується четвіркою: $G = (V, T, P, S)$, де V – кінцева множина нетермінальних символів; T – кінцева множина термінальних символів, що не перетинається з V ; P – кінцева множина правил продукцій, записаних у вигляді нотацій Бекуса, що містять символи з T і V ; S – початковий символ грамматики.

Використання запропоновано підходу до формального опису сценарії дозволяє автоматизувати аналіз формального опису сценаріїв та використовувати отримані результати аналізу для подальшій генерації сценаріїв поведінки антагоністичних агентів.

2.3. Системно-динамічна модель поведінки антагоністичних агентів

Системно-динамічна модель поведінки антагоністичних агентів процесі кібернападу [18], виконана верифікація моделі з подальшим сценарним моделюванням відповідних процесів. Визначення основних понять, що

використовуються при розробці моделі поведінки антагоністичних агентів наведені у таблиці 2.1.

Таблиця 2.1

Визначення основних понять моделі поведінки антагоністичних агентів

Поняття	Визначення
Репутація (Rep)	Сприятливе і загальновизнане ім'я або позиція за заслуги, досягнення, надійність тощо. У цьому випадку репутація відноситься до публічного престижу компанії.
Уразливість (Vul)	Рівень безпеки, яким володіють активи компанії. Це також можна назвати рівнем захисту активу.
Вектори безпеки (V_i)	Вектори безпеки – це зовні видимі та доступні системні ресурси, які можуть бути використані для здійснення атаки на систему і згодом зважені відповідно до потенційного збитку, який може бути заподіяний будь-якою експлуатацією вразливості.
Здатності захисників (C^A)	Наявні ресурси, що підлягають розподілу серед активів для підвищення рівня стійкості активів. Після того, як ці можливості будуть вкладені в певний актив, вони призведуть до витрат на захисників.
Можливості нападників (C^D)	Частина ресурсів зловмисників, доступних для розподілу серед активів захисника.
Частка інвестицій (FI)	Частина можливостей, призначених для захисту активів компанії.
Частка атак (AF^i)	Кількість атак, які зловмисники розповсюджують серед векторів безпеки захисників відповідно до успішних історичних атак. Після того, як ці можливості будуть адресовані певному вектору,
Успішні атаки (A_i^S)	Кримінальні напади, які можуть порушити захист активів через вектори безпеки.
Прибуток захисників (DAP)	Грошовий прибуток від підвищення рівня захисту активів, що, в свою чергу, підвищує репутацію, тим самим збільшуючи фінансові показники
Багатство нападників (C^A)	Грошова перевага від порушення активів захисників.

Основні співвідношення для кожної моделі мають вигляд:

– модель захисника:

$$\frac{d(A_i^{RS})}{dt} = R_i - D_i, \quad R_i = A_i^S / T^{RA},$$

$$FI_i = A_i^{RS} / \sum_{i=1}^3 A_i^{RS}, \quad \frac{d(Rep)}{dt} = BU - ER, \quad BU = \begin{cases} Ad / T^{BUR} & \text{if } Ad > 0 \\ 0 & \text{if } Ad \leq 0 \end{cases},$$

$$ER = \begin{cases} |Ad / T^{RL}| & \text{if } Ad < 0 \\ 0 & \text{if } Ad \geq 0 \end{cases}, \quad Ad = IR - Rep, \quad IR = R^B - \sum_{i=1}^3 V_i \times Vul_i,$$

$$DFP = (RMR * Rep) + BFP, \quad \frac{d(DAP)}{dt} = IFP$$

де R_i – збільшення кількості успішних атак на конкретний вектор за час, необхідний захиснику для повідомлення про успішні атаки; D_i – кількість відбитих атак, про які повідомлялося, розділене на час, необхідний захисникам для припинення таких атак; A_i^{RS} – успішні атаки, про які повідомлялось; A_i^S – успішні атаки; T^{RA} – час, необхідний для повідомлення про атаки; N^{DA} – кількість відхилених атак; T^D – час відбиття атаки; FI_i – частка інвестицій у захист вектору i ; Rep – репутація; T^{BUR} – час для зміцнення репутації; T^{RL} – час втрати репутації; R^B – базова репутація; V_i – Значення вектору i ; Vul_i – вектор вразливості i ; DFP – фінансові показники захисників; $RMRC$ – співвідношення репутації до грошової ставки; BFP – базові фінансові показники; DAP – накопичений прибуток захисників; IFP – підвищення фінансових показників.

– модель середовища протистояння:

$$Vul_i = (C^A \times AF_i \times C^{UA}) - (C^D \times FI_i)$$

$$SA_i = \begin{cases} (C^A * AF_i) - ((C^D * AF_i) / C^{UA}) & \text{if } Vul_i > 0 \\ 0 & \text{if } Vul_i \leq 0 \end{cases},$$

де C^A – можливості нападників; AF_i – частка вектора атаки i ; C^{UA} – вартість одиночної атаки; C^D – можливості захисників.

– модель зловмисника:

$$\frac{d(A_i^{AS})}{dt} = B_i, \quad B_i = A_i^S / T^{RA}, \quad V_i^P(t) = A_i^{AS}(t-1), \quad S_i = \begin{cases} 0 & \text{if } A_i^{AS} - V_i^P < 1 \\ 1 & \text{if } A_i^{AS} - V_i^P \geq 1 \end{cases},$$

$$A_i^F = S_i \times A_i^{AS} / \sum_{i=1}^3 S_i \times A_i^{AS}, \quad P^A = \sum_{i=1}^B B_i \times C^{UA}, \quad \frac{d(AAW)}{dt} = IAW,$$

де: A_i^{AS} – вектор i накопичених успішних атак; A_i^S – вектор i успішних атак; T^{RA} – час повідомлення про атаку; V_i^P – минуле значення i ; S_i – перемикач i ; P^A – продуктивність нападників; B_i – порушення за вектором i ; W^{AA} – накопичення багатства нападників; W^{IA} – збільшення багатства нападників.

Запропонована модель дозволяє визначити критичну точку рівня ефективного інвестування в систему безпеки, забезпечити ефективну протидію сучасним гібридним загрозам на елементи структури контуру бізнес-процесів, підвищити рівень безпеки організації за рахунок ефективного рівня інвестуванні в систему безпеки (рис. 2.6.).

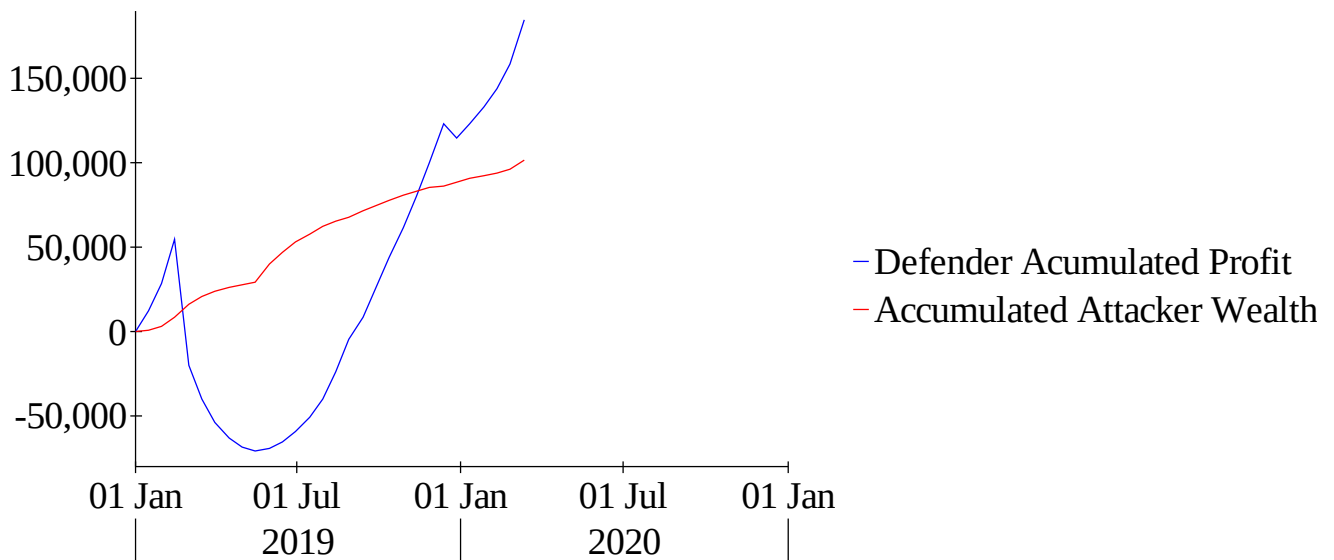


Рис. 2.6. Оцінка критичності зламу системи безпеки

Модель взаємодії агентів в умовах кіберконфлікту, була реалізована як системно-динамічна модель в середовищі візуального програмування.

2.4. Динамічні моделі безпеки на основі підходу Лотки-Вольтери

Для оцінки безпеки кіберфізичних систем в умовах впливу сучасних цільових кіберзагроз, які виявляють ознаки гібридності та синергізму [1],

враховується їхнє комплексування з методами соціальної інженерії на елементи інфраструктур. При формуванні моделі безпеки також визначений підхід їх класифікації та формування коефіцієнтів [26, 53].

Модель безпеки соціокіберфізичних систем на основі моделі “хижак-жертва” з урахуванням обчислювальних можливостей та спрямованості цільових кібератак (модель 1) визначимо:

де
$$\tilde{N}_1 = \sum_{i=1}^Q \left(N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \right) -$$
 чисельність об'єктів, що

представляють цілі атак з урахуванням їхньої гібридності;

$$N_2 = N_2 \times |W_{\text{hybrid } C, I, A, Au, Af \text{ synerg}}| -$$
 рівняння зміни чисельності сучасних загроз на

SCS з урахуванням можливості їх ознак синергізму та гібридності, де

$$|W_{\text{hybrid } C, I, A, Au, Af \text{ synerg}}| -$$
 потужність множини гібридних загроз (тобто їх

кількість), а
$$W_{\text{hybrid } C, I, A, Au, Af \text{ synerg}} = W_{\text{synerg}}^C \cap W_{\text{synerg}}^I \cap W_{\text{synerg}}^A \cap W_{\text{synerg}}^{Au} \cap W_{\text{synerg}}^{Aff},$$
 де множина

гібридних загроз, які відповідно до прийнятого припущення, визначається як множина загроз одночасно для всіх служб безпеки.

$$A_1^{SCS} = \begin{cases} \frac{dN_1}{dt} = \left(\arg \max_{\forall Tr_i \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum_{i=1}^Q \left(N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \right) \right) - \\ - \left(\sum_{i=1}^M \left(w_{SCSi}^C \cap w_{SCSi}^I \cap w_{SCSi}^A \cap w_{SCSi}^{Au} \cap w_{SCSi}^{Aff} \right) \chi_i^{SCS} \right) \tilde{N}_1 \times, \\ \times \left(N_2 \times |W_{\text{hybrid } C, I, A, Au, Af \text{ synerg}}| \right); \\ \frac{dN_2}{dt} = - \left(\frac{1}{M} \sum_{i=1}^M v_i \times p_{rj} \times r_{motiv} \right) \overline{N_2} + \\ + \left(\frac{1}{KB} \sum_{k=1}^K \sum_{g=1}^B \left(\mu_{kg}^l \times w_{kg}^l \right) \right) \overline{N_2 N_1}. \end{cases}$$

Використання моделі дозволяє оцінити обчислювальні можливості та сформувати класифікацію зловмисників.

Такий підхід формує точку незворотності при якому визначається «неможливість» проведення цільовий атаки [23].

Наступна модель дозволяє враховувати «зацікавленості» злочинців та/або кібергруп у проведенні цільової атаки, їх мотивацію та конкуренцію.

Модель безпеки соціокіберфізичних систем на основі моделі «хижак-жертва» з урахуванням можливої конкуренції зловмисників по відношенню до «жертви» (модель 2) визначимо:

$$A_2^{SCS} = \left\{ \begin{aligned} & \frac{dN_1}{dt} = \left(\arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ & \times \left(\sum_{i=1}^Q \left(N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \right. \right. \\ & \left. \left. + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \right) \right) - \\ & - \left(\sum_{i=1}^M \left(w_{SCSi}^C \cap w_{SCSi}^I \cap w_{SCSi}^A \cap w_{SCSi}^{Au} \cap w_{SCSi}^{Aff} \right) \chi_i^{SCS} \right) \times \\ & \times \tilde{N}_1 \left(N_2^1 \cap N_2^2 \cap \dots \cap N_2^w \right); \\ & \frac{dN_2}{dt} = - \left(\frac{1}{M} \sum_{i=1}^M \nu_i \times p_{rj} \times r_{motiv} \right) \times \left(\overline{N_2^1 \cap N_2^2 \cap \dots \cap N_2^w} \right) + \\ & + \left(\frac{1}{KB} \sum_{k=1}^K \sum_{g=1}^B \left(\mu_{kg}^l \times w_{kg}^l \right) \right) \times \left(\overline{N_2^1 \cap N_2^2 \cap \dots \cap N_2^w} \right) N_1, \end{aligned} \right.$$

де кількість «хижаків» належить множині $\left\{ \overline{N_2^j} \right\}, j \in 1, \dots, Q$.

Таким чином запропонована модифікація моделі Лотки-Вольтери дозволяє формувати вектор «зацікавленості» цільових (змішаних) атак з урахуванням еволюційного розвитку технологій.

Модель безпеки соціокіберфізичних систем на основі моделі «хижак-жертва» з урахуванням можливості групування зловмисників/кібергруп з метою досягнення цілей кібератаки визначимо (модель 3):

Модель дозволяє враховувати політичні та/або економічні та/або соціальні складові мотивації реалізації загроз. Це пов'язано з загальною

тенденцію розвитку мирового суспільства, етнічними та культурними цінностями, а також формуванню кіберугруповань які підконтрольні державі та виконують замовлення за рахунок фінансування та підтримки держави в цілому. прикладом такої моделі може бути військова частина №61398 НВАК (Відділ АРТ1) Китаю, яка реалізує електронний шпіонаж.

$$A_3^{SCS} = \left\{ \begin{array}{l} \frac{dN_1}{dt} = \left(\arg \max_{\forall T_{\eta} \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ \times \left(\sum_{i=1}^Q \left(N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \right. \right. \\ \left. \left. + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \right) \right) - \\ - \left(\sum_{i=1}^M \left(w_{SCSi}^C \cap w_{SCSi}^I \cap w_{SCSi}^A \cap w_{SCSi}^{Au} \cap w_{SCSi}^{Aff} \right) \times \right. \\ \left. \times \chi_i^{SCS} \right) \times \\ \times \tilde{N}_1 \left(\sum_{j=1}^w N_2^w \right); \\ \frac{dN_2}{dt} = - \left(\frac{1}{M} \sum_{i=1}^M v_i \times p_{rj} \times r_{motiv} \right) \left(\sum_{j=1}^w N_2^w \right) + \\ + \left(\frac{1}{KB} \sum_{k=1}^K \sum_{g=1}^B \left(\mu_{kg}^l \times w_{kg}^l \right) \right) \times \left(\sum_{j=1}^w N_2^w \right) \overline{N_1}, \end{array} \right.$$

Модель безпеки соціокіберфізичних систем на основі моделі “хижак-жертва” з урахуванням взаємозв’язків між “видами жертв” та “видами хижаків” (модель 4) визначимо:

$$A_4^{SCS} = \left\{ \begin{aligned} & \frac{dN_1}{dt} = \left(\arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \times K_l^A \right) \times \\ & \times \left(\sum_{i=1}^Q \left(N_{1_i}^C \times A_i^C + N_{1_i}^I \times A_i^I + N_{1_i}^A \times A_i^A + \right. \right. \\ & \left. \left. + N_{1_i}^{Au} \times A_i^{Au} + N_{1_i}^{Aff} \times A_i^{Aff} \right) \right) - \\ & - \left(\sum_{i=1}^M \left(w_{SCSi}^C \cap w_{SCSi}^I \cap w_{SCSi}^A \cap w_{SCSi}^{Au} \cap w_{SCSi}^{Aff} \right) \times \right. \\ & \left. \times \chi_i^{SCS} \right) \times \\ & \times \tilde{N}_1 \left(\sum_{j=1}^w N_2^w \right) - \varepsilon N_1^2; \\ & \frac{dN_2}{dt} = - \left(\frac{1}{M} \sum_{i=1}^M v_i \times p_{rj} \times r_{motiv} \right) \left(\sum_{j=1}^w N_2^w \right) + \\ & + \left(\frac{1}{KB} \sum_{k=1}^K \sum_{g=1}^B \left(\mu_{kg}^l \times w_{kg}^l \right) \right) \times \left(\sum_{j=1}^w N_2^w \right) \overline{N_1 - \xi N_2^2}, \end{aligned} \right.$$

де коефіцієнти $\varepsilon, \zeta > 0$, і описують завдання шкоди “жертви” і “хижака” він відповідно. Запропоновані моделі практично дозволяють враховувати сучасні фінансові, обчислювальні можливості зловмисників. Крім цього, запропонований підхід враховує можливість не тільки впливу на “жертву” за рахунок комплексування цільових (змішаних) атак з методами соціальної інженерії, а також враховувати соціально-політико-економічний стан соціуму, в якому знаходиться “жертва” [41, 56].

2.5. Концепція побудови диференціально-ігрових розподілених систем інформаційної безпеки

Питання захисту об’єктів критичної інфраструктури державного та приватного секторів економіки, побудованих за архітектурою відкритих систем за моделлю OSI від розподілених кібератак (КБа) знаходиться сьогодні в центрі уваги більшості провідних фахівців з інформаційної безпеки. Основною причиною такої уваги є високий ступінь загрози, який несе така кібератака. Підвищення рівня захищеності інформаційних ресурсів об’єктів критичної інфраструктури в розподілених системах є однією з ключових проблем безпеки відкритих систем.

Спираючись на ідею захисту від розподілених кібератак шляхом побудови розподілених систем безпеки, в основу концепції побудови розподілених систем покладемо авторський диференціально-ігровий підхід [62, 107, 114, 115, 117].

На першому етапі розв'яжемо задачу розроблення заходу захисту – диференціально-ігрової політики безпеки об'єкта критичної інфраструктури.

Етап 1. Розроблення диференціально-ігрової політики безпеки: формалізація задачі. Вихідні дані, припущення та обмеження.

Відомо, що при реалізації процесу кібернападу (КБн) бот-мережею у вигляді розподіленої кібератаки (наприклад, DDoS) на об'єкт критичної інфраструктури мережевий трафік втрачає самоподібну структуру.

Тому не всі моделі потоків пакетів заявок, таких, наприклад, як фальшивих запитів на припинення TCP-з'єднання або звуження смуги пропускання каналу передачі інформації, повідомлень електронної пошти з файлами повідомлень до яких інтегровано комп'ютерні черв'яки тощо можливо описати моделями найпростіших потоків.

Зважаючи на це припустимо, що стратегії гравців під час такого інформаційного конфлікту у формалізованому вигляді можна подати як:

-
- для гравців кіберзахисту (КБз):

$$\lambda_i(t) = F_i(\lambda_i, T, t)$$

при обмеженнях:

$$\lambda_{i\min}(t) \leq \lambda_i(t) \leq \lambda_{i\max}(t);$$

- для гравців КБн (реалізують процес КБн – розподілену КБа):

$$\mu_j(t) = F_j(\mu_j, T, t)$$

при обмеженнях:

$$\mu_{j\min}(t) \leq \mu_j(t) \leq \mu_{j\max}(t),$$

де λ_i та μ_j – параметри законів розподілу стратегій i -го та j -го гравців, які невідомі ($i = 0..X$, $j = 0..Y$, де X і Y – кількість гравців КБз та КБн відповідно);

t – часовий аргумент, $t \in [t_0, T]$ (t_0 – початок атаки, T – тривалість ІК);
 $\lambda_{i\min}(t)$ і $\mu_{j\min}(t)$ – мінімальні, а $\lambda_{i\max}(t)$ і $\mu_{j\max}(t)$ – максимальні
інтенсивності потоків КБз та КБа i -го та j -го гравців.

Стратегії гравців $\lambda_i(t)$ та $\mu_j(t)$, що визначають правила розподілу їх
ресурсів, належать замкненим множинам $\Lambda \in E_\lambda$ та $M \in E_\mu$, які обмежені в
евклідових просторах R_λ і R_μ .

Виходячи з прийнятих вище припущень та обмежень на рис. 2.7 в
загальному вигляді графічно подано стратегії гравців в ІК під час реалізації
КБн у вигляді розподіленої КБа на інформаційні ресурси (ІР) об'єкта
критичної інфраструктури (ОКІ).

На рис. 2.8 прийнято такі позначення: ГЗ 1 – перший об'єкт КБз (перший
гравець КБз ОКІ); ГЗ i – i -й об'єкт КБз тощо; ГН 1 – перший гравець КБн,
ГН j – j -й гравець КБн. Штрихпунктирні лінії навколо гравців КБн
позначають гравців, стратегії яких спрямовано на реалізацію розподіленої
атаки на ОКІ, а навколо об'єктів захисту – РСІБ. Тонкими та товстими
стрілками позначено інтенсивності витрат ресурсів гравцями.

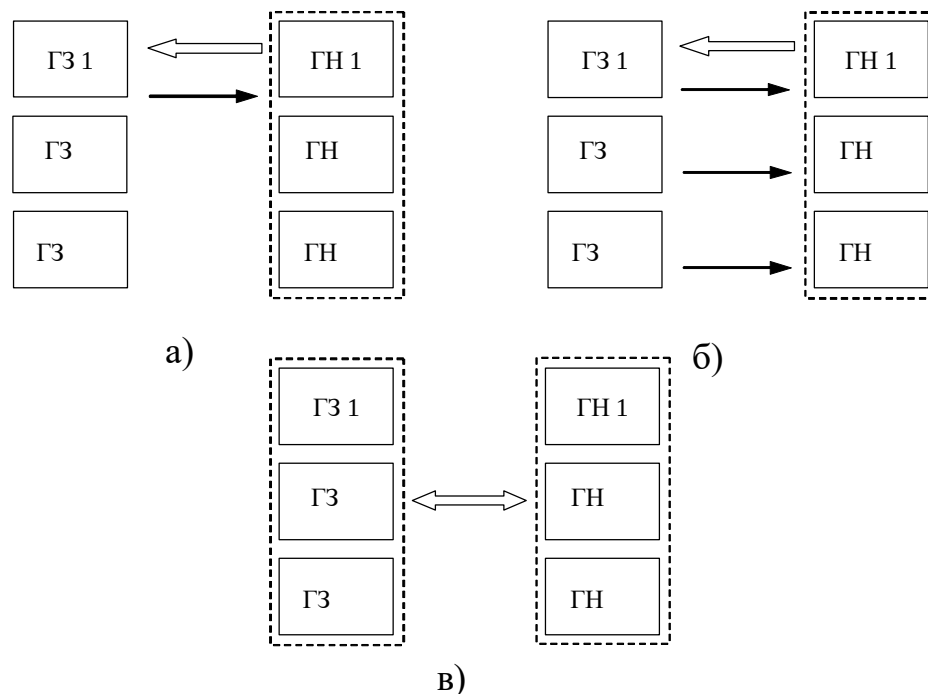


Рис. 2.7. Стратегії гравців під час інформаційного конфлікту:
а – розподілена КБа на ОКІ ГЗ 1; б – розподілена КБа на ОКІ ГЗ 1
при індивідуальному захисті гравців; в – розподілена атака на РСІБ

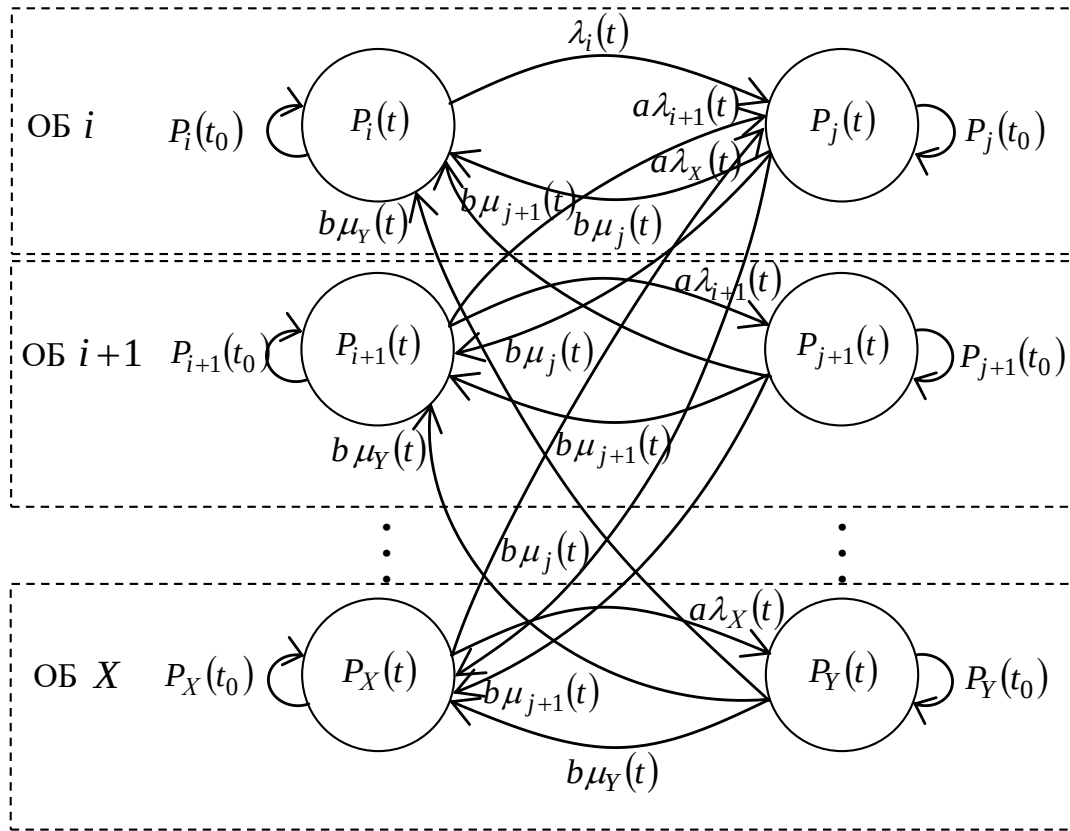


Рис. 2.8. Графова модель станів розподіленої системи інформаційної безпеки під час розподіленої кібератаки

Дослідимо третій варіант реалізації стратегії КБз на ОКІ, який передбачає захист ОКІ від розподіленої КБа шляхом побудови відповідної РСІБ (див. рис. 2.7 в). Спираючись на відому теорему ЗІ про захищеність системи (захищеність системи визначається захищеністю її найменш захищеного об'єкта – ОКІ), формалізація задачі розробки диференціально-ігрової політики безпеки полягає у потребі організації процесу КБз ІР на ОКІ у вигляді розподіленої системи інформаційної безпеки (РСІБ) (див. рис. 2.7 в).

Суть задачі зводиться до зменшення потужності КБа на об'єкт шляхом розосередження її інтенсивності між відповідними гравцями КБз та залученні ресурсів цих гравців для забезпечення заданого РЗ – I_R^G [108, 109]. Другий етап концепції побудови РСІБ [106] зводиться до вирішення задачі розробки засобу захисту – РСІБ, яка підтримує диференціально-ігрову політику безпеки [63].

Етап 2. Розробка диференціально-ігрової РСІБ.

Відповідно до рис. 2.7 в на рис. 2.8 в загальному вигляді подамо графову модель станів РСІБ під час розподіленої КБа. На рис. 2.8 кружками позначено множини можливих станів диференціально-ігрової РСІБ $\{P_X(t)\}$ та $\{P_Y(t)\}$ в яких може перебувати система безпеки ОКІ з відповідними значеннями ймовірності. Над стрілками переходів проставлено інтенсивності потоків, які

переводять систему у відповідні стани. Вагові коефіцієнти a обираються на основі стратегії половинного захисту свого ОКІ X та підтримки захисту ОКІ i гравця КБз, а коефіцієнти b – виходячи зі стратегії, в основу якої покладено рівномірний принцип, тобто $b = X^{-1}$. За початкових умов $P_i(t_0) = 1$, $P_{i+1}(t_0) = \dots = P_Y(t_0) = 0$ та умов нормування $P_i(t_0) + \dots + P_X(t_0) + P_j(t_0) + \dots + P_Y(t_0) = 1$ при відповідних обмеженнях вказаних вище на ресурси гравців, ІК в РСІБ описується системою нелінійних диференціальних рівнянь Колмогорова-Чепмена (див. рис. 2.8):

$$\begin{cases} \frac{dP_i(t)}{dt} = -\lambda_i(t)P_i(t) + b\mu_j(t)P_j(t) + b\mu_{j+1}(t)P_{j+1}(t) + \\ \quad + b\mu_Y(t)P_Y(t); \\ \frac{dP_{i+1}(t)}{dt} = -2a\lambda_{i+1}(t)P_{i+1}(t) + b\mu_j(t)P_j(t) + b\mu_{j+1}(t)P_{j+1}(t) + \\ \quad + b\mu_Y(t)P_Y(t); \\ \quad \vdots \\ \frac{dP_Y(t)}{dt} = -3b\mu_Y(t)P_Y(t) + a\lambda_X(t)P_X(t). \end{cases} \quad (2.1)$$

Рівень захищеності ІР на ОКІ для i -го гравця КБз в РСІБ є платою гравців I_R , що захищаються за витрати власних ресурсів. На інтервалі $t \in [t_0, T]$ плата I_R в загальному вигляді є інтегральною моделлю вигляду:

$$I_R = \frac{1}{T} \int_{t_0}^T P_i(t) dt. \quad (2.2)$$

Для забезпечення заданого РЗ ІР I_R^G в РСІБ гравець КБз обирає свою стратегію відповідно до принципу мінімаксу [118]:

$$\min_{\lambda_i(t) \in E_\lambda} \max_{\mu_j(t) \in E_\mu} = I_R,$$

тобто стратегії $\lambda_i(t)$, що обираються гравцями КБз ГЗ 1 – ГЗ X мінімізують плату (2.2), за умови її максимізації гравцями КБн ГН 1–ГН Y . Гравці КБн ГН 1–ГН Y обирають стратегії $\mu_j(t)$, що максимізують плату (2.2) при умові мінімізації плати гравцями КБз ГЗ 1–ГЗ X :

$$\max_{\mu_j(t) \in E_\mu} \min_{\lambda_i(t) \in E_\lambda} = I_R.$$

При цьому сформульована на першому етапі диференціально-ігрова політика безпеки виконується за умови існування в даній диференціальній грі сідлової точки Δ . Існування сідлової точки Δ забезпечує досягнення РСІБ заданого РЗ ІР на ОКІ:

$$\min_{\lambda_i(t) \in E_\lambda} \max_{\mu_j(t) \in E_\mu} = \max_{\mu_j(t) \in E_\mu} \min_{\lambda_i(t) \in E_\lambda} = I_R^G. \quad (2.3)$$

Таким чином, виконання умови (2.3) гарантує рівність заданого РЗ ІР на ОКІ не гірше за ціну гри I_R^G . Шукана з системи (2.1) траєкторія гри $P_i^{opt}(t)$ при дотриманні гравцями відповідної політики безпеки називається оптимальною та такою, що відображає динаміку протікання процесу КБн в кіберпросторі у вигляді розподіленої КБа на ОКІ. Виконання умови (2.3) також дозволяє стверджувати, що стратегії гравців є оптимальними, тобто $\lambda_i(t) \Rightarrow \lambda_i^{opt}(t)$ і $\mu_j(t) \Rightarrow \mu_j^{opt}(t)$. Існування в грі сідлової точки Δ підтверджує про нераціональність відхилення гравцями від своїх оптимальних стратегій, оскільки кожен з них неминуче програє в платі (2.2).

Оцінювання прогнозованого РЗ ІР на ОКІ I_R^G , що забезпечує створювана диференціально-ігрова РСІБ, а також процедура знаходження траєкторії гри $P_i^{opt}(t)$, пов'язані з обчислюваними труднощами, що впливають з нелінійності системи диференціальних рівнянь (2.1).

Тому для подолання проблеми обчислювальної складності здійснимо процедуру моделювання процесу КБн методом диференціальних перетворень та перейдемо від системи (2.3) в області оригіналів до системи спектральних рівнянь в області зображень [93, 124]:

$$\left\{ \begin{array}{l} \frac{k+1}{H} P_i(k+1) = -\lambda_i(k) * P_i(k) + b \mu_j(k) * P_j(k) + b \mu_{j+1}(k) * P_{j+1}(k) + \\ \quad + b \mu_Y(k) * P_Y(k); \\ \frac{k+1}{H} P_{i+1}(k+1) = -2a \lambda_{i+1}(k) * P_{i+1}(k) + b \mu_j(k) * P_j(k) + \\ \quad + b \mu_{j+1}(k) * P_{j+1}(k) + b \mu_Y(k) * P_Y(k); \\ \vdots \\ \frac{k+1}{H} P_Y(k+1) = -3b \mu_Y(k) * P_Y(k) + a \lambda_X(k) * P_X(k), \end{array} \right. \quad (2.4)$$

де H – масштабна стала, яка обирається рівною тривалості диференціальної гри, що дорівнює тривалості ІК T , $H = T$;

$P_i(k), \dots, P_Y(k)$ – диференціальні спектри для відповідних процесів, що протікають в РСІБ.

В області зображень плата (2.2) виражається через дискрети диференціального спектра $P_i(k)$ моделі (2.4) як:

$$I_R = \sum_{k=0}^{k=\infty} \frac{P_i(k)}{k+1}. \quad (2.5)$$

Умови дотримання диференціально-ігрової політики безпеки передбачають дотримання гравцями оптимальних стратегій $\lambda_i^{opt}(t)$ і $\mu_j^{opt}(t)$ розподілу ресурсів гравців в ІК, які визначаються з умов існування екстремуму функціоналу (2.5), тобто:

$$\left\{ \begin{array}{l} \frac{\partial I(\lambda_i(t), \mu_j(t))}{\partial \lambda_i(t)} = 0; \\ \frac{\partial I(\lambda_i(t), \mu_j(t))}{\partial \mu_j(t)} = 0; \end{array} \right. \Rightarrow \left\{ \begin{array}{l} \lambda_i^{opt}(t); \\ \mu_j^{opt}(t). \end{array} \right. \quad (2.6)$$

Перевірка достатніх умов дозволяє визначити знаки знайдених в (2.6) екстремумів, тобто:

$$\begin{cases} \frac{\partial^2 I(\lambda_i(t), \mu_j(t))}{\partial \lambda_i(t)^2} > 0; \\ \frac{\partial^2 I(\lambda_i(t), \mu_j(t))}{\partial \mu_j(t)^2} < 0; \end{cases} \Rightarrow \begin{cases} \lambda_i^{opt}(t) \rightarrow \lambda_{i\min}^{opt}(t); \\ \mu_j^{opt}(t) \rightarrow \mu_{j\max}^{opt}(t). \end{cases} \quad (2.7)$$

У результаті виконання умов (2.6) та (2.7) стратегії $\lambda_{i\min}^{opt}(t)$ і $\mu_{j\max}^{opt}(t)$ є оптимальними. Існування в грі сідлової точки дозволяє визначити прогнозований рівень захищеності ІР на ОКІ від розподіленої КБа, що забезпечує розроблена у результаті синтезу диференціально-ігрова РСІБ (див. рис. 2.9):

$$I_R^G = \sum_{k=0}^{k=\infty} \frac{P_i^{opt}(k)}{k+1}. \quad (2.8)$$

Кількість дискрет $P_i^{opt}(k)$ в моделі (2.4) варіюється залежно від вимог, що висуваються до точності оцінювання РЗ I_R^G . На практиці, як правило, доцільно обмежитися трьома-чотирма дискретами $P_i^{opt}(0), \dots, P_i^{opt}(3)$.

Таким чином, відновлена за дискретами $P_i^{opt}(k)$ модель процесу КБн, що протікає в РСІБ при виборі гравцями оптимальних стратегій має вигляд:

$$P_i^{opt}(t) = \sum_{k=0}^{k=\infty} \left(\frac{t}{T} \right)^k P_i^{opt}(k). \quad (2.9)$$

Отже, РСІБ, яка розробляється й функціонує за диференціально-ігровою концепцією забезпечує показник захищеності ІР не гірше за заданий [78]. Прогнозований рівень захищеності (РЗ) I_R^G (2.5) досягається за рахунок дотримання гравцями оптимальних стратегій $\lambda_{i\min}^{opt}(t)$ і $\mu_{j\max}^{opt}(t)$, що забезпечує виконання умови (2.3).

2.6. Диференціально-ігрова модель розподіленої системи інформаційної безпеки

У рамках впровадження вищевикладеної концепції синтезуємо РСІБ та оцінимо її ефективність шляхом розробки відповідної диференціально-ігрової моделі [84, 91, 95, 105, 106].

Розроблення диференціально-ігрової політики безпеки: формалізація задачі. Вихідні дані, припущення та обмеження.

Нехай для трьох об'єктів ОБ 1, ОБ 2, ОБ 3, що функціонують за технологією відкритих систем за моделлю OSI, серед яких перший об'єкт ОБ 1 є об'єктом ОКІ, що піддається розподіленій КБа (наприклад *DDoS-атаці*) створюється РСІБ, графова модель станів РСІБ під час розподіленої КБа подано на рис. 2.9 [62].

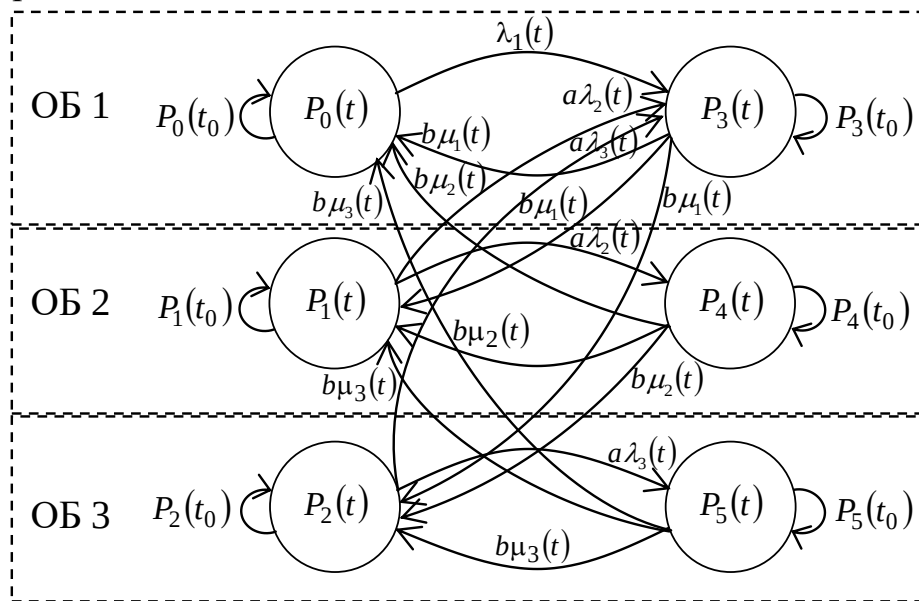


Рис. 2.9. Графова модель станів розподіленої системи інформаційної безпеки під час розподіленої кібератаки

На рис. 2.9 прийнято такі позначення: ОБ 1 – перший об'єкт КБз (перший гравець, що захищає ОКІ); ОБ 2, ОБ 3 – 2-й та 3-й об'єкти КБз відповідно. Усі об'єкти на рис. 2.9 виділено штрихпунктирними лініями. Кружками позначено стани, в яких може перебувати РСІБ. Над стрілками переходів проставлено відповідні інтенсивності потоків, які переводять систему в даний стан. $P_z(t_0)$ – початкові умови при перебуванні системи в z -му стані ($z = \overline{0,5}$), де t_0 – час початку гри. $\lambda_i(t)$ – інтенсивність потоку КБз при переведенні системи в z -й стан, $i = \overline{0,3}$; $\mu_j(t)$ – інтенсивність потоку КБа при переведенні системи в z -й стан, $j = \overline{0,3}$. В термінах теорії диференціальних ігор $\lambda_i(t)$ та $\mu_j(t)$ – це стратегії гравців [65]. Стратегії гравців $\lambda_i(t)$ та $\mu_j(t)$, що визначають правила розподілу їх ресурсів, належать

замкненим множинам $\Lambda \in E_\lambda$ та $M \in E_\mu$, які обмежені в евклідових просторах R_λ і R_μ . Тривалість диференціальної гри T обирається рівною тривалості ІК, що визначається тривалістю розподіленої КБа на ОКІ, де $t \in [t_0, T]$. Гравцем КБз ОБ 1 вжито організаційні, технічні, криптографічні [64, 80, 127–129] та програмні методи захисту інформації [43].

Виходячи з диференціально-ігрової політики безпеки в РСІБ вагові коефіцієнти a та b дорівнюють відповідно $a = \frac{1}{2}$ та $b = \frac{1}{3}$ [62].

Розподілена КБа на ОКІ, що здійснюється декількома гравцями призводить до поступової втрати мережевим трафіком самоподібної структури. Тоді для гравців КБз (див. рис. 2.10) стратегії КБз для КБа І-го та ІІ-го класів можна подати моделями загального вигляду:

$$\lambda_1(t) = \lambda, \quad (2.10)$$

$$\lambda_2(t) = \lambda t, \quad (2.11)$$

$$\lambda_3(t) = e^{\lambda t} \quad (2.12)$$

при обмеженнях описаних вище, а для гравців КБн:

$$\mu_1(t) = \mu, \quad (2.13)$$

$$\mu_2(t) = \mu t, \quad (2.14)$$

$$\mu_3(t) = e^{\mu t} \quad (2.15)$$

при обмеженнях описаних вище відповідно, де λ та μ – параметри законів розподілу стратегій i -го та j -го гравців, які невідомі.

Розробка диференціально-ігрової РСІБ.

Аналіз диференціально-ігрової політики безпеки, сформульованої вище, дозволяє формалізувати ІК в РСІБ при протіканні процесу КБн під час розподіленої КБа у вигляді системи нелінійних диференціальних рівнянь Колмогорова-Чепмена [62]:

$$\left\{ \begin{array}{l} \frac{dP_0(t)}{dt} = -\lambda_1(t)P_0(t) + b\mu_1(t)P_3(t) + b\mu_2(t)P_4(t) + b\mu_3(t)P_5(t); \\ \frac{dP_1(t)}{dt} = -2a\lambda_2(t)P_1(t) + b\mu_1(t)P_3(t) + b\mu_2(t)P_4(t) + b\mu_3(t)P_5(t); \\ \frac{dP_2(t)}{dt} = -2a\lambda_3(t)P_2(t) + b\mu_1(t)P_3(t) + b\mu_2(t)P_4(t) + b\mu_3(t)P_5(t); \\ \frac{dP_3(t)}{dt} = -3b\mu_1(t)P_3(t) + \lambda_1(t)P_0(t) + a\lambda_2(t)P_1(t) + a\lambda_3(t)P_2(t); \\ \frac{dP_4(t)}{dt} = -3b\mu_2(t)P_4(t) + a\lambda_2(t)P_1(t); \\ \frac{dP_5(t)}{dt} = -3b\mu_3(t)P_5(t) + a\lambda_3(t)P_2(t). \end{array} \right. \quad (2.16)$$

Система (2.16) справедлива за наступних початкових умов $P_0(t_0)=1$, $P_2(t_0)=\dots=P_5(t_0)=0$ та умов нормування $P_0(t_0)+\dots+P_5(t_0)=1$ при відповідних обмеженнях на ресурси гравців (2.10)–(2.15) та (2.13)–(2.15) відповідно.

Плата I , що є критерієм оптимізації, може бути подана як модель інтегральної оптимальності вигляду (2.2). Для забезпечення заданого РЗ ІР в РСІБ гравці КБз обирають свої стратегії відповідно до диференціально-ігрової політики безпеки й дотримуються принципу мінімаксу. Для визначення стратегій гравців $\lambda_i^{opt}(t)$ і $\mu_j^{opt}(t)$, що забезпечують дотримання диференціально-ігрової політики безпеки застосуємо операційний метод диференціальних перетворень.

Перейдемо від моделі (2.16) в області оригіналів до її спектральної моделі в області зображень, врахувавши: по-перше що масштабна стала H дорівнює тривалості ІК T , тобто $H=T$; по-друге зображення для стратегій (2.10)–(2.15) та (2.13)–(2.15) відповідно, мають вигляд:

$$\lambda_1(k) = \lambda_3(k) = \begin{cases} \lambda, & k=0; \\ 0, & k \geq 1, \end{cases} \quad (2.17)$$

$$\lambda_2(k) = \lambda_4(k) = \begin{cases} \lambda T, & k=1; \\ 0, & k \neq 1, \end{cases} \quad (2.18)$$

$$\lambda_3(k) = \frac{(\lambda T)^k}{k!}, \quad (2.19)$$

$$\mu_1(k) = \mu \mathfrak{b}(k) = \begin{cases} \mu, & k = 0; \\ 0, & k \geq 1, \end{cases} \quad (2.20)$$

$$\mu_2(k) = \mu T \mathfrak{b}(k-1) = \begin{cases} \mu T, & k = 1; \\ 0, & k \neq 1, \end{cases} \quad (2.21)$$

$$\mu_3(k) = \frac{(\mu T)^k}{k!}. \quad (2.22)$$

У результаті отримаємо систему спектральних рівнянь:

$$\left\{ \begin{aligned} P_0(k+1) &= \frac{T}{k+1} \left[-\lambda P_0(k) + \frac{1}{3} \mu P_3(k) + \frac{1}{3} \mu T P_4(k-1) + \right. \\ &\quad \left. + \frac{1}{3} \sum_{l=0}^k \frac{(\mu T)^{k-l}}{(k-l)!} P_5(l) \right]; \\ P_1(k+1) &= \frac{T}{k+1} \left[-\lambda T P_1(k-1) + \frac{1}{3} \mu P_3(k) + \frac{1}{3} \mu T P_4(k-1) + \right. \\ &\quad \left. + \frac{1}{3} \sum_{l=0}^k \frac{(\mu T)^{k-l}}{(k-l)!} P_5(l) \right]; \\ P_2(k+1) &= \frac{T}{k+1} \left[-\sum_{l=0}^k \frac{(\lambda T)^{k-l}}{(k-l)!} P_2(l) + \frac{1}{3} \mu P_3(k) + \right. \\ &\quad \left. + \frac{1}{3} \mu T P_4(k-1) + \frac{1}{3} \sum_{l=0}^k \frac{(\mu T)^{k-l}}{(k-l)!} P_5(l) \right]; \\ P_3(k+1) &= \frac{T}{k+1} \left[-\mu P_3(k) + \lambda P_0(k) + \frac{1}{2} \lambda T P_1(k-1) + \right. \\ &\quad \left. + \frac{1}{2} \sum_{l=0}^k \frac{(\lambda T)^{k-l}}{(k-l)!} P_2(l) \right]; \\ P_4(k+1) &= \frac{T}{k+1} \left[-\mu T P_4(k-1) + \frac{1}{2} \lambda T P_1(k-1) \right]; \\ P_5(k+1) &= \frac{T}{k+1} \left[-\sum_{l=0}^k \frac{(\mu T)^{k-l}}{(k-l)!} P_5(l) + \frac{1}{2} \sum_{l=0}^k \frac{(\lambda T)^{k-l}}{(k-l)!} P_2(l) \right], \end{aligned} \right. \quad (2.23)$$

де $\{P_z(k)\}$ – диференціальні спектри для відповідних процесів, що протікають в РСІБ, k – цілочисловий аргумент, $k = 0, 1, 2$.

Виходячи з спектральної моделі ІК (2.23) дискрети спектральної диференціально-ігрової моделі процесу КБн $P_0(k)$ при відповідних значеннях цілочислового аргументу $k = 0, 1, 2$ дорівнюють:

$$P_0(0) = [P_0(t_0)] = 1, \quad (2.24)$$

$$P_0(1) = -\lambda T, \quad (2.25)$$

$$P_0(2) = \frac{1}{2} \lambda \left(\lambda + \frac{1}{3} \mu \right) T, \quad (2.26)$$

$$P_0(3) = -\frac{1}{6} \lambda \left(\lambda \left(\lambda + \frac{1}{3} \mu \right) + \frac{1}{3} \mu (\lambda + \mu) \right) T^3. \quad (2.27)$$

Спектральна модель для плати (2.12) з урахуванням дискрет (2.24)–(2.27) визначатиметься як:

$$I_R \approx 1 - \lambda T + \frac{1}{2} \lambda \left(\lambda + \frac{1}{3} \mu \right) T - \frac{1}{6} \lambda \left(\lambda \left(\lambda + \frac{1}{3} \mu \right) + \frac{1}{3} \mu (\lambda + \mu) \right) T^3. \quad (2.28)$$

Для знаходження оптимальних стратегій $\lambda_i^{opt}(t)$ і $\mu_j^{opt}(t)$, знайдемо стаціонарні точки для функціонала (2.28) відповідно до необхідних умов (2.16). Дослідження функціонала (2.28) на екстремум (2.16) зводиться до розв'язання СЛАР вигляду:

$$\begin{cases} -\frac{1}{2}T + \frac{1}{6}\left(\lambda + \frac{1}{3}\mu\right)T^2 + \frac{1}{6}\lambda T^2 = 0; \\ \frac{1}{18}\lambda T^2 - \frac{1}{36}\lambda(\lambda + \mu)T^3 = 0, \end{cases} \quad (2.29)$$

звідки:

$$\begin{aligned} \lambda^{opt} &= \frac{7}{5T}, \\ \mu^{opt} &= \frac{3}{5T}. \end{aligned} \quad (2.30)$$

Виконання достатніх умов (2.30):

$$\begin{cases} \frac{1}{3}T^2 > 0; \\ -\frac{1}{36}\lambda T^3 < 0, \end{cases} \quad (2.31)$$

дозволяє стверджувати, що параметри законів розподілу стратегій гравців є відповідно:

$$\begin{aligned}\lambda_{\min}^{opt} &= \frac{7}{5T}, \\ \mu_{\max}^{opt} &= \frac{3}{5T}.\end{aligned}\tag{2.32}$$

Виконання необхідних (2.16) і достатніх (2.17) умов дозволяє стверджувати, що набір стратегій гравців (2.10)–(2.12) та (2.13)–(2.15) з параметрами є оптимальним і в даній диференціальній грі існує сідлова точка.

Ціна гри, що визначає прогнозований рівень захищеності ІР в РСІБ (див. рис. 2.9) з урахуванням (2.30) дорівнює:

$$I_R^G = \frac{779}{1500}.\tag{2.33}$$

В часовій області при виборі гравцями оптимальних стратегій відповідно до (2.19) диференціально-ігрова модель гарантовано захищеної РСІБ, що описує процес КБн при розподіленій КБа матиме вигляд:

$$P_0^{opt}(t) \approx 1 - \frac{7}{5} \frac{t}{T} + \frac{28}{25} \left(\frac{t}{T} \right)^2 - \frac{77}{125} \left(\frac{t}{T} \right)^3.\tag{2.34}$$

Таким чином, для забезпечення заданого РЗ ІР в РСІБ гравцям потрібно дотримуватися таких стратегій [120]:

– гравцям КБз:

$$\lambda_{1\min}^{opt}(t) = \frac{7}{5T},\tag{2.35}$$

$$\lambda_{2\min}^{opt}(t) = \frac{7}{5} \frac{t}{T},\tag{2.36}$$

$$\lambda_{3\min}^{opt}(t) = e^{\frac{7}{5} \frac{t}{T}};\tag{2.37}$$

– гравцям КБн:

$$\mu_{1\max}^{opt}(t) = \frac{3}{5T},\tag{2.38}$$

$$\mu_{2\max}^{opt}(t) = \frac{3}{5} \frac{t}{T}, \quad (2.39)$$

$$\mu_{3\max}^{opt}(t) = e^{\frac{3}{5}(\frac{t}{T})}. \quad (2.40)$$

Таким чином, дотримання гравцями КБз оптимальних стратегій (2.25)–(2.27) дозволяє реалізувати основні функції МЕ для захисту ОКІ, на якому СІБ побудована за концепцією диференціально-ігрової РСІБ.

2.7. Диференціально-ігрова нетейлорівська модель

Застосуємо до диференціально-ігрової моделі $\frac{dP_0(t)}{dt} = -\lambda(t)P_0(t) + \mu(t)(1 - P_0(t))$ диференціальні перетворення. Як наслідок, за початкових умов $P_0(t_0) = 1$, її спектральна модель $P_0(k+1)$ матиме вигляд:

$$P_0(k+1) = \frac{T}{k+1} (\mu \text{ в } (k) - (\lambda + \mu) P_0(k)), \quad (2.41)$$

де T – час закінчення гри, що дорівнює масштабній сталій H , $H = T$;

λ , μ – інтенсивності потоку КБз та КБа, відповідно;

$$\text{в}(k) - \text{теда [116], } \text{в}(k) = \begin{cases} 1, & k = 0; \\ 0, & k \geq 1. \end{cases}$$

Умови нормування для спектральної моделі [113, 123, 125] (2.41) та критерій оптимізації аналогічні описаній в попередньому підрозділі [62].

Для пошуку вигляду траєкторії диференціальної гри за спектральною моделлю (2.41) обмежимося її першими чотирма дискретами. Присвоївши цілочисловому аргументу k значення $k = 0, 1, 2$ перші чотири дискрети дорівнюватимуть:

$$P_0(0) = [P_0(t=0)] = 1, \quad (2.42)$$

$$P_0(1) = -\lambda T, \quad (2.43)$$

$$P_0(2) = \frac{1}{2} \lambda(\lambda + \mu) T^2, \quad (2.44)$$

$$P_0(3) = -\frac{1}{6} \lambda (\lambda + \mu)^2 T^3. \quad (2.45)$$

Нехай диференціально-ігрова нетейлорівська модель $P_0^{NT}(t)$ є відрізком ряду Діріхле вигляду:

$$P_0^{NT}(t) = A_1 e^{u_1 t} + A_2 e^{u_2 t}, \quad (2.46)$$

де A_1 , A_2 , u_1 та u_2 – коефіцієнти ряду, що підлягають визначенню. Тоді спектральне рівняння для моделі (2.46) відповідно до (2.41) матиме вигляд:

$$A_1 u_1^k + A_2 u_2^k = \frac{k! P_0(k)}{H^k} = P_{0k}, \quad P_{0k} = \left[\frac{d^k P_0(t)}{dt^k} \right]_{t=0}. \quad (2.47)$$

Присвоївши послідовно цілочислові значення аргументу $k = 0, 1, 2$, складається СЛАР

$$\begin{array}{|c|c|} \hline 1 & 1 \\ \hline u_1 & u_2 \\ \hline u_1^2 & u_2^2 \\ \hline u_1^3 & u_2^3 \\ \hline \end{array} \begin{array}{|c|} \hline A_1 \\ \hline A_2 \\ \hline \end{array} = \begin{array}{|c|} \hline P_{00} \\ \hline P_{01} \\ \hline P_{02} \\ \hline P_{03} \\ \hline \end{array}. \quad (2.48)$$

Праві частини СЛАР (3.9) з урахуванням (2.42)–(2.45) та (2.47) дорівнюватимуть:

$$P_{00} = 1, \quad (2.49)$$

$$P_{01} = -\lambda, \quad (2.50)$$

$$P_{02} = \lambda(\lambda + \mu), \quad (2.51)$$

$$P_{03} = -\lambda(\lambda + \mu)^2. \quad (2.52)$$

З урахуванням (2.49)–(2.52) система (2.48) може бути подана у формі:

$$u_1 = \frac{-\lambda(\lambda + \mu)^2 - u_2^3 A_2}{\lambda(\lambda + \mu) - u_2^2 A_2}, \quad (2.53)$$

$$u_2 = \frac{-\lambda - u_1 A_1}{1 - A_1}, \quad (2.54)$$

$$A_1 = \frac{-\lambda(\lambda + \mu)^2 - u_2^3 A_2}{u_1^3}, \quad (2.55)$$

$$A_2 = \frac{-\lambda - u_1 A_1}{u_2} \quad (2.56)$$

і вирішена методом ітерації. У результаті отримаємо такі рішення:

$$u_1 = -(\lambda + \mu), \quad (2.57)$$

$$u_2 = 0, \quad (2.58)$$

$$A_1 = \frac{\lambda}{\lambda + \mu}, \quad (2.59)$$

$$A_2 = \frac{\mu}{\lambda + \mu}. \quad (2.60)$$

Таким чином, диференціально-ігрова нетейлорівська модель процесу КБн відновлена у вигляді ряду Діріхле з урахуванням (2.57)–(2.60), матиме вигляд:

$$P_0^{NT}(t) = \frac{\lambda}{\lambda + \mu} e^{-(\lambda + \mu)t} + \frac{\mu}{\lambda + \mu}. \quad (2.61)$$

Для оцінювання точності моделі (2.61) взято відрізок ряду Тейлора за тими ж вихідними даними, що й дана модель, тобто:

$$P_0(t) = 1 - \lambda t + \frac{1}{2} \lambda(\lambda + \mu)t^2 - \frac{1}{6} \lambda(\lambda + \mu)^2 t^3. \quad (2.63)$$

Точність моделей (2.61) і (2.63) перевірено шляхом обчислення значень відповідних функцій у точці $t = 1$ при $\lambda = \mu = 1$. Як впливає з одержаних результатів $P_0^{NT}(t) = 0.5685$ та $P_0(t) = 0.3333$. Отже, точність моделювання диференціальними перетвореннями нетейлорівського типу (2.47) з використанням 4-х дискрет диференціального спектра в 1,7 разів більше в порівнянні з основними диференціальними перетвореннями. Оптимальні стратегії гравців та ціна гри для моделі (2.61) визначаються аналогічно як і для тейлорівських моделей. Таким чином, застосування ДП нетейлорівського типу

дозволяє отримувати клас точних, в рамках нетейлорівської теорії, диференціально-ігрових нетейлорівських моделей процесів КБн [112].

Отже, застосування диференціально-ігрової нетейлорівської моделі усуває протиріччя між потребою забезпечення високої точності моделі та зниження її аналітичної складності. Але слід зауважити, що при дослідженні ІК в СІБ ОКІ, динаміка яких описується системами лінійних та нелінійних диференціальних рівнянь, кількість рівнянь в яких є більше чотирьох, можуть виникати труднощі з аналітичною складністю отримуваних рішень [116].

2.8. Синтез оптимальної поведінки в системі кіберзахист-кібератака

Типовою задачею дослідження поведінки СІБ в умовах КБн є оптимальний розподіл ресурсів гравця КБз відносно ресурсів гравця КБн [88, 90]. Для двох протидіючих систем одна з яких є гравцем (системою атаки (СА)) здійснює кібернапад на ІР другої системи – СІБ, гравця КБз. Для цього СА використовує певну кількість методів і засобів КБн. Засоби КБн СА складаються з S_1 типів, причому в деяких умовних одиницях кількість засобів m -го типу дорівнює a_m . Сумарний атакуючий ресурс (потенціал) СА M_1

становить величину, що дорівнює $M_1 = \sum_{m=1}^{S_1} a_m$. Аналогічно СІБ складається з

S_2 типів підсистем захисту, причому кількість засобів захисту j -го типу в умовних одиницях дорівнює d_j . Сумарний захисний потенціал СІБ M_2

визначається як $M_2 = \sum_{j=1}^{S_2} d_j$.

Інформаційний ресурс, що підлягає захисту має n інформаційних блоків $B_1, \dots, B_n$, причому цінність B_i -го блоку оцінюється деякою умовною величиною v_i , де $i=1, \dots, n$. Нехай також інформаційні блоки $B_1, \dots, B_n$ упорядковані за їх цінністю, тобто $v_1 \geq \dots \geq v_n$.

Припустимо, що кожен незахищений інформаційний блок B_i під час КБн та реалізації однієї КБа засобами m -го типу втрачає свої властивості – цілісність, доступність та конфіденційність. Величина втрат від КБа на ІР в СІБ на B_i -й інформаційний блок оцінюються величиною $v_i \varepsilon_m$.

Величину сумарних втрат цілісності, доступності та конфіденційності ІР $I(\lambda, \mu)$, що визначають його РЗ при наявності КБа та протидії ним можна

оцінити величиною пропорційною різниці їх сумарної кількості, якщо ця різниця позитивно визначена і рівною нулю в – протилежному випадку, тобто плата дорівнюватиме [119, 126]:

$$I(\lambda, \mu) = \sum_{i=1}^n v_i \max \left\{ 0, \sum_{m=1}^{S_1} \varepsilon_m \left(\mu_{im} - \sum_{j=1}^{S_2} \lambda_{mj} \lambda_{ij} \right) \right\}, \quad (2.64)$$

де μ_{im} – інтенсивність потоку КБа виділених СА для КБа на V_i -й інформаційний блок засобами КБн m -го типу;

λ_{ij} – інтенсивність потоку КБз виділених СІБ для захисту V_i -го інформаційного блоку засобами КБз j -го типу;

λ_{mj} – інтенсивність потоку КБз, що виділяється СІБ для відбиття КБа від засобів m -го типу засобами КБз j -го типу.

Розподіл засобів КБз j -го типу, що виділяються СІБ для відбиття КБа від засобів m -го типу за умови $\sum_{m=1}^{S_1} \lambda_{mj} = 1$, $1 \leq j \leq S_2$ та $1 \leq m \leq S_1$ може бути поданий у матричному вигляді:

$$\Lambda = \|\lambda_{mj}\| \quad (2.65)$$

за відповідних обмежень:

$$0 \leq \lambda_{mj} \leq \lambda_{mj_{\max}}, \quad (2.66)$$

де $\lambda_{mj_{\max}}$ – максимальна інтенсивність потоку захисних дій, $\lambda_{mj_{\max}} = 1$.

Нехай сумарна величина втрат ІР в СІБ $I(\lambda, \mu)$ (2.64) виступатиме основною характеристикою ІК, джерелом якого є протиріччя інтересів СІБ та СА. Варіюючи своєю поведінкою в ІК СІБ намагається підвищити РЗ ІР шляхом зменшення величини сумарних втрат (2.64), що наносяться атакуючими діями СА. Ціль СА – протилежна. Тому функція (2.64) може бути прийнята як плата СІБ системі атаки. У результаті задача синтезу оптимальної поведінки в системі кіберзахист-кібератака зводиться до антагоністичної гри двох гравців з опуклою по одній змінній λ функцією виграшу $I(\lambda, \mu)$ при

довільному фіксованому значенні другої змінної μ .

Виходячи з методики знаходження розв'язків антагоністичних ігор для опуклих по одній змінній функцій виграшу сформулюємо задачу синтезу оптимальної поведінки в системі кіберзахист-кібератака у вигляді наступної теореми.

Теорема 2.1. Нехай плата $I(\lambda, \mu)$ є неперервною за двома змінними λ та μ функцією виграшу для антагоністичної гри, яка строго опукла по λ для кожного довільно фіксованого μ і така, що має на одиничному інтервалі першу похідну по λ . Тоді існує єдина оптимальна стратегія захисту для СІБ λ^{opt} , що є ступінчатою функцією плати $I(\lambda^{opt}, \mu)$, причому $\lambda^{opt} = const$ та є єдиним розв'язком рівняння:

$$I(\lambda^{opt}, \mu) = \max_{0 \leq \mu \leq 1} I(\lambda^{opt}, \mu). \quad (2.67)$$

У випадку вибору обома гравцями СА та СІБ оптимальних стратегій μ^{opt} та λ^{opt} відповідно ціна гри I^* може бути визначена як:

$$I^* = \min_{0 \leq \lambda \leq 1} \max_{0 \leq \mu \leq 1} I(\lambda^{opt}, \mu^{opt}). \quad (2.68)$$

Доведення теореми 2.1. Оптимальна стратегія гравця КБн μ^{opt} може бути визначена в залежності від значення оптимальної стратегії гравця КБз λ^{opt} . Якщо гравець КБз обирає одну з оптимальних стратегій:

$$\lambda^{opt} = \begin{cases} 1, & \frac{\partial I(\lambda^{opt}, \mu^{opt})}{\partial \lambda} \leq 0; \\ 0, & \frac{\partial I(\lambda^{opt}, \mu^{opt})}{\partial \lambda} > 0, \end{cases} \quad (2.69)$$

то гравець КБн обиратиме таку оптимальну стратегію $\mu^{opt} = const$, що буде задовольняти умовам:

$$0 \leq \mu^{opt} \leq 1 \quad (2.70)$$

та (2.68).

Якщо гравець КБз відхиляється від оптимальної стратегії λ^{opt} у

границях обмежень $0 < \lambda < 1$, то гравець КБн обиратиме стратегію вигляду:

$$\mu(\alpha) = \alpha I(\lambda, \mu_1) + (1 - \alpha) I(\lambda, \mu_2), \quad (2.71)$$

де α, μ_1, μ_2 – довільні сталі, що задовольняють умовам:

$$\begin{aligned} 0 \leq \alpha \leq 1, 0 \leq \mu_1 \leq 1, 0 \leq \mu_2 \leq 1, I(\lambda^{opt}, \mu_1) = I(\lambda^{opt}, \mu_2) = I, \\ \frac{\partial I(\lambda^{opt}, \mu_1)}{\partial \lambda} \geq 0, \alpha \frac{\partial I(\lambda^{opt}, \mu_1)}{\partial \lambda} + (1 - \alpha) \frac{\partial I(\lambda^{opt}, \mu_2)}{\partial \lambda} = 0. \end{aligned} \quad (2.72)$$

Зауваження 2.1. Накладені на функцію плати $I(\lambda, \mu)$ вимоги можливо послабити.

По-перше можна знехтувати умовами існування похідних. Але у даному випадку передбачається існування односторонніх похідних функції $I(\lambda, \mu)$ в кожній точці інтервалу її визначення, за виключенням деякої зліченної і скінченної кількості точок. Тоді умови накладені на похідні $\frac{\partial I(\lambda^{opt}, \mu_1)}{\partial \lambda}$ і $\frac{\partial I(\lambda^{opt}, \mu_2)}{\partial \lambda}$ замінюються відповідними умовами для односторонніх похідних у вказаних точках.

По-друге умову строгої опуклості функції виграшу $I(\lambda, \mu)$ можна послабити, замінивши її умовою, що вона є просто опуклою. Але це призводить до того, що оптимальні стратегії як для першого μ^{opt} так і для другого λ^{opt} гравців не є єдиними.

Твердження 2.2. На основі теореми 2.1 та з урахуванням сформульованого зауваження 3.1 чиста оптимальна стратегія КБз СІБ λ^{opt} може бути визначена з рівняння

$$\inf_{\lambda} \sup_{\mu} I(\lambda, \mu) = \sup_{\mu} I(\lambda^{opt}, \mu) = I. \quad (2.73)$$

Враховавши це СА обирає змішану оптимальну стратегію $\mu^*(\alpha)$, що є певною опуклою комбінацією скінченної кількості чистих стратегій.

Введемо деякі позначення. Нехай $X_i = \|\mu_{i1}, \dots, \mu_{iS_1}\|$, $Y_i = \|\lambda_{i1}, \dots, \lambda_{iS_2}\|$, $\xi_i = \|v_i \varepsilon_1, \dots, v_i \varepsilon_{S_1}\|$. Тоді плата з урахуванням прийнятих позначень може бути

подана у матричній формі:

$$I(\lambda, \mu) = \sum_{i=1}^n \max \{ 0, \xi'(X_i - \Lambda Y_i) \}, \quad (2.74)$$

де ξ' – транспонована матриця до матриці ξ .

Оскільки функція плати $I(\lambda, \mu)$ опукла по λ для кожного довільно фіксованого μ , то СА при побудові оптимальної стратегії μ^{opt} може використовувати рандомізовану лише серед тих чистих стратегій, які є вершинами симплекса:

$$\mu^{opt} = \left\{ \sum_{i=1}^{S_1} \delta_i \alpha_i \right\}, \quad (2.75)$$

де $\delta_i \geq 0$, $\sum_{i=1}^{S_1} \delta_i = 1$. При цьому плата з урахуванням (2.75) набуватиме вигляду:

$$I(\lambda, \mu) = I\left(\lambda, \sum_{i=1}^{S_1} \delta_i \alpha_i\right) \leq \sum_{i=1}^{S_1} \delta_i I(\lambda, \alpha_i). \quad (2.76)$$

Позначимо через I_m частину ціни гри I^* , яка може бути отримана СА за рахунок застосування засобів КБа m -го типу, так що $\sum_{m=1}^{S_1} I_m = I^*$ і $Q = \|a_1, \dots, a_{S_1}\|$. Тоді для визначення стратегії КБз B_i -го інформаційного блоку для СІБ згідно з сформульованою теоремою 2.1 отримуємо матричне рівняння:

$$Q - \Lambda Y_i = I_i. \quad (2.77)$$

Для розв'язку матричного рівняння (2.77) доцільно застосувати узагальнену обернену матрицю Мура-Пенроуза.

Нехай для прямокутної матриці Λ (2.65) існує узагальнена обернена матриця Мура-Пенроуза Λ^+ для якої справедливі наступні умови:

$$\Lambda \Lambda^+ \Lambda = \Lambda, \quad \Lambda^+ \Lambda \Lambda^+ = \Lambda^+, \quad (\Lambda \Lambda^+)^* = \Lambda \Lambda^+, \quad (\Lambda^+ \Lambda)^* = \Lambda^+ \Lambda, \quad (2.78)$$

де Λ^* – ермітово спряжена матриця, яка для матриці Λ над полем дійсних чисел є транспонованою, тобто $\Lambda^* = \Lambda'$. Так для неособливої прямокутної матриці Λ визначена таким чином узагальнена обернена матриця Λ^+ співпадає зі звичайною зворотною матрицею Λ^{-1} , тобто $\Lambda^+ = \Lambda^{-1} = \|\beta_{ij}\|$.

З урахуванням властивостей узагальненої оберненої матриці (2.78) з матричного рівняння (2.78) отримуємо:

$$Y_i = \Lambda^+(Q - I_i), \quad (2.79)$$

звідки стратегія захисту B_i - го інформаційного блоку засобами захисту j - го типу СІБ λ_{ij} , що визначає інтенсивність потоку КБз з урахуванням прийнятих вище позначень приймає вигляд:

$$\lambda_{ij} = \sum_{m=1}^{S_1} \beta_{jm} \left(a_m - \frac{I_m}{v_i \varepsilon_m} \right). \quad (2.80)$$

Припустимо, що СІБ розміщує свої засоби протидії j - го типу серед найбільш цінної інформації $\psi(j)$, тобто:

$$\lambda_{\psi(j)+1, j} = \lambda_{\psi(j)+2, j} = \dots = \lambda_{n, j} = 0. \quad (2.81)$$

Сумуючі величини (3.68) за всіма n інформаційними блоками $B_1, \dots, B_n$ та враховуючи припущення (3.69), визначаємо стратегію КБз для гравця КБз на випадок захисту найбільш цінного ІР:

$$\sum_{i=1}^{\psi(j)} \lambda_{ij} = \psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m - L_{\psi(j)} \sum_{m=1}^{S_1} \beta_{jm} \frac{I_m}{\varepsilon_m}, \text{ де } L_{\psi(j)} = \sum_{i=1}^{\psi(j)} \frac{1}{v_i}. \quad (2.82)$$

Так як $\sum_{i=1}^{\psi(j)} \lambda_{ij} = d_j$ згідно прийнятого припущення, то з (2.82) маємо:

$$\sum_{m=1}^{S_1} \beta_{jm} \frac{I_m}{\varepsilon_m} = \frac{1}{L_{\psi(j)}} \left[\psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m - d_j \right]. \quad (2.83)$$

Позначимо $W = \left\| \frac{I_1}{\varepsilon_1}, \dots, \frac{I_{S_1}}{\varepsilon_{S_1}} \right\|$, $S = \left\| \begin{array}{cccc} \frac{\psi(1)}{L_{\psi(1)}} & 0 & \dots & 0 \\ & \frac{\psi(2)}{L_{\psi(2)}} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \frac{\psi(S_2)}{L_{\psi(S_2)}} \end{array} \right\|$,

$$R = \left\| \frac{d_1}{\psi(1)}, \dots, \frac{d_{S_1}}{\psi(S_2)} \right\|.$$

Виходячи з прийнятих позначень перейдемо від рівняння (2.83) до його матричної форми:

$$\Lambda^+ W = S (\Lambda^+ Q - R). \quad (2.84)$$

Скориставшись властивостями узагальненої оберненої матриці з виразу (2.84) після спрощень маємо:

$$W = \Lambda S (\Lambda^+ Q - R), \quad (2.85)$$

звідки частина ціни гри I_m , що є платою СІБ за втрати найбільш цінного ІР, визначається як:

$$I_m = \varepsilon_m \sum_{j=1}^{S_2} \frac{\lambda_{mj}}{L_{\psi(j)}} \left[\psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m - d_j \right]. \quad (2.86)$$

Твердження 3.3. Система атаки, поступить оптимально, якщо реалізувати КБн на найбільш цінний ІР $\psi = \max \psi(j)$, що захищається СІБ з деякою ймовірністю p_i . При цьому ціна гри для СА може бути визначена як:

$$I^* = \sum_{m=1}^{S_1} I_m = \sum_{m=1}^{S_1} \sum_{j=1}^{S_2} \frac{\varepsilon_m \lambda_{mj}}{L_{\psi(j)}} \left[\psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m - d_j \right]. \quad (2.87)$$

Слідство з теореми 2.1. Математичне очікування виграшу від КБа усіма засобами КБн на кожен блок інформації B_i , що захищається усіма засобами захисту СІБ не залежить від номеру інформаційного блоку i , тобто $p_i v_i = c = \text{const}$. Врахувавши умову нормування $\sum_{i=1}^{\psi} p_i = 1$, маємо:

$$p_i = \begin{cases} c/v_i, & 1 \leq i \leq \psi; \\ 0, & i > \psi, \end{cases} \quad \text{де } c = \left(\sum_{i=1}^{\psi} \frac{1}{v_i} \right)^{-1} = \frac{1}{L_{\psi}}.$$

Таким чином, синтез оптимальної поведінки в системі кіберзахист-кібератака визначається відповідно оптимальними стратегіями гравців в ІК, вирази (2.75) та (2.80) відповідно.

Для доведення сформульованих тверджень 3.2 і 3.3 розглянемо модельний приклад.

Нехай стратегія КБн СА не є оптимальною. Тоді виходячи з матричного рівняння (2.85) втрати ІР в СІБ не перевищуватимуть деякої величини E_2 , тобто:

$$\begin{aligned} E_2 &= v_i \sum_{m=1}^{S_1} \varepsilon_m \left\{ \mu_{im} - \sum_{j=1}^{S_2} \lambda_{mj} \left[\beta_{jm} \left(a_m - \frac{I_m}{v_i \varepsilon_m} \right) \right] \right\} \leq \\ &\leq v_i \left\{ \sum_{m=1}^{S_1} \varepsilon_m \left[a_m - \sum_{j=1}^{S_2} \sum_{m=1}^{S_1} \beta_{jm} a_m \lambda_{mj} + \sum_{j=1}^{S_2} \sum_{m=1}^{S_1} \beta_{jm} \frac{I_m}{v_i \varepsilon_m} \lambda_{mj} \right] \right\} = \\ &= v_i \left\{ \sum_{m=1}^{S_1} \varepsilon_m a_m - \left[\sum_{m=1}^{S_1} \varepsilon_m a_m + \sum_{m=1}^{S_1} \frac{I_m}{v_i} \right] \right\} = I. \end{aligned} \quad (2.88)$$

Нехай СІБ реалізує довільну стратегію КБз, але таку, що не є оптимальною. Тоді вибір СА оптимальної стратегії гарантує їй виграш в платі E_1 не менше ціни гри I^* (2.87), тобто:

$$E_1 = \sum_{i=1}^{\psi} \frac{1}{v_i} \sum_{m=1}^{S_1} \varepsilon_m \left[a_m - \sum_{j=1}^{S_2} \lambda_{mj} \lambda_{ij} \right] = \quad (2.89)$$

$$\begin{aligned}
&= \frac{\psi}{L_\psi} \varepsilon_m \left[\sum_{j=1}^{S_2} \sum_{m=1}^{S_1} \beta_{jm} a_m \lambda_{mj} \right] - \sum_{i=1}^{\psi} \frac{1}{L_\psi} \sum_{m=1}^{S_1} \varepsilon_m \sum_{j=1}^{S_2} \lambda_{mj} \lambda_{ij} \geq \\
&\geq \sum_{m=1}^{S_1} \varepsilon_m \sum_{j=1}^{S_2} \left[\psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m \lambda_{mj} \right] \frac{1}{L_{\psi(j)}} - \sum_{m=1}^{S_1} \varepsilon_m \sum_{j=1}^{S_2} \frac{\lambda_{mj} d_j}{L_{\psi(j)}} = \\
&= \sum_{m=1}^{S_1} \sum_{j=1}^{S_2} \frac{\varepsilon_m \lambda_{mj}}{L_{\psi(j)}} \left[\psi(j) \sum_{m=1}^{S_1} \beta_{jm} a_m - d_j \right] = I^*.
\end{aligned}$$

Виходячи зі співвідношень (2.88) та (2.89) слідує справедливність сформульованих згідно теореми 2.1 тверджень 2.2 та 2.3. Отже, теорема 2.1 доведена.

Таким чином, на основі теореми 2.1 та тверджень 2.2 та 2.3 доведено, що виграш гравців в ІК залежить не тільки від співвідношення їх ресурсів, які виділяються для організації КБн та КБз, а й від стратегій їх застосування. Отже, синтез оптимальної поведінки гравців в системі кіберзахист-кібератака гарантує кожному з них відповідно заданий програш та виграш у платі – рівні захищеності ОКІ від кібератак заданого класу.

2.9. Багатокритерійна диференціально-ігрова модель процесу кібернападу на державні інформаційні ресурси об'єкта критичної інфраструктури

Нехай динаміка ІК в СІБ ОКІ описується системою диференціальних рівнянь Колмогорова-Чепмена загального вигляду [102, 121, 122]:

$$\frac{dP_i(t)}{dt} = f_i(t, \lambda_i(t), \mu_i(t), P_1(t), P_2(t), \dots, P_{n-1}(t)), \quad i = \overline{0, n-1}, \quad (2.90)$$

де $P_i(t)$ – змінні стану процесу, котрий моделюється, $n-1$ -мірного фазового простору R_{n-1} , що характеризує процеси в області $P \in R_{n-1}$ з відповідним значенням імовірності перебування у даному стані;

$\lambda_i(t)$, $\mu_i(t)$ – інтенсивності потоків розподілу ресурсів гравців КБз та КБа, які відповідно належать $\Lambda \in E_\lambda$, $M \in E_\mu$ замкненим, обмеженим у евклідових просторах R_λ і R_μ множинам, що визначають можливі стратегії

гравців. Розподіл інтенсивностей потоків $\lambda_i(t)$ і $\mu_i(t)$ нестационарний, але обмежений за величинами:

$$\lambda_{i \min}(t) \leq \lambda_i(t) \leq \lambda_{i \max}(t), \quad (2.91)$$

$$\mu_{i \min}(t) \leq \mu_i(t) \leq \mu_{i \max}(t), \quad (2.92)$$

де $\lambda_{i \min}(t)$ і $\mu_{i \min}(t)$ – мінімальні, а $\lambda_{i \max}(t)$ і $\mu_{i \max}(t)$ – максимальні інтенсивності потоків КБз та КБа відповідно на заданому часовому інтервалі моделювання t , що обмежується тривалістю T , $t_0 = 0$;

$$\sum_{i=0}^{n-1} P_i(t) = 1 \text{ – умова нормування;}$$

$$P_0(t_0) = 1, P_1(t_0) = \dots = P_{n-1}(t_0) = 0 \text{ – початкові умови;}$$

$f_i = (f_0, f_1, \dots, f_{n-1})$ – дійсні функції, визначені на прямому добутку $P \times E_\lambda \times E_\mu$ вказаних множин.

Стратегії гравців $\lambda_i(t)$ і $\mu_i(t)$, визначені на P , приймають значення відповідно з E_λ і E_μ та вибираються з умови оптимізації деякого критерію, який в ігрових задачах називається платою. Наприклад, для першого гравця плата I_j в загальному вигляді може бути подана сукупністю частинних критеріїв, заданих функціоналами:

$$I_j = \Phi_j[\lambda_i(t), \mu_i(t), T, P_0(t)], \quad j = \overline{1, r}, \quad (2.93)$$

де Φ_j – функції, що мають неперервні частинні похідні за $\lambda_i(t)$ і $\mu_i(t)$;

$P_0(t)$ – багатокритерійна модель процесу КБн.

Частинні критерії (2.93) є компонентами r -мірного векторного критерію $I_0 = I_1, I_r$. Вектор частинних критеріїв обмежений допустимою областю $I_0 \in M$.

Розв'язання системи (2.90) при обраних стратегіях $\lambda_i(t)$ і $\mu_i(t)$ з початковими умовами $P_i(t_0) = P_i$, де t_0 – момент початку гри (початку КБа), що починається у точці P_i , називається траєкторією або партією і позначається як $P_i(t)$. Розвиток гри відбувається в області P , до якої належать ці траєкторії.

Гра закінчується, коли точка P_i досягне термінального багатовиду M .

Основна задача диференціальної гри, а відповідно, і моделювання процесу КБн за багатокритерійною моделлю (2.93) зводиться до визначення ціни гри I_0^{VR} – прогнозованого РЗ, котра є платою при виборі гравцями оптимальних стратегій $\lambda_i^{opt}(t)$ і $\mu_i^{opt}(t)$ і траєкторії $P_0^{opt}(t)$, що їм відповідає.

Визначимо частинні критерії, що входять до функціонала (2.93).

Перший частинний критерій I_1 є усередненою на інтервалі моделювання ймовірністю перебування СІБ ОКІ під впливом методів НСД.

Другий частинний критерій I_2 відповідає за витрати ресурсів, які виділено на захист ІР гравцеві захисту:

$$I_2 = \int_0^T \lambda_i^2(t) dt, \quad (2.94)$$

з обмеженням:

$$0 \leq I_2 \leq I_{2\max}, \text{ де } I_{2\max} = \lim_{t \rightarrow T} I_2. \quad (2.95)$$

Третій частинний критерій I_3 обрано, виходячи з умов антагонізму інтересів гравців визначається як:

$$I_3 = \int_0^T \mu_i^2(t) dt \quad (2.96)$$

з обмеженням:

$$0 \leq I_3 \leq I_{3\max}, \text{ де } I_{3\max} = \lim_{t \rightarrow T} I_3. \quad (2.97)$$

З позицій першого гравця його гарантований виграш досягається, коли частинні критерії I_1-I_3 розподіляються таким чином:

$$\left. \begin{array}{l} I_1 \rightarrow \min \\ I_2 \rightarrow \min \\ I_3 \rightarrow \max \end{array} \right\}. \quad (2.98)$$

Згідно нелінійної схеми компромісів плата гравця КБз I_0^{VR} передбачає скалярну згортку описаних вище частинних критеріїв. Плата I_0^{VR} відповідає векторній моделі оптимізації, яка позбавлена від недоліків попередньої моделі

та, на відміну від неї, дозволяє знайти оптимальний компроміс між критеріями, які входять до її складу, оскільки отримуване рішення належатиме області компромісів, тобто є оптимальним за Парето.

У такому випадку поставлена багатокритерійна задача зводиться до [121]:

$$I_0^{VR} = \arg \min_{I_0 \in M} \sum_{j=1}^r \frac{1}{1 - \frac{I_j}{I_{j\max}}} . \quad (2.99)$$

За необхідності введення пріоритету одних критеріїв над іншими та потребі мати різну чутливість до варіації параметрів задачі замість одиниці в чисельнику виразу (2.99) вводять вагові коефіцієнти α_j , на які накладають

$$\text{обмеження } \alpha_j > 0, \sum_{j=1}^r \alpha_j = 1.$$

Тоді модель (2.99) набуває вигляду:

$$I_0^{VR} = \arg \min_{I_0 \in M} \sum_{j=1}^r \frac{\alpha_j}{1 - \frac{I_j}{I_{j\max}}} . \quad (2.100)$$

Концепція коректного застосування нелінійної схеми компромісів вигляду (2.100), що є платою у даній диференціальній грі, передбачає нормалізацію частинних критеріїв та зведення їх до єдиного способу екстремізації, наприклад до мінімуму.

З метою збереження рівнозначності частинних критеріїв нормалізацію компонентів нормалізуючого вектора доцільно здійснити за супремумами відповідних критеріїв, що визначені на просторі рішень $I_0 \in M$:

$$I_{j\max} = \left\{ \sup_{I_0 \in M} I_j \right\}_{j=1}^r . \quad (2.101)$$

Усі інші відомі підходи описані в [62] позбавлені такої переваги.

З урахуванням умови нормалізації частинних критеріїв багатокритерійна модель векторної оптимізації за нелінійною схемою компромісів набуватиме вигляду:

$$I_0^{VR} = \arg \min_{I_0 \in M} \left[\alpha_1 \frac{1}{1 - \frac{I_1}{I_{1\max}}} + \alpha_2 \frac{1}{1 - \frac{I_2}{I_{2\max}}} + \alpha_3 \frac{I_{3\max}}{I_3} \right] = \quad (2.102)$$

$$= \arg \min_{I_0 \in M} \left[\alpha_1 \frac{I_{1\max}}{I_{1\max} - I_1} + \alpha_2 \frac{I_{2\max}}{I_{2\max} - I_2} + \alpha_3 \frac{I_{3\max}}{I_3} \right].$$

Виконання необхідних умов існування екстремумів скалярного критерію за кожною з стратегій гравців зводиться до системи кінцевих рівнянь:

$$\begin{cases} \frac{\partial I_0^{VR}}{\partial \lambda_i} = 0; \\ \frac{\partial I_0^{VR}}{\partial \mu_i} = 0, \end{cases} \quad (2.103)$$

де з урахуванням (4.66) вона набуватиме загального вигляду:

$$\begin{cases} \frac{\partial I_0^{VR}}{\partial \lambda_i} = \alpha_1 \frac{I_{1\max} \frac{\partial I_1}{\partial \lambda_i}}{(I_{1\max} - I_1)^2} + \alpha_2 \frac{I_{2\max} \frac{\partial I_2}{\partial \lambda_i}}{(I_{2\max} - I_2)^2} + \alpha_3 \frac{I_{3\max} \frac{\partial I_3}{\partial \lambda_i}}{I_3^2} = 0; \\ \frac{\partial I_0^{VR}}{\partial \mu_i} = \alpha_1 \frac{I_{1\max} \frac{\partial I_1}{\partial \mu_i}}{(I_{1\max} - I_1)^2} + \alpha_2 \frac{I_{2\max} \frac{\partial I_2}{\partial \mu_i}}{(I_{2\max} - I_2)^2} + \alpha_3 \frac{I_{3\max} \frac{\partial I_3}{\partial \mu_i}}{I_3^2} = 0, \end{cases} \quad (2.104)$$

або

$$\left\{ \begin{array}{l} \frac{\partial I_0^{VR}}{\partial \lambda_i} = \alpha_1 I_{1\max} (I_{2\max} - I_2)^2 I_3^2 \frac{\partial I_1}{\partial \lambda_i} + \alpha_2 I_{2\max} (I_{1\max} - I_1)^2 \times \\ \times I_3^2 \frac{\partial I_2}{\partial \lambda_i} + \alpha_3 I_{3\max} (I_{1\max} - I_1)^2 (I_{2\max} - I_2)^2 \frac{\partial I_3}{\partial \lambda_i} = 0; \\ \frac{\partial I_0^{VR}}{\partial \mu_i} = \alpha_1 I_{1\max} (I_{2\max} - I_2)^2 I_3^2 \frac{\partial I_1}{\partial \mu_i} + \alpha_2 I_{2\max} (I_{1\max} - I_1)^2 \times \\ \times I_3^2 \frac{\partial I_2}{\partial \mu_i} + \alpha_3 I_{3\max} (I_{1\max} - I_1)^2 (I_{2\max} - I_2)^2 \frac{\partial I_3}{\partial \mu_i} = 0. \end{array} \right. \quad (2.105)$$

Проведемо перетворення (2.105) й отримаємо:

$$\left\{ \begin{array}{l} \alpha_1 \frac{\partial I_1}{\partial \lambda_i} + \alpha_2 \frac{I_{2\max} (I_{1\max} - I_1)^2}{I_{1\max} (I_{2\max} - I_2)^2} \frac{\partial I_2}{\partial \lambda_i} + \\ + \alpha_3 \frac{I_{3\max} (I_{1\max} - I_1)^2}{I_{1\max} I_3^2} \frac{\partial I_3}{\partial \lambda_i} = 0; \\ \alpha_1 \frac{\partial I_1}{\partial \mu_i} + \alpha_2 \frac{I_{2\max} (I_{1\max} - I_1)^2}{I_{1\max} (I_{2\max} - I_2)^2} \frac{\partial I_2}{\partial \mu_i} + \\ + \alpha_3 \frac{I_{3\max} (I_{1\max} - I_1)^2}{I_{1\max} I_3^2} \frac{\partial I_3}{\partial \mu_i} = 0. \end{array} \right. \quad (2.106)$$

Введемо параметри регуляризації γ^{VR} та φ^{VR} для некоректної задачі векторної оптимізації та визначимо їх як:

$$\gamma^{VR} = \frac{I_{2\max} (I_{1\max} - I_1)^2}{I_{1\max} (I_{2\max} - I_2)^2}, \quad (2.107)$$

$$\varphi^{VR} = \frac{I_{3\max} (I_{1\max} - I_1)^2}{I_{1\max} I_3^2}. \quad (2.108)$$

Врахувавши введені параметри регуляризації γ^{VR} та φ^{VR} , модель (2.106) набуватиме вигляду:

$$\begin{cases} \alpha_1 \frac{\partial I_1}{\partial \lambda_i} + \alpha_2 \gamma^{VR} \frac{\partial I_2}{\partial \lambda_i} + \alpha_3 \varphi^{VR} \frac{\partial I_3}{\partial \lambda_i} = 0; \\ \alpha_1 \frac{\partial I_1}{\partial \mu_i} + \alpha_2 \gamma^{VR} \frac{\partial I_2}{\partial \mu_i} + \alpha_3 \varphi^{VR} \frac{\partial I_3}{\partial \mu_i} = 0. \end{cases} \quad (2.109)$$

Диференціювання системи (2.109) з використанням диференціальних перетворень вигляду зводить її до СЛАР. Для розв'язання такої системи відносно $\lambda_i^{opt}(t)$ і $\mu_i^{opt}(t)$ використовують відомі методи, наприклад, метод Ньютона. Далі згідно диференціально-ігрового методу знаходиться ціна гри – прогнозований I_0^{optVR*} та проточний I_0^{optVR} рівні захищеності, а також в області оригіналів відновлюється відповідна модель процесу КБн.

Твердження 2.1. Перевагами моделі (2.109) над відомими є її гнучка адаптація до різних ігрових ситуацій, що можуть виникати під час ІК.

Розглянувши такі ситуації подамо змістовний аналіз розробленої моделі та доведемо її переваги.

Доведення. Розглянемо типові ігрові ситуації. Численність ситуацій, що виникають в даній диференціальній грі, обумовлена законами розподілу ресурсів гравців.

Ситуація 1. Гравець, що захищається, намагається організувати захист інформації, у напруженій ситуації, що склалася.

У першій, напруженій ситуації, при потребі прийняття рішення гравцем КБз на захист, кожен з гравців проявляє власні жорсткі антагоністичні прагнення, обумовлені абсолютною протилежністю своїх цілей. Під напруженістю ситуації розуміють міру близькості відносних частинних критеріїв до свого граничного значення (до одиниці).

Наприклад, частинний критерій I_2 прирівнюємо до його мінімального значення $I_{2\min}$ ($I_2 = I_{2\min}$), інший I_3 – до максимального $I_{3\max}$ ($I_3 = I_{3\max}$). Дана ситуація відповідає випадку, коли гравці обирають стратегії $\lambda_{i\min}(t)$ і $\mu_{i\max}(t)$, відповідно. Тоді, як впливає з виразу (2.109), плата за критерієм I_3 різко зростає, що призводить на практиці до оптимізаційної задачі за Чебишевським принципом мінімаксу. У результаті з усіх частинних критеріїв

мінімізується лише найгірший частинний критерій I_3 , що дає найбільше значення $\frac{I_{3\max}}{I_3}$ в платі, тобто:

$$I_0^{VR} = \min_{I_2} \max_{I_3} I_3. \quad (2.110)$$

Ситуація 2. Гравці обирають стратегії, виходячи з принципу мінімізації витрат власних ресурсів.

Частинні критерії близькі до своїх мінімальних значень, тобто $I_1 \approx I_{1\min}$, $I_2 \approx I_{2\min}$ та $I_3 \approx I_{3\min}$. Даній ситуації відповідає економічна схема компромісів, що забезпечує для заданих умов сумарні втрати в платі за частинними критеріями. Тоді нелінійна схема компромісів (2.109) зводиться до моделі інтегральної оптимальності.

Ситуація 3 Гравцями обираються довільні стратегії.

До таких ситуацій належать всі інші випадки, які непередбачені у першій та другій ситуаціях. Тобто частинні критерії знаходяться в границях своїх обмежень. Застосування диференціально-ігрової моделі дає можливість їх вирівнювати за рахунок варіювання ваговими коефіцієнтами α_j особою, що приймає рішення.

У результаті багатокритерійна модель процесу нападу КБн, що є оптимальною траєкторією диференціальної гри $P_0^{optVR}(t)$, у кожній з розглянутих ситуацій знаходиться шляхом підстановки в аналітичний вираз для траєкторії $P_0^{VR}(t)$, отриманої диференціальними перетвореннями, відповідних значень оптимальних стратегій $\lambda_i^{opt}(t)$ і $\mu_i^{opt}(t)$.

Отже, твердження 3.1 доведено. Крім даної переваги розроблена модель забезпечує вирівнювання частинних критеріїв за рахунок варіювання ваговими коефіцієнтами α_j експертом з ІБ.

Таким чином, проведений аналіз розробленої моделі (2.109) показує можливість її адаптації до різних ігрових ситуацій, які виникають в АС та комп'ютерних мережах під час вирішення широкого спектру прикладних задач захисту інформації, що є її перевагою над відомими моделями.

2.10. Ієрархічна диференціально-ігрова модель для задач оцінювання ефективності систем інформаційної безпеки

Постановка задачі. Нехай множина станів в яких може перебувати СІБ ОКІ описується системою диференціальних рівнянь Колмогорова-Чепмена загального вигляду [104]:

$$\frac{dP_i(t)}{dt} = f_i(t, \lambda_i, \mu_i, \beta_i, \gamma_i, \varphi_i, \rho_i, P_0(t), P_1(t), \dots, P_7(t)), \quad i = \overline{0, 7}, \quad (2.111)$$

де $P_i(t)$ – змінні стану процесу, що моделюється, 7 – мірного фазового простору R_7 , що характеризує процеси в області $P \in R_7$ з відповідним значенням ймовірності перебування СІБ у даному стані;

$f_i = (f_0, f_1, \dots, f_7)$ – дійсні функції, визначені на прямому добутку $P \times E_\lambda \times E_\mu$ вказаних множин;

λ_i, μ_i – інтенсивності потоків розподілу інформаційних ресурсів гравця, що захищається та нападає, які відповідно належать $\Lambda \in E_\lambda, M \in E_\mu$ замкненим обмеженням у евклідових просторах R_λ і R_μ множинам, що визначають можливі стратегії гравців [101];

β_i – інтенсивність відмов СІБ;

γ_i – інтенсивність знаходження вразливостей у СІБ;

φ_i – інтенсивність усунення вразливостей;

ρ_i – інтенсивність створення нової інформації.

Система (2.111) справедлива за дотримання умов нормування:

$$\sum_{i=0}^7 P_i(t) = 1, \quad (2.112)$$

де $P_0(t_0) = \dots = P_6(t_0) = 0, P_7(t_0) = 1$ – початкові умови.

Розподіл інтенсивностей потоків λ_i і μ_i стаціонарний, але обмежений за величиною:

$$\lambda_{i \min} \leq \lambda_i \leq \lambda_{i \max} \quad (2.113)$$

та

$$\mu_{i \min} \leq \mu_i \leq \mu_{i \max}, \quad (2.114)$$

де $\lambda_{i\min}$ і $\mu_{i\min}$ – мінімальні, а $\lambda_{i\max}$ і $\mu_{i\max}$ – максимальні інтенсивності потоків КБз та КБн, відповідно ($\lambda_i = [0,1]$; $\mu_i = [0,1]$).

Такі ж обмеження накладаються й на інтенсивності β_i , γ_i , φ_i та ρ_i відповідно, тобто [62]:

$$\beta_{i\min} \leq \beta_i \leq \beta_{i\max}, \quad (2.115)$$

$$\gamma_{i\min} \leq \gamma_i \leq \gamma_{i\max}, \quad (2.116)$$

$$\varphi_{i\min} \leq \varphi_i \leq \varphi_{i\max}, \quad (2.117)$$

$$\rho_{i\min} \leq \rho_i \leq \rho_{i\max}. \quad (2.118)$$

Зауваження. Кількість рівнянь у системі (2.111) відповідає кількості станів, у яких може перебувати СІБ ОКІ під впливом відповідних інтенсивностей λ_i , μ_i , β_i , γ_i , φ_i та ρ_i .

Потрібно розробити ієрархічну диференціально-ігрову модель оцінювання ефективності СІБ та, спираючись на неї, оцінити кількісно та якісно оцінку ефективності даної альтернативи I_0^* .

Розв'язок. Для знаходження розв'язку поставленої задачі згідно з диференціально-ігровим методом оцінювання ефективності СІБ на першому кроці формалізуємо задачу оцінювання ефективності, як (2.111)–(2.118).

На другому кроці здійснимо вибір та обґрунтування частинних критеріїв ефективності СІБ. Виходячи з формалізації задачі (2.111)–(2.118) для оцінювання ефективності СІБ I_0^* оберемо наступні критерії.

Зауваження. Критерії оцінювання ефективності СІБ можуть бути задані як в аналітичній формі так і виражені кількісними показниками, що є перевагою розробленого методу.

Критерії першого рівня ієрархії: середня ймовірність перебування СІБ в захищеному стані під впливом МЗІ $P_7^{opt}(t)$ – критерій $I_1^{(1)}$ (задається аналітично);

середні витрати ресурсів захисту $I_2^{(1)}$ гравцем КБз (задається аналітично);

середні витрати ресурсів нападу $I_3^{(1)}$ гравцем КБн (задається аналітично);

середня інтенсивність відмов СІБ $I_{04}^{(1)}$ (задається кількісно);

середня інтенсивність знаходження вразливостей у СІБ $I_{05}^{(1)}$ (задається кількісно);

середня інтенсивність усунення вразливостей СІБ $I_{06}^{(1)}$ (задається кількісно);

середня інтенсивність створення нової інформації $I_{07}^{(1)}$ (задається кількісно).

Критерій другого рівня ієрархії:

заданий рівень захищеності ІР, що забезпечує досліджувана СЗІ $I_{01}^{(2)}$ (кількісно-якісна оцінка);

середні витрати ресурсів гравців $I_{02}^{(2)}$ (кількісно-якісна оцінка);

надійність функціонування СІБ $I_{03}^{(2)}$ (кількісно-якісна оцінка).

Критерій третього рівня ієрархії:

критерій ефективності СІБ (кількісно-якісна оцінка) $I_{01}^{(3)}$.

При формалізації відповідних частинних критеріїв нульовим індексом позначено ті критерії, які нормовані відносно своїх максимальних значень.

Обґрунтуємо обрані частинні критерії ефективності.

З позиції гравця, що захищається середня ймовірність перебування СІБ ОКІ в захищеному стані під впливом МЗІ $P_7^{opt}(t)$ на інтервалі $[t_0, T]$, де $t_0 = 0$ при вказаних обмеженнях, може бути подана аналітичною залежністю вигляду:

$$I_1^{(1)} = \frac{1}{T} \int_{t_0}^T P_7(t) dt. \quad (2.119)$$

Тобто перший частинний критерій ефективності $I_1^{(1)}$ обирається виходячи з потреби забезпечення заданого рівня захищеності ІР, що реалізує досліджувана СІБ. Якщо прийняти, що $I_{1\max}^{(1)} = 1$, то нормування критерію $I_1^{(1)}$ дозволяє подати його як $I_1^{(1)} = I_{01}^{(1)}$.

Другий частинний критерій $I_2^{(1)}$ обирається гравцем КБз для забезпечення заданого рівня захищеності та за обмежень може бути поданий аналітичною залежністю вигляду:

$$I_2^{(2)} = \frac{1}{T} \lambda_i^2 \int_{t_0}^T dt. \quad (2.120)$$

Гравець КБз також передбачає, що гравець КБн реалізуючі власні антагоністичні прагнення в середньому витратить ресурсів не менше:

$$I_3^{(1)} = \frac{1}{T} \mu_i^2 \int_{t_0}^T dt. \quad (2.121)$$

Також відомо, що досліджувана СІБ на добовому інтервалі ($T = 1$ доба) згідно обраних частинних критеріїв ефективності забезпечує такі кількісні показники:

середня інтенсивність відмов СІБ не більше $I_{04}^{(1)} = 0.0027$;

середня інтенсивність знаходження вразливостей у СІБ не менше $I_{05}^{(1)} = 0.0328$;

середня інтенсивність усунення вразливостей СІБ не гірше $I_{06}^{(1)} = 0.0328$;

середня інтенсивність створення нової інформації $I_{07}^{(1)} = 1$.

Фізичний зміст частинних критеріїв ефективності на кожному з рівнів ієрархії може бути поданий ієрархічною векторною моделлю вигляду [87]:

$$\left\{ \begin{array}{l} I_{01}^{(1)} \rightarrow \max; \\ I_{02}^{(1)} \rightarrow \min; \\ I_{03}^{(1)} \rightarrow \max; \\ I_{04}^{(1)} \rightarrow \min; \\ I_{05}^{(1)} \rightarrow \max; \\ I_{06}^{(1)} \rightarrow \max; \\ I_{07}^{(1)} \rightarrow \max; \end{array} \right. \rightarrow \left\{ \begin{array}{l} I_{01}^{(2)} \rightarrow \max; \\ I_{02}^{(2)} \rightarrow \min; \\ I_{03}^{(2)} \rightarrow \max; \end{array} \right. \rightarrow I_{01}^{(3)} \rightarrow \max. \quad (2.122)$$

Реалізація третього кроку методу передбачає побудову відповідної ієрархічної моделі частинних критеріїв [81, 82] у вигляді структурної схеми.

Виділивши на попередньому кроці відповідні рівні ієрархії частинних критеріїв, їх структурну схему можна подати у вигляді рис. 2.15 [102, 110, 111].

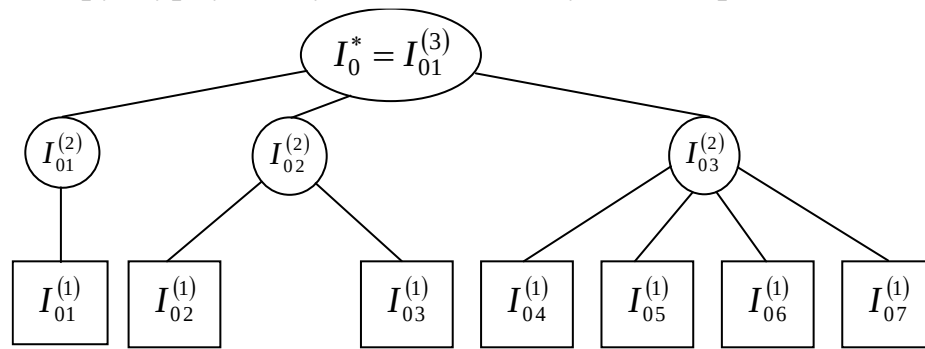


Рис. 2.10. Структурна схема ієрархії критеріїв для оцінювання ефективності системи інформаційної безпеки

На рис. 2.10 усі частинні критерії $I_{01}^{(1)}, \dots, I_{07}^{(1)}$, $I_{01}^{(2)}, \dots, I_{03}^{(2)}$ та $I_{01}^{(3)}$ є нормованими відносно своїх максимальних значень.

При оцінюванні ефективності СІБ, що досліджується приймається допущення про рівнозначність усіх частинних критеріїв, тобто $\alpha_{s\theta}^{(j-1)} = 1$. Тоді вираз набуває вигляду:

$$I_{0\theta}^{(j)} = 1 - L_{\theta}^{(j-1)} \left\{ \sum_{s=1}^{L_{\theta}^{(j-1)}} [1 - I_{0s\theta}^{(j-1)}]^{-1} \right\}^{-1}, \quad \theta \in [1, L^{(j)}], \quad j \in [2, m]. \quad (2.123)$$

На четвертому, заключному кроці, застосуємо метод вкладених скалярних згорток та метод диференціально-ігрового моделювання.

Перший етап композиції частинних критеріїв другого рівня полягає у такому. По-перше визначимо прогнозований РЗ ІР $I_1^{(2)}$ на основі методу диференціально-ігрового моделювання. Так, плата гравця КБз за забезпечення заданого РЗ $I_{01}^{(2)}$ – критерій другого рівня ієрархії виходячи з рекурентного виразу (2.123) в зальному вигляді визначається як:

$$I_{01}^{(2)} = 1 - L_1^{(1)} \left\{ \sum_{s=1}^{L_1^{(1)}} [1 - I_{0s1}^{(1)}]^{-1} \right\}^{-1}, \quad (2.124)$$

де $L_1^{(1)} = 1$, $I_{011}^{(1)} = I_{01}^1$.

Застосувавши метод диференціально-ігрового Р-моделювання визначимо оптимальні стратегії гравців $\lambda_{\min}^{opt}$ та $\mu_{\max}^{opt}$ в ІК при реалізації процесу кібернападу. Врахувавши (2.123) маємо:

$$\left\{ \begin{array}{l} \frac{\partial I_{01}^{(2)}}{\partial \lambda} = 0; \\ \frac{\partial I_{01}^{(2)}}{\partial \mu} = 0; \end{array} \right\} \rightarrow \left\{ \begin{array}{l} \frac{\partial (1 - I_{01}^1)}{\partial \lambda} = 0; \\ \frac{\partial (1 - I_{01}^1)}{\partial \mu} = 0; \end{array} \right\} \rightarrow \left\{ \begin{array}{l} \lambda^{opt}; \\ \mu^{opt}; \end{array} \right\} \rightarrow \left\{ \begin{array}{l} \frac{\partial^2 (1 - I_{01}^1)}{\partial \lambda^2} > 0; \\ \frac{\partial^2 (1 - I_{01}^1)}{\partial \mu^2} < 0; \end{array} \right\} \rightarrow \left\{ \begin{array}{l} \lambda_{\min}^{opt}; \\ \mu_{\max}^{opt}. \end{array} \right. \quad (2.125)$$

Якщо надати обраним частинним критеріям відповідні показники $\beta_i = 0.0027$, $\gamma_i = 0.0328$, $\varphi_i = 0.0328$ та $\rho_i = 1$ за добу ($T = 1$), то скориставшись згідно з виразу (4.101) матимемо:

$$\left\{ \begin{array}{l} \lambda_{\min}^{opt} = 0.5014; \\ \mu_{\max}^{opt} = 0.9645. \end{array} \right. \quad (2.126)$$

Для отримання кількісної оцінки ефективності СІБ за критерієм забезпечення заданого РЗ з урахуванням (2.124) згідно (2.122) маємо:

$$I_{01}^{(2)} = 1 - 0.66 = 0.34. \quad (2.127)$$

Співставлення з відомою інтервальною нормованою оберненою шкалою дозволяє стверджувати, що СІБ за даним критерієм є *достатньо ефективною*.

Оцінимо ефективність СІБ за витратами ресурсів гравців. Оцінка витрат ресурсів гравців в аналітичному вигляді має наступний вигляд (другий рівень ієрархії (див. рис. 2.10)):

$$I_{02}^{(2)} = 1 - L_2^{(1)} \left\{ \sum_{i=1}^{L_2^{(1)}} [1 - I_{0i2}^{(1)}]^{-1} \right\}^{-1}, \quad (2.128)$$

де $L_2^{(1)} = 2$; $I_{012}^{(1)} = I_{02}^{(1)}$; $I_{022}^{(1)} = I_{03}^{(1)}$.

Звівши до єдиного способу екстремізації (мінімізації) частинні критерії, отримаємо кількісну оцінку ефективності СІБ за витратами ресурсів захисту:

$$I_{02}^{(2)} = 1 - \frac{2}{\frac{1}{1-0.5014} + \frac{1}{0.9645}} = 0.34, \quad (2.129)$$

де прийнято $I_{2\max}^{(2)} = \lim_{\substack{\lambda_i \rightarrow \lambda_{i\max} \\ t \rightarrow T}} I_2^{(2)} = 1$ при $\lambda_{i\max} = 1$ та $I_{3\max}^{(1)} = \lim_{\substack{\mu_i \rightarrow \mu_{i\max} \\ t \rightarrow T}} I_3^{(1)} = 1$ при

$$\mu_{i\max} = 1.$$

У відповідності відомої шкали ефективність СІБ за витратою ресурсів гравців є *достатньо ефективною*.

Для визначення частинного критерію $I_{03}^{(2)}$ від рекурентного виразу, з урахуванням частинних критеріїв $I_{04}^{(1)}, \dots, I_{07}^{(1)}$, перейдемо до виразу вигляду:

$$I_{03}^{(2)} = 1 - L_3^{(1)} \left\{ \sum_{i=1}^{L_3^{(1)}} [1 - I_{0i3}^{(1)}]^{-1} \right\}^{-1}, \quad (2.130)$$

де $L_3^{(1)} = 4$; $I_{013}^{(1)} = I_{04}^{(1)}$; $I_{023}^{(1)} = I_{05}^{(1)}$; $I_{033}^{(1)} = I_{06}^{(1)}$; $I_{043}^{(1)} = I_{07}^{(1)}$.

Підставивши чисельні значення отримуємо:

$$I_{03}^{(2)} = 1 - \frac{4}{\frac{1}{1-0.0027} + \frac{1}{0.0328} + \frac{1}{0.0328} + 1} \approx 0.94. \quad (2.231)$$

Так відповідно до таблиці ефективності СІБ за даною групою критеріїв є *абсолютно неефективною*.

Заключний (другий) етап композиції критеріїв згідно рекурентного виразу набуває вигляду:

$$I_0^* = I_{01}^{(3)} = 1 - L_1^{(2)} \left\{ \sum_{i=1}^{L_1^{(2)}} [1 - I_{0i3}^{(1)}]^{-1} \right\}^{-1}, \quad (2.132)$$

де $L_1^{(2)} = 3$, $I_{013}^{(2)} = I_{01}^{(2)}$, $I_{023}^{(2)} = I_{02}^{(2)}$, $I_{033}^{(2)} = I_{03}^{(2)}$.

Таким чином, з урахуванням розрахованих критеріїв, маємо:

$$I_0^* = 1 - \frac{3}{\frac{1}{0.34} + \frac{1}{1-0.34} + \frac{1}{0.94}} = 0.46.$$

Отже, одержавши узагальнену оцінку ефективності СІБ за сукупністю частинних критеріїв, виходячи з інтервальної оберненої нормованої фундаментальної шкали оцінок ефективності СІБ, можна зробити висновок [103], що досліджувана СІБ *є ефективною*. Для підвищення ефективності СІБ при її переході до вищої якості, доцільно забезпечити значення показників за висунутими критеріями відмінні від відомих, але такими, що знаходяться в границях визначених обмежень.

Висновки за главою 2

Розроблена модель онтології поведінки агентів в умовах конфлікту, яка містить базові поняття процесів взаємодії агентів систем безпеки, та на відміну від існуючих містить поняття та відносини, що відображають процеси взаємодії агентів протистояння, а не технічні сторони кіберконфлікту, що дозволяє обґрунтувати вибір моделі поведінки антагоністичних агентів в умовах гібридних загроз.

Вдосконалено класифікатор загроз безпеці інформаційних ресурсів, який на відміну від існуючих, містить показники вартості здійснення загрози та протидії їй, а також оцінки збитків від порушення безпеки інформаційного ресурсу та потенційної корисності використання його зловмисником. Удосконалений класифікатор дозволяє оцінити ймовірність реалізації тієї чи іншої загрози та розробити ефективну оборонну стратегію.

Розроблений метод оцінки рівня захищеності інформаційних ресурсів, який на відміну від існуючих базується на сумісному розгляді вартісних показників ресурсів, що підлягають захисту, та вартості здійснення атаки. Метод дозволяє виявити той діапазон ресурсів, який є найбільш ймовірним вірогідним для здійснення кібератак.

Розроблена рекурсивна модель рефлексивного агента, яка на відміну від існуючих містить моделі поведінки сторони нападу та дозволяє моделювати

ймовірні дії протилежної сторони конфлікту, і тим самим передбачати наслідки від прийнятих рішень сторони захисту.

Розроблена модель взаємодії агентів, яка дозволить проводити імітаційне моделювання взаємодії агентів системи безпеки під час здійснення кіберконфлікту, яка на відміну від існуючих описує поведінку усіх сторін конфлікту та їх взаємодію під час конфлікту, що дозволяє створити ефективну стратегію мережевого захисту.

Вдосконалені методи координації у групах агентів безпеки на відміну від існуючих методів для ієрархічних систем, враховують мережеву структуру взаємодії агентів, що дозволяє організувати співробітництво між агентами системи безпеки для виконання задач кіберзахисту.

Вдосконалена модель самоорганізації системи безпеки, що базується на запропонованих в роботі моделях, які описують окремі сторони моделювання тих чи інших процесів та складових системи безпеки, яка відрізняється від існуючих поєднанням в єдиній моделі складових прийняття рішень, рефлексивності, адаптації та навчання, а її реалізація призводить до появи синергетичного ефекту захисту контуру бізнес-процесів.

Запропоновано метод опису сценаріїв поведінки агентів, який базується на використанні контекстно-вільної граматики, який на відміну від існуючих методів описує поведінку агентів, а не проведення конкретної атаки, що дозволяє автоматизувати аналіз формального опису сценаріїв та використовувати отримані результати аналізу для подальшої генерації сценаріїв поведінки антагоністичних агентів.

Розроблено методологію моделювання поведінки взаємодіючих агентів, базис якої становить трирівнева структура моделювання суб'єктів та бізнес-процесів контурів системи безпеки та функціонування організацій, яка орієнтована на моделювання відрізняється від існуючих моделюванням поведінки антагоністичних агентів для оцінки та підвищення поточного рівня безпеки. Методологія дозволяє прогнозувати можливу поведінку нападаючої сторони, обґрунтувати вибір засобів протидії на системному рівні кіберзагрозам та розрахувати необхідні суми інвестицій у кібербезпеку з відповідним розподілом за складовими безпеки та часу інвестування.

Розроблено моделі безпеки кіберфізичних систем з урахуванням обчислювальних можливостей та спрямованості цільових кібератак, можливої конкуренції зловмисників стосовно “жертви”. Моделі відображають можливості групування з метою досягнення цілей кібератаки, взаємозв'язків між “видами жертв” та “видами хижаків”. Отримано коефіцієнти моделі

Лотки-Вольтери, які враховують синергізм та гібридність сучасних загроз, фінансування на формування та вдосконалення системи захисту, а також дозволяє визначити фінансові та обчислювальні можливості зловмисника щодо виявлених загроз. Проведено дослідження практичної реалізації запропонованого підходу, отримано оцінки рівня безпеки кіберфізичної системи, виконано імітаційне моделювання динаміки розвитку системи “хижак-жертва” для кіберфізичної системи та її системи безпеки.

Розроблена диференціально-ігрова нетейлорівська модель прогнозування розвитку динаміки процесів кібернападу, яка належить до класу точних, в рамках нетейлорівської теорії, диференціально-ігрових нетейлорівських моделей. При цьому відновлення оригіналу, а відповідно і подання моделі процесів кібернападу на інформаційні ресурси об’єктів критичної інфраструктури у часовій області здійснено із застосуванням диференціально-експоненціальних перетворень, апроксимуюча функція в яких є рядом Діріхле.

Розвинуто ігровий підхід до організації захисту інформаційних ресурсів в прогресивних систем інформаційної безпеки, які функціонують за схемою кіберзахист-кібератака. Такий підхід до організації систем безпеки об’єктів критичної інфраструктури дозволяє з гарантованою якістю керувати рівнем захищеності їх інформаційних ресурсів.

Розроблено багатокритерійну диференціально-ігрову модель процесу кібернападу на інформаційні ресурси об’єктів критичної інфраструктури на основі нелінійної схеми компромісів та диференціальних перетворень, що дозволяє регуляризувати вихідну некоректну задачу моделювання з конфліктуючими частинними критеріями та зводити проблему динамічної векторної оптимізації до рішення системи лінійних алгебричних рівнянь відносно вхідних параметрів розроблюваної моделі. На основі розробленого диференціально-ігрового методу оцінювання ефективності системи інформаційної безпеки об’єкта критичної інфраструктури розроблено відповідну ієрархічну диференціально-ігрову модель. Її застосування в задачах захисту інформації дозволяє отримувати кількісні та якісні оцінки ефективності системи інформаційної безпеки. Крім того, застосування моделі відкриває шлях до подальшого розвитку науково обґрунтованого підходу щодо вибору показників ефективності за обраними частинним критеріями, а також дозволяє встановлювати емерджентні властивості комплексних систем захисту інформації об’єктів критичної інфраструктури.

ГЛАВА 3.

МЕХАНІЗМИ ТА МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ПОСЛУГ БЕЗПЕКИ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ.

3.1. Властивості постквантових алгоритмів забезпечення послуг безпеки об'єктів критичної інфраструктури

Для забезпечення безпеки інформаційних ресурсів об'єктів критичної інфраструктури перспективним напрямком є використання несиметричних криптосистем на основі крипто-кодових конструкцій (ССС) Мак-Еліса і Нідеррайтера [8, 15, 16], що інтегровано (одним механізмом) забезпечують показники достовірності на рівні $2^9 - 2^{12}$ і криптостійкості – $2^{30} - 2^{35}$ групових операцій при її побудові над полем $GF(2^{10})$. На рис. 3.1 наведені результати досліджень швидкодії криптоперетворень сучасними симетричними і несиметричними криптосистемами [11].

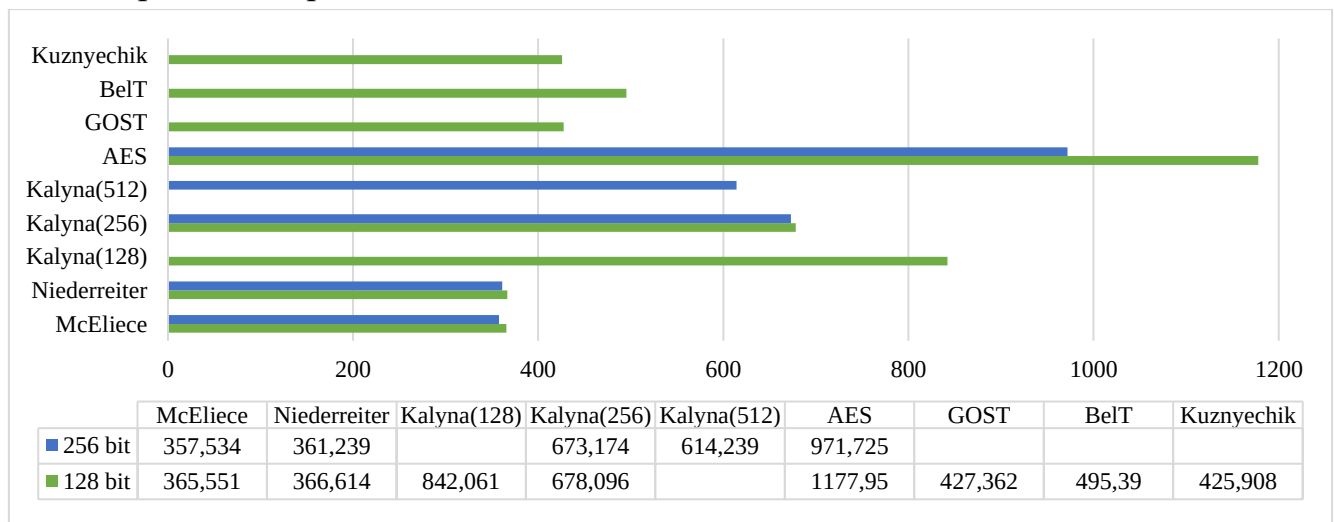


Рисунок 3.1 – Результати аналізу швидкодії перетворення інформації

У табл. 3.1 наведені результати порівняльних досліджень ефективності криптографічних методів захисту інформації при фіксованому рівні стійкості [13]:

- середньому (складність криптоаналізу найкращим відомим алгоритмом не менше 2^{128} операцій);
- високому (складність криптоаналізу найкращим відомим алгоритмом не менше 2^{256} операцій);
- надвисокому (складність криптоаналізу найкращим відомим алгоритмом не менше 2^{512} операцій).

Таким чином, як впливає з наведених результатів порівняльного аналізу (рис. 3.1 та табл. 3.1) несиметричні криптоалгоритми з використанням ССС дозволяють реалізувати криптографічний захист інформації за технологією відкритих ключів і забезпечити при цьому швидкість крипто-кодового перетворення інформації зі швидкістю шифрування БСШ [44, 48].

Таблиця 3.1

Результати порівняльних досліджень ефективності криптографічних методів захисту інформації при фіксованому рівні стійкості

Методи криптографічного перетворення	Модель безпеки	Довжина ключових даних, біт	Швидкість криптоперетворень, біт / с	Додаткові функції
Блокові симетричні шифри	Практична безпека	128, 256, 512	$10^6 - 10^9$	Немає
Потокові симетричні шифри	Практична безпека	128, 256, 512	$10^7 - 10^{10}$	Немає
Несиметричні RSA-подібні криптоалгоритми	Доказова безпека	3248 (128), 15424 (256)	$10^2 - 10^3$	Немає
Несиметричні СССз використанням кодових конструкцій	Доказова безпека	$0,5 \cdot 10^6$ (128), $2 \cdot 10^6$ (256)	$10^6 - 10^8$	Контроль помилок, підвищення достовірності

Загальна класифікація крипто-кодових систем і послуг безпеки, які забезпечують їх використання наведені на рис. 3.2 [29].

Для ССС Мак-Еліса забезпечують швидкість криптоперетворень на рівні швидкості криптоперетворень у БСШ, криптостійкість за рахунок NP -задачі – декодування випадкового коду, достовірність за рахунок використання завадостійких алгебраїчних кодів [9, 54].

Для модифікації еліптичного коду, що не зменшує мінімальну кодову відстань, запропоновано скоротити кількість інформаційних символів. $I = (I_1, I_2, \dots, I_k)$ – інформаційний вектор (n, k, d) блокового коду, підмножина h інформаційних символів, $h = x$, $x \leq 1/2 k$ визначає нульові символи. При кодуванні інформаційного вектора символи множини h не застосовуються (вони нульові) і їх можна відкинути, а отримане кодове слово буде коротше на x кодових символів [7]. Другий спосіб модифікації використовує збільшення довжини шляхом формування вектора ініціалізації (визначення символів скорочення) і заміни нульових символів символами інформаційного вектора. Вектор ініціалізації (IV) є додатковим секретним параметром системи.

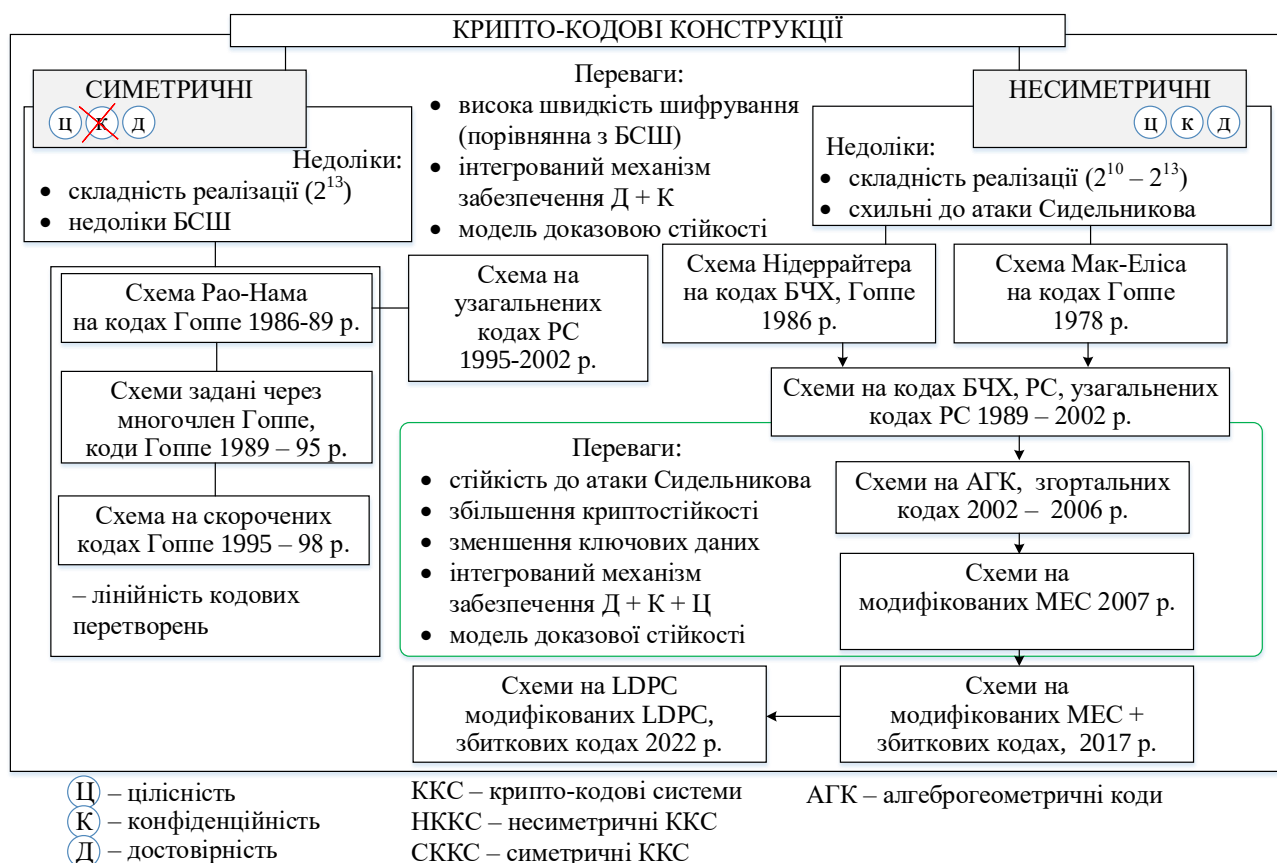


Рис. 3.2. Класифікація криптосистем на основі ССС

Основні властивості *МЕС* наведені у табл. 3.1, основні параметри ССС Мак-Еліса на МЕС в табл. 3.2 .

Таблиця 3.1

Основні (n, k, d) властивості *МЕС*

Властивість	Укорочені <i>МЕС</i>	Подовжені <i>МЕС</i>
(n, k, d) параметри коду, який побудований через відображення виду $\varphi: X \rightarrow P^{k-1}_1$	$n = 2\sqrt{q} + q + 1 - x,$ $k \geq \alpha - x, d \geq n - \alpha,$ $\alpha = 3 \times \deg F,$ $k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1,$ $k \geq \alpha - x + x_1, d \geq n - \alpha,$ $\alpha = 3 \times \deg F$
$n, k, d)$ параметри коду, який побудований через відображення виду $\varphi: X \rightarrow P^{r-1}_1$	$n = 2\sqrt{q} + q + 1 - x,$ $k \geq n - \alpha, d \geq \alpha,$ $\alpha = 3 \times \deg F, k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1,$ $k \geq n - \alpha, d \geq \alpha,$ $\alpha = 3 \times \deg F$

Таблиця 3.2

Основні параметри ССС Мак-Еліса на *MEC*

Властивість	Укорочені <i>MEC</i>	Подовжені <i>MEC</i>
розмірність секретного ключа	$l_{K+} = x \times \lceil \log_2(2\sqrt{q} + q + 1) \rceil$	$l_{K+} = (x - x_1) \times \log_2(2\sqrt{q} + q + 1)$
розмірність інформаційного вектора	$l_I = (\alpha - x) \times m$	$l_I = (\alpha - x + x_1) \times m$
розмірність криптограми	$l_S = (2\sqrt{q} + q + 1 - x) \times m$	$l_S = (2\sqrt{q} + q + 1 - x + x_1) \times m$
відносна швидкість передачі	$R = (\alpha - x) / (2\sqrt{q} + q + 1 - x)$	$R = (\alpha - x + x_1) / (2\sqrt{q} + q + 1 - x + x_1)$

Для нанесення збитку використовується універсальний механізм C_m за алгоритмом *MV2*(збиткові коди, *DC*):

$$\begin{aligned}
 CFT / CH_{FT} &= E_1(M, KU^{EC}), \quad CHD / CH_D = E_2(M, KU^{EC}), \\
 M &= E_{1,2}^{-1}(CFT / CH_{FT}, CHD / CH_D, KU^{EC}),
 \end{aligned} \tag{3.1}$$

$$\begin{aligned}
 \text{де } CFT / CH_{FT} &= CFT / CH_{FT}^i, \dots, CFT / CH_{FT}^m, \quad KU^{EC} = \varphi(K_D^i, \dots, K_D^m, KU_1^{EC}, \dots, KU_m^{EC}, \\
 CHD / CH_D &= CHD / CH_D^i, \dots, CHD / CH_D^m.
 \end{aligned}$$

Таким чином, шифртекст вихідного повідомлення (M) в результаті має два шифртексти (збиток (CHD) і збитковий текст (FTC)), кожен з яких окремо не може відновити вихідний текст.

Результати порівняльних досліджень ССС Мак-Еліса, на *EC*, *MEC*, збиткових кодах наведені в табл. 3.3, 3.4, де умовні скорочення (префікси): *ukh* / *udh* – гібридні ССС (НССС) з укороченими *MEC* / гібридні ССС з подовженими *MEC*; *uk* – ССС з укороченими *MEC*; *ud* – ССС з подовженими *MEC*.

При розрахунках параметрів криптосистем були використані поля Галуа: для ССС Мак-Еліса – $GF(2^{10})$; для ССС з укороченими/подовженими *MEC* – $GF(2^6)$; для гібридних НССС – $GF(2^4)$.

Складність процесу декодування для ССС на ЕС задається виразами:

– для ССС на ЕС: $O_{K+} = N_{\text{покр}} \times n \times r$,

$$\text{де } N_{\text{покр}} \geq \frac{C_n^{\rho \cdot t}}{C_{n-k}^{\rho \cdot t}} = \frac{n(n-1) \dots (n - \rho \cdot t - 1)}{(n-k)(n-k-1) \dots (n-k - \rho \cdot t - 1)}, \quad t = \lfloor (d-1)/2 \rfloor,$$

– для ССС на укорочених кодах: $O_{K+} = N_{\text{покр}} \times (2\sqrt{q} + q + 1 - 1/2k) \times r$;

– для ССС на подовжених кодах: $O_{K+} = N_{\text{покр}} \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times r$.

Складність процесу декодування для НССС на укорочених МЕС має вигляд:

– для НССС на укорочених МЕС:

$$O_{K+} = N_{\text{покр}} \times (2\sqrt{q} + q + 1 - 1/2k) \times r + N_F \text{ або } (N_K),$$

де $N_F \approx \frac{K_C^z}{2^{1-K_C^{z+1}}} \times |F|$; $K_C=97/128$; $|F|$ – сумарна довжина вихідних прапорів

(збитків) (бітів) – при відомому зловмисникові залишку (збитковому тексті) і заданих прапорах (збитках), при невідомому ключі: $N_K \approx 2^{1190 \times z}$; $z = 16$;

– для НССС на подовжених МЕС:

$$O_{K+} = N_{\text{покр}} \times (2\sqrt{q} + q + 1 - 1/2k + 1/2k) \times r + N_F \text{ або } (N_K).$$

Таблиця 3.3

Результати аналізу складності злому і складності кодування для різних швидкостей ЕС (МЕС)

$lg(l_s)$	Відносна швидкість кодування, R					
	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
1	4.75	12.1	15.6	18.23	19.12	19.82
2	10.52	21.76	32.47	35.67	38.63	39.18
3	18.22	33.17	43.75	51.61	56.88	58.03
4	21.42	51.75	59.43	72.81	78.92	80.52
5	38.77	61.09	68.26	87.32	94.91	104.56
6	54.13	78.37	101.72	112.46	120.83	128.79
7	82.14	83.72	156.75	164.72	182.39	189.74
8	165.84	179.13	223.64	231.57	276.27	287.33
9	358.33	371.09	421.97	428.63	459.81	476.52
10	672.37	684.94	716.41	722.26	783.46	794.28

Таблиця 3.4

Результати аналізу складності злому і складності кодування для різних швидкостей $MEC(MEC+DC)$

$lg(l_s)$	Відносна швидкість кодування, R							
	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
1	15.6	18.23	19.12	19.82	7.21	9.17	12.54	14.56
2	32.47	35.67	38.63	39.18	21.46	23.72	27.48	29.82
3	43.75	51.61	56.88	58.03	31.68	33.83	37.38	38.43
4	59.43	72.81	78.92	80.52	41.72	42.27	47.48	58.23
5	68.26	87.32	94.91	104.56	56.63	58.91	62.86	66.53
6	101.72	112.46	120.83	128.79	72.32	74.79	89.5	97.71

Аналіз табл. 3.3, 3.4 підтверджує, що використання збиткових кодів і подальше зменшення потужності поля Галуа призводить до значного зменшення складності формування ($\approx$ в 12 разів) і декодування криптограми ($\approx$ в 20 разів).

У табл. 3.5, 3.6 наведені результати досліджень залежності ємнісної характеристики від потужності поля Галуа для програмної реалізації.

Таблиця 3.5

Залежність швидкості програмної реалізації від потужності поля (кількість групових операцій)

Криптосистеми	$GF(q^m)$					
	2^5	2^6	2^7	2^8	2^9	2^{10}
ССС Мак-Еліса на еліптичних кодах	10018042	18048068	32847145	47489784	63215578	82467897
ССС Мак-Еліса на укорочених модифікованих еліптичних кодах	10007947	17787431	28595014	44079433	61974253	79554764
ССС Мак-Еліса на подовжених модифікованих еліптичних кодах	11156138	18561228	33210708	48297112	65171690	84051337

Таблиця 3.6

Залежність швидкості програмної реалізації від потужності поля
(кількість групових операцій)

Криптосистеми	$GF(q^m)$						
	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
ССС Мак-Еліса на на укорочених <i>MEC</i>	8293075	10007947	17787431	28595014	44079433	61974253	79554764
ССС Мак-Еліса наа подовжених <i>MEC</i>	8506422	11156138	18561228	33210708	48297112	65171690	84051337
НССС подовжених <i>MEC</i>	5612316	7900315	14892945	25565274	42279183	58963778	76564173
НССС укорочених <i>MEC</i>	5942627	7905257	14682411	25595014	42116327	58468143	75474764

У табл. 3.7 наведені результати досліджень статистичних властивостей запропонованих методів на основі пакета *NIST STS 822*.

Таблиця 3.7

Результати дослідження статистичної безпеки

Криптосистеми	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей	Кількість тестів, в яких тестування пройшли менше 96% послідовностей
ССС Мак-Еліса	149 (78,83 %)	189 (100 %)	0 (0 %)
ССС Мак-Еліса на укорочених <i>MEC</i>	151 (79,89 %)	189 (100 %)	0 (0 %)
ССС Мак-Еліса на подовжених <i>MEC</i>	152 (80,42 %)	189 (100 %)	0 (0 %)
НССС Мак-Еліса на подовжених <i>MEC</i>	153 (80,95 %)	189 (100 %)	0 (0 %)
НССС Мак-Еліса на укорочених <i>MEC</i>	155 (82 %)	189 (100 %)	0 (0 %)

Табл. 3.7 продемонструвала, що не зважаючи на зменшення потужності поля Галуа до $GF(2^6)$ для ССС і $GF(2^4)$ для НССС, статистичні характеристики таких крипто-кодових конструкцій виявилися, як мінімум, не гірше традиційних ССС Мак-Еліса на $GF(2^{10})$. Всі криптосистеми пройшли 100 % тестів, причому найкращий результат показала НССС на укорочених *MEC*: 155 з 189 тестів пройдено на рівні 0,99, що становить 82 % від усієї кількості тестів.

При цьому традиційна ССС Мак-Еліса на $GF(2^{10})$ показала 149 тестів на рівні 0,99.

Таким, чином запропоновані методи забезпечують основні послуги безпеки, необхідний рівень стійкості та достовірності інформаційних ресурсів об'єктів критичної інфраструктури.

3.2. Забезпечення послуг безпеки об'єктів критичної інфраструктури на основі крипто-кодових конструкцій на *ЕС (МЕС)*

Для формування математичної моделі методу забезпечення конфіденційності та автентичності у бездротових каналах об'єктів критичної інфраструктури запропонована наступна математична модель [25].

Вихідними даними для математичних моделей ССС Мак-Еліса на завадостійких (алгеброгеометричних), LDPC-кодах є:

- множина відкритих текстів для ССС Мак-Еліса $M = \{M_1, M_2, \dots, M_{q^k}\}$, де $M_i = \{I_0, I_{h_1}, \dots, I_{h_j}, I_{k-1}\}, \forall I_j \in GF(q), h_j$ – інформаційні символи рівні нулю, $h \neq \frac{1}{2}k$, Тобто $I_i=0, \forall I_i \in h$. На основі алгоритму рівноважного кодування відкритий текст перетворюється на вектор помилки;

- множина закритих текстів (кодограм) для ССС Мак-Еліса $C = \{C_1, C_2, \dots, C_{q^k}\}$, де $C_i = (c_{x_0}^*, c_{h_1}^*, \dots, c_{h_j}^*, c_{x_{n-1}}^*), \forall c_{x_j}^* \in GF(q)$;

- множина прямих відображень (на основі використання відкритого ключа – породжувальної/перевірочної матриці

$$\left(\begin{array}{l} G_j^{U_j}, \forall j \in \{U_j\}, U_1 - EC, U_2 - MEC, U_3 - FC, U_1 - LDPC, \\ H_j^{U_j}, \forall j \in \{U_j\}, U_1 - EC, U_2 - MEC, U_3 - FC, U_1 - LDPC, \end{array} \right) \quad \text{завадових кодів}$$

(алгеброгеометричних кодів: *ЕС, МЕС; LDPC*; збиткових кодів):

для ССС Мак-Еліса – $\phi = (\phi_1, \phi_2, \dots, \phi_s)$, де $\phi_i : M \rightarrow C_{k-h_j}, i=1, 2, \dots, s$;

- множина зворотних відображень (на основі використання закритого (особистого) ключа – матриць маскування):

для ССС Мак-Еліса – $\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, \dots, \phi_s^{-1}\}$, де $\phi_i^{-1} : C_{k-h_j} \rightarrow M, i=1, 2, \dots, s$;

- множина ключів, що параметризують прямі відображення (відкритий ключ уповноваженого користувача):

для CCC Мак-Еліса $KU_i = \{KU_1, KU_2, \dots, KU_s\} = \{G_1^{U_1}, G_2^{U_2}, \dots, G_s^{U_s}\}$, – де $G_{x_{a_i}}^{U_i}$ – матриця $n \times k$, що породжує замаскований під випадковий код. Матриця визначається з ортогональності матриць породжувальної та перевіркою;
 - множина особистих (закритих) ключів користувачів:

$$KR = \{KR_1, KR_2, \dots, KR_r\} = \left\{ \begin{matrix} \{X, P, D\}_1, \\ \{X, P, D\}_2, \dots, \{X, P, D\}_r \end{matrix} \right\}, \quad (3.1)$$

$$\{X, P, D\}_i = \{X^i, P^i, D^i\},$$

де X^i – невироджена, що маскує, випадково рівномірно сформована джерелом ключів $k \times k$ матриця з елементами $GF(q)$;

P^i – переставна випадково рівномірно сформована джерелом ключів $n \times n$ матриця з елементами $GF(q)$;

D^i – діагональна сформована джерелом ключів $n \times n$ матриця з елементами $GF(q)$. За рахунок того, що діагональна матриця дорівнює одиничній матриці, значення можна знехтувати, що дає зменшення ємності та складності обчислення.

Відкритий ключ формується шляхом перемноження матриць маскування на матриці, що породжує/перевірочну:

$$\text{для CCC Мак-Еліса} - G_{x_{a_i}}^{U_i} = X^u \times G^{U_i} \times P^u, u \in \{1, 2, \dots, s\};$$

У канал зв'язку надходить:

для CCC Мак-Еліса – кодове слово: $C_j = M_i \times G_{x_{a_i}}^{U_i} + e$, де e – додатковий сеансовий ключ кожної інформаційної посилки.

На приймальній стороні уповноважений користувач, який знає матриці маскування, використовує швидкий алгоритм декодування:

- для CCC Мак-Еліса:

$$M_i = f_u^{-1}(C_j^*, \{X, P, D\}_u). \quad (3.2)$$

Для відновлення відкритого тексту уповноважений користувач додає нульові інформаційні символи $C_j^* = C_j + C_{k-h_j}$, з відновленого закритого тексту C_j знімає дію секретних переставної та діагональної матриць P^u та D^u :

$$\begin{aligned}
 C &= C_j^* \times (D^u)^{-1} \times (P^u)^{-1} = \left(M_i \times \left(G_{x_{a_i}}^{U_i} \right)^T + e \right) \times \\
 &\times (D^u)^{-1} \times (P^u)^{-1} = \left(M_i \times \begin{pmatrix} X^u \times G_{x_{a_i}}^{U_i} \times \\ \times P^u \times D^u \end{pmatrix}^T + e \right) \times \\
 &\times (D^u)^{-1} \times (P^u)^{-1} = M_i \times (X^u)^T \times \left(G_{x_{a_i}}^{U_i} \right)^T \times (P^u)^T \times \\
 &\times (D^u)^T \times (D^u)^{-1} \times (P^u)^{-1} + e \times (D^u)^{-1} \times (P^u)^{-1} = \\
 &= M_i \times (X^u)^T \times \left(G_{x_{a_i}}^{U_i} \right)^T + e \times (D^u)^{-1} \times (P^u)^{-1},
 \end{aligned} \tag{3.3}$$

Разкодування отриманого вектору проводять за алгоритмом Берлекемпа-Мессі:

$$C = M_i \times (X^u)^T \times \left(G_{x_{a_i}}^{U_i} \right)^T + e \times (D^u)^{-1} \times (P^u)^{-1}, \tag{3.4}$$

тобто позбвляється від другого доданку і від співмножника $\left(G_{x_{a_i}}^{U_i} \right)^T$ у першому доданку у правій частині рівності, після чого знімає дію матриці маскування X^u . Для цього отриманий результат разкодування $M_i \times (X^u)^T$ слід помножити на $(X^u)^{-1}$: $(M_i \times (X^u))^T \times (X^u)^{-1} = M_i$. Отримане рішення – це відкритий текст M_i .

Далі уповноважений користувач, використовуючи набір матриць $\{X, P, D\}^u = \{X^u, P^u, D^u\}$ формує вектор: $\bar{c}^* = c_X^* \times (D^u)^{-1} \times (P^u)^{-1}$, таким чином демаскує кодову послідовність $c_{X_i}^*$. Після підстановки отримаємо рівність:

$$\begin{aligned}
 \bar{c}^* &= c_X^* \times (D^u)^{-1} \times (P^u)^{-1} = \\
 &= (c_{X_i} + M_i) \times (D^u)^{-1} \times (P^u)^{-1} = \\
 &= c_{X_i} \times (D^u)^{-1} \times (P^u)^{-1} + M_i \times (D^u)^{-1} \times (P^u)^{-1}.
 \end{aligned} \tag{3.5}$$

Уповноважений користувач, який сформував вектор, має можливість застосувати швидкий (поліноміальної складності) алгоритм завадостійкого

декодування та сформувати таким чином вектор $\bar{c}^* = c_x^* \times (D^u)^{-1} \times (P^u)^{-1}$ та вектор $M_i^u = M_i \times (D^u)^{-1} \times (P^u)^{-1}$. Для відновлення інформаційної рівноважної послідовності M_i достатньо знову помножити вектор M_i^u на матриці маскування P^u і D^u , у зворотній послідовності:

$$M_i = M_i^u \times P^u \times D^u = M_i \times (D^u)^{-1} \times (P^u)^{-1} \times P^u \times D^u = M_i. \quad (3.6)$$

Таким чином, запропонована модель дозволяє без зниження рівня стійкості забезпечити необхідні послуги безпеки інформаційних ресурсів об'єктів критичної інфраструктури, а також забезпечує можливість використання програмно-апаратних засобах з малою енергоємністю.

3.3. Забезпечення послуг безпеки об'єктів критичної інфраструктури на основі гібридних крипто-кодових конструкцій на збиткових кодах

Для реалізації НССС Мак-Еліса на *MEC* (*LDPC*-кодах) із заподіянням шкоди запропоновані методи формування криптограми (кодограми) та декодування [11], структурна схема передачі даних представлена на рис. 3.3 [46].

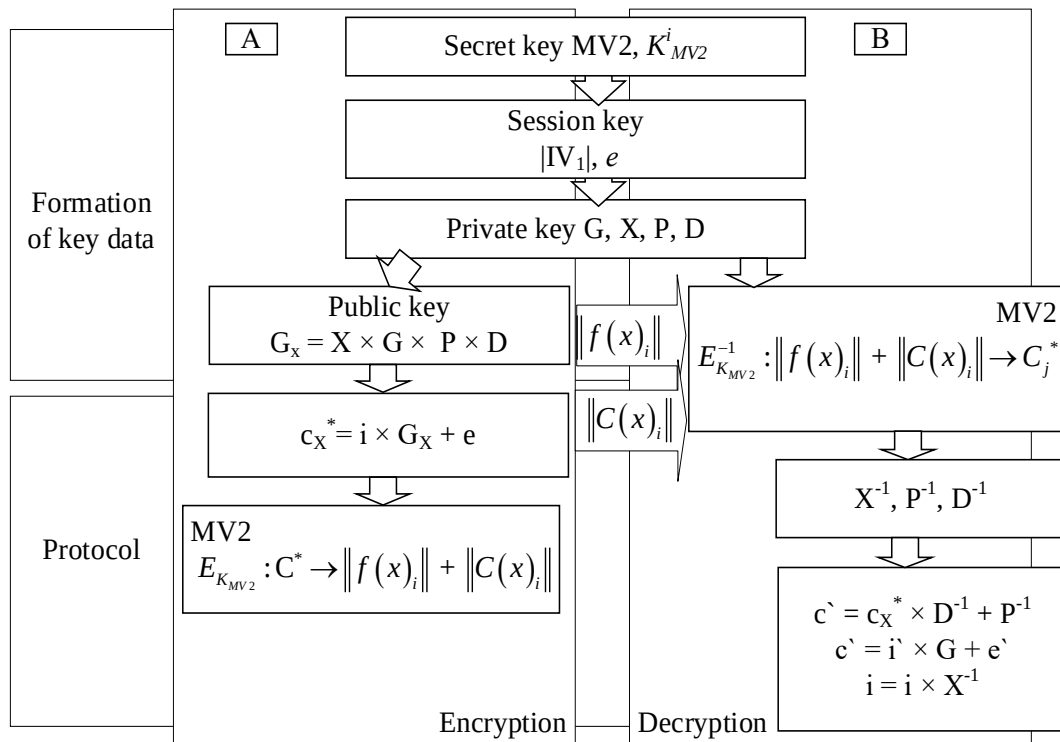


Рис. 3.3. Структурна схема гібридної *ССС Мак-Еліса* на *LDPC*-кодах із заподіянням збитку

Математична модель НССС Мак-Еліса використовує такі вихідні дані [37]:

- множина інформаційних ресурсів $I = \{I_1, I_2, \dots, I_{q^k}\}$, для всіх $I_j \in GF(q)$.
- множина криптоперетворень для формування кодового слова на матриці *LDPC*-коду, що породжує:

$C = (C_1, C_2, \dots, C_s)$, де $\phi_i : I \rightarrow C_{k-h_j}$, $i = 1, 2, \dots, s$. де h_j – формує вектори ініціалізації (IV_1 – вектор ініціалізації, який визначає кількість та місця «виколювання» символів у кодовому слові, IV_2 – вектор ініціалізації, який визначає кількість та місця «до давлення» інформаційних символів у кодовому слові);

- множина криптоперетворень, які дозволяють отримати вихідний інформаційний ресурс:

$$\phi^{-1} = \{\phi_1^{-1}, \phi_2^{-1}, \dots, \phi_s^{-1}\},$$

де $\phi_i^{-1} : C_{k-h_j} \rightarrow I$;

- множина відкритих ключів:

$$KU_i = \{KU_1, KU_2, \dots, KU_s\} = \{G_1^{U_j}, G_2^{U_j}, \dots, G_s^{LDPC}\}, \forall i \in \overline{1, \dots, s}$$

де $\begin{pmatrix} G_j^{U_j}, \forall j \in \{U_j\}, U_1 - EC, U_2 - MEC, U_3 - FC, U_1 - LDPC, \\ H_j^{U_j}, \forall j \in \{U_j\}, U_1 - EC, U_2 - MEC, U_3 - FC, U_1 - LDPC, \end{pmatrix}$ завадових кодів

(алгеброгеометричних кодів: *EC*, *MEC*, *LDPC*, збиткових кодів):

Для формування ключа використовуємо:

$$G_{x_{a_i}}^{U_j} = X^u \times G^{U_j} \times P^u, u \in \{1, 2, \dots, s\}; \quad (3.6)$$

- множина особистих (закритих) ключів користувачів:

$$KR = \{KR_1, KR_2, \dots, KR_r\} = \{X^i, P^i, D^i\}, \quad (3.7)$$

- множина збиткових текстів $(C(x)_i) - CFT = \{CFT_1, CFT_2, \dots, CFT_{q^k}\}$;
- множина збитків $(f(x)_i - \text{прапор})$, $CHD = \{CHD_1, CHD_2, \dots, CHD_{q^k}\}$;
- множина формування збиткового тексту та шкоди (на основі ключа алгоритму MV2) $- E = \{E_{K_{MV2}}^1, E_{K_{MV2}}^2, \dots, \phi_{K_{MV2}}^S\}$, $f(x) = n - |C(x)|$, якщо $|C(x)| > r$, де r
- певний параметр, $r \in_R Z_{q^m}$, $0 < r < n$;
- множина відображення $MV2 \rightarrow F_n^r$, що задає бієктивне відображення між множиною перестановок $\{S_1, S_2, \dots, S_{2^n}\}$ і множиною $\#F_n^r$, $\#F_n^r = \#\{(c, f)\} = 2^n!$;
- множина відображення неповноцінного тексту в інформаційний ресурс (на основі ключа $- K_{iMV2}$, і алгоритму MV2) $- E^{-1} = \{E_{K_{MV2}}^{1^{-1}}, E_{K_{MV2}}^{2^{-1}}, \dots, E_{K_{MV2}}^{S^{-1}}\}$, де $E_{K_{MV2}}^{-1} : \|f(x)_i\| + \|C(x)_i\| \rightarrow I$.

Відправник формує кодове слово: $C_j = M_i \times G_{x_{a_i}}^{U_j^T} + e$, де e додатковий сеансовий ключ кожної інформаційної посилки.

До алгоритму MV2 надходить кодове слово $C_j = M_i \times G_{x_{a_i}}^{U_j^T} + e$; перетворюється в алгоритмі MV2 у збитковий текст (залишок) та збиток (прапор):

$$E_{K_{MV2}} : C^* \rightarrow \|f(x)_i\| + \|C(x)_i\|. \quad (3.8)$$

У канал зв'язку надходить $\|f(x)_i\|$ і $\|C(x)_i\|$ при цьому передача може проводитись як по одному, так і по двох незалежних каналах.

На стороні прийому одержувач використовує правило завдання шкоди F_n^r , маскування, кількість та місця нульових інформаційних символів може розкодувати кодове слово та отримати інформаційне повідомлення:

$$E_{K_{MV2}}^{-1} : \|f(x)_i\| + \|C(x)_i\| \rightarrow C_j^*, I_i = \phi_u^{-1}(C_j^*, \{X, P, D\}_u). \quad (3.9)$$

При використанні подовженого модифікованого завадостійкого-коду одержувач додає нульові інформаційні символи (по вектору ініціалізації V_1), а також і «отримує» інформаційні символи (по вектору ініціалізації V_2).

З $C_j^* = C_j + C_{k-h_j}$ знімається дія матриць маскування:

$$\begin{aligned} C &= C_j^* \times (P^u)^{-1} = \left(I_i \times \left(G_{x_{a_i}}^{U_j} \right)^T + e \right) \times (P^u)^{-1} = \left(I_i \times \left(X^u \times G_{x_{a_i}}^{U_j} \times P^u \right)^T + e \right) \times \\ &\times (P^u)^{-1} = I_i \times (X^u)^T \times \left(G_{x_{a_i}}^{U_j} \right)^T \times (P^u)^T \times (P^u)^{-1} + e \times (P^u)^{-1} = \\ &= I_i \times (X^u)^T \times \left(G_{x_{a_i}}^{U_j} \right)^T + e \times (P^u)^{-1}, \end{aligned} \quad (3.10)$$

а потім розкодує отриманий вектор за алгоритмом Берлекемпа-Месі:

$$C = I_i \times (X^u)^T \times \left(G_{x_{a_i}}^{U_j} \right)^T + e \times (D^u)^{-1} \times (P^u)^{-1}, \quad (3.11)$$

Отримуємо інформаційний ресурс:

$$\left(I_i \cdot (X^u)^T \right) \times (X^u)^{-1} = I_i. \quad (3.12)$$

Таким чином, запропоновані підходи дозволяють використовувати ССС (НССС) Мак-Еліса для забезпечення послуг конфіденційності цілісності та автентичності та практично реалізувати запропонований метод [12, 33, 42].

Основною відмінністю від відомих підходів є за збереження рівня пропускних можливостей бездротового каналу інтегровано забезпечити необхідний рівень захищеності (криптостійкості) каналу (криптостійкість на основі постквантових алгоритмів на рівні 10^{25} – 10^{35} групових операцій), достовірності ($P_{ном}$ не нижче 10^{-9} – 10^{-12}) [43].

Висновки за главою 3

Запропоновані математичні моделі побудови несиметричних криптосистем на основі постквантових алгоритмів крипто-кодові конструкції Мак-Еліса та Нідеррайтера на алгеброгеометричних кодах (еліптичних,

модифікованих еліптичних кодах (укорочених та/або подовжених) забезпечують зменшення складності криптоперетворення у порівнянні з БСШ (формування ($\approx$ в 12 разів) і розкодування криптограми ($\approx$ у 20 разів), що дозволяє забезпечити послуги безпеки в умовах постквантового періоду (появи повномасштабного квантового комп'ютера).

Запропоновані різні конструкції алгеброгеометричних кодів забезпечує можливість використання крипто-кодових конструкцій Мак-Еліса та Нідеррайтера в програмно-апаратних (апаратних) засобах (застосунках) з низьким використанням енергомісткості, що дозволяє їх використання у будь-яких каналах зв'язку з урахуванням типу (міри секретності) інформаційних ресурсів.

Запропоновані гібридні крипто-кодові конструкції Мак-Еліса та Нідеррайтера на алгеброгеометричних кодах (еліптичних, модифікованих еліптичних кодах (укорочених та/або подовжених) на основі багатоканальної криптографії (зі збитковими) забезпечують необхідний рівень безпеки у постквантовий період та швидкодію криптоперетворень (кодування та розкодування) в офлайн режимі мобільного інтернет-трафіку. При цьому забезпечуються: криптостійкість (на основі постквантових алгоритмів на рівні 10^{25} – 10^{35} групових операцій), достовірність ($P_{ном}$ не нижче 10^{-9} – 10^{-12}).

РОЗДІЛ 4

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ КЕРУВАННЯ ОБ'ЄКТАМИ ТА БАЗИ ЗНАНЬ НА ОСНОВІ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

4.1. Архітектури та алгоритми функціонування безперервних нейронних мереж адаптивної резонансної теорії, здатних визначати декілька рішень

Дискретні нейронні мережі АРТ-1s дають можливість визначати кілька рішень (якщо вони існують), за рахунок того, що в архітектуру цієї мережі включений шар реєструючих нейронів – $Y_1^1, Y_2^1, \dots, Y_m^1$. Результати, що стосуються можливості отримання кількох рішень за допомогою дискретних нейронних мереж АРТ-1s можуть бути узагальнені і на безперервні нейронні мережі адаптивної резонансної теорії (АРТ-2). За аналогією з дискретною нейронною мережею АРТ-1s в архітектуру безперервної мережі АРТ-2 можна ввести шар Y^1 реєструючих нейронів і додатковий нейрон керуючий R^1 (рис. 4.1). На рис. 4.1 пунктирною лінією виділено класичну архітектуру безперервної нейронної мережі АРТ-2.

У режимі навчання класична безперервна нейронна мережа АРТ-2 і розроблювана безперервна нейронна мережа АРТ-2s, яка може вирішувати задачі з кількома рішеннями, функціонують аналогічно, оскільки нейрони R^1 і реєструючого Y^1 -шару у навчанні не беруть участі.

У режимі розпізнавання під час пошуку кількох рішень функціонування нейронних мереж АРТ-2 і АРТ-2s відрізняється. При цьому відмінність полягає у наступному. Перед початком режиму розпізнавання по ланцюгах, що управляють, всі нейрони мережі, включаючи і елементи реєструючого шару, переводяться в стан з нульовим вихідним сигналом. В активний стан нейрони реєструючого шару $Y_1^1, Y_2^1, \dots, Y_m^1$, як і нейрони Y -і Z -шару, перекладаються за правилом «два з трьох», коли поодинокі сигнали одночасно з'являються на виході нейрона-переможця Y_j розпізнає шару і на виході керуючого нейрона R^1 . Ці сигнали вказують на те, що вхідний вектор та вектор, що зберігається у вагах зв'язків нейрона-переможця, відповідають один одному за величиною параметра подібності і, отже, знайдено один із класів, до якого належить вхідний вектор. Одиничний вихідний сигнал нейрона Y_j^1 по ланцюгу зворотного зв'язку з ваговим коефіцієнтом два

надходить на його третій вхід і фіксує одиничний сигнал на виході елемента Y_j^1 . Вихідний сигнал нейрона Y_j^1 також загальмовує нейрон-переможець Y_j^1 ($U_{\text{вих}Y_j^1} = -1$). Потім у шарі нейронів, що розпізнають, починається пошук нового нейрона-переможця. Цей процес пошуку нейронів-переможців та їх загальмовування триває доти, доки не будуть загальмовані всі розподілені розпізнавальні Y -нейрони.

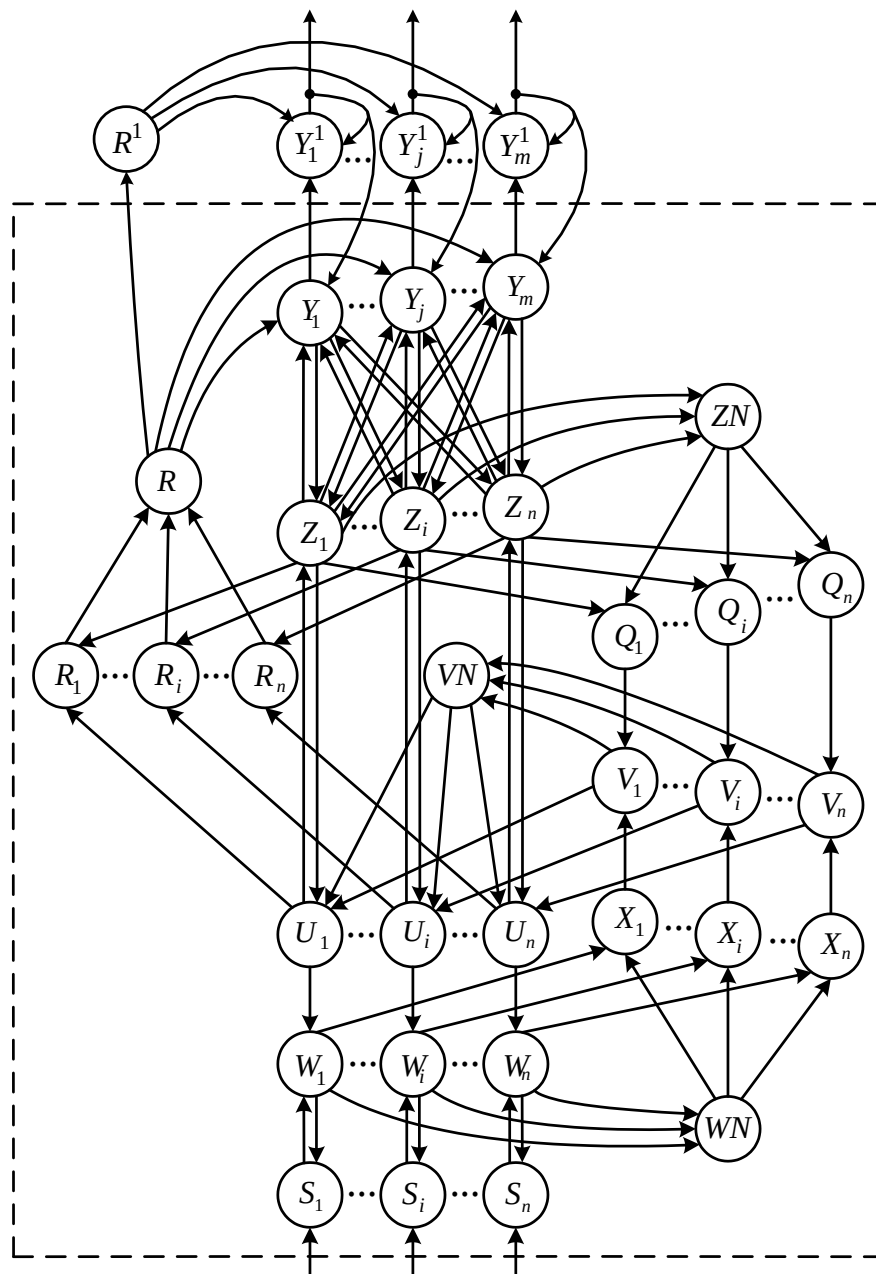


Рис. 4.1. Архітектура безперервної нейронної мережі ART-2s для пошуку кількох рішень

При цьому на виходах нейронів реєструючого шару можуть бути отримані такі варіанти рішення:

- на виходах елементів Y^1 -шару всі сигнали нульові, у цьому випадку на вхід нейронної мережі пред'явлено вектор, не схожий на жоден з векторів, що зберігаються в пам'яті мережі;

- на виходах елементів Y^1 -шару лише один одиничний сигнал, що вказує на належність вхідного вектора до одного з класів векторів, що зберігаються в пам'яті мережі;

- на виходах елементів Y^1 -шару є кілька одиничних сигналів, що вказують на те, що вхідний вектор належить кільком класам векторів або знаходиться на межі кількох класів.

Таким чином, безперервна нейронна мережа АРТ-2s дозволяє визначати одно-, два або більше рішень (якщо вони існують).

Даний алгоритм був реалізований у вигляді програмної функції для бібліотеки нейронних мереж, що входить до структури програмного забезпечення, яка здійснює інтелектуальне керування об'єктами. Однак, як показала практика застосування нейронних мереж АРТ-2s, складне нормування сигналів, яке закладено в її архітектурі, робить застосування даної нейромережі не завжди зручним. Тому була розроблена модифікація, пов'язана з можливістю визначення кількох рішень, для нейронної мережі АРТ-2m [130, 131], яка за своїми властивостями аналогічна нейронній мережі АРТ-2s але має більш просту архітектуру. Для цього в архітектуру цієї нейронної мережі, як і у випадку нейронної мережі АРТ-2s був введений шар Y^1 реєструючих нейронів і керуючий нейрон R^1 (рис. 4.2).

На рис. 4.2 наведена архітектура пропонованої безперервної нейронної мережі АРТ-2ms, причому, пунктирною лінією виділена базова архітектура існуючої нейронної мережі АРТ-2m.

У режимі навчання безперервні нейронні мережі АРТ-2m і АРТ-2ms функціонують аналогічно, як це описано в [130, 131], а в режимі розпізнавання функціонування цих нейронних мереж відрізняється. Розглянемо лише відмінності у функціонуванні пропонованої безперервної нейронної мережі АРТ-2ms як розпізнавання.

За аналогією з мережами АРТ-2s після визначення нейрона-переможця Y_J в розпізнавальному шарі нейронів за заданою величиною параметра подібності, поодинокі вихідні сигнали нейронів R^1 і Y_J переводять в активний стан елемент Y_J^1 реєструючого шару: $U_{\text{вих}Y_J^1} = 1$. Сигнал з виходу нейрона

Y_j^1 загальмовує нейрон Y_j і ланцюгом зворотного зв'язку фіксує активний стан нейрона Y_j^1 . Після чого перевіряється умова зупинки $U_{\text{вих}Y_k} = -1, k = 1, \dots, q$.

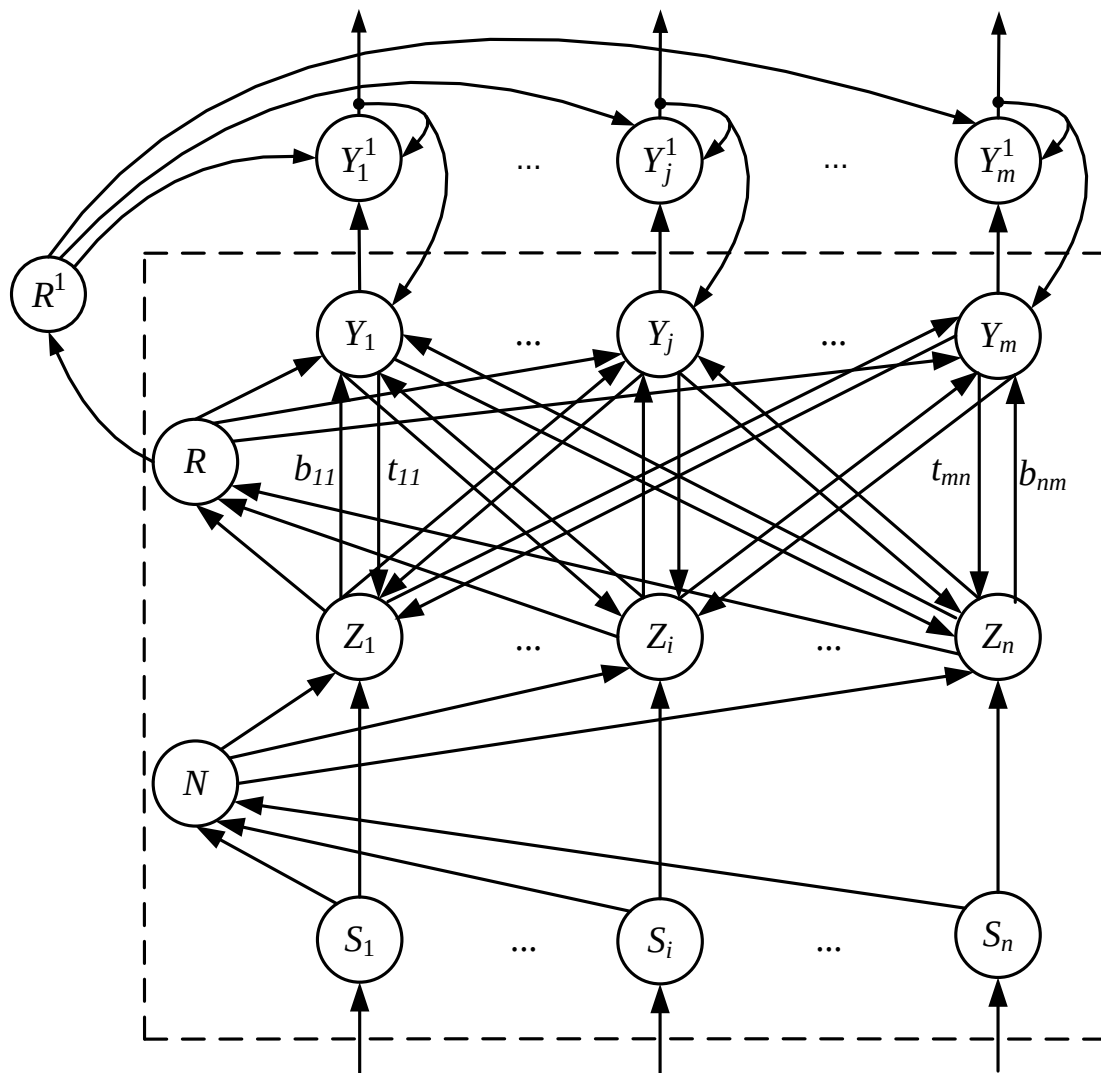


Рис. 4.2. Архітектура безперервної нейронної мережі ART-2 ms для пошуку кількох рішень

Якщо умова зупинки роботи алгоритму не виконується, перехід до пошуку нового нейрона-переможця. В іншому випадку здійснюється перехід на останній крок алгоритму.

Як і у випадку, розглянутому вище, для нейронних мереж ART-2s, на виходах нейронів Y^1 -шару може не бути жодного, один або кілька одиничних сигналів. У першому випадку вхідне зображення не схоже на жодне з зображень, що зберігаються в пам'яті мережі.

У другий випадок у пам'яті мережі є лише одне зображення, відповідне вхідному зображенню за величиною параметра подібності, у разі – таких зображень кілька.

Таким чином, розроблена безперервна нейронна мережа АРТ-2 ms , яка дозволяє вирішувати задачі з декількома рішеннями та має простішу архітектуру та алгоритм функціонування, порівняно з нейронними мережами АРТ-2 s .

Нейронна мережа АРТ-2 ms також була реалізована у вигляді програмної функції для бібліотеки нейронних мереж, що входить до структури розробленого програмного забезпечення.

Підхід, пов'язаний з можливістю визначення нейронною мережею декількох рішень (у разі їх існування), що передбачає модифікацію вихідної архітектури мережі шаром реєструючих нейронів, може бути узагальнений і на інші нейронні мережі, які мають аналогічний безперервним нейронним мережам АРТ розпізнавальний шар елементів, який дозволяє в певні моменти часу, визначатиме лише одне рішення.

Наведемо приклади таких модифікованих нейронних мереж.

Безперервні нейронні мережі АРТ-2Д [140, 156] призначені для розпізнавання процесів щодо їх приналежності до певних областей зміни змінних. Кордони цих областей сформовані за допомогою верхніх і нижніх обгинаючих в режимі навчання.

Якщо процес протікає на межі двох таких областей, його можна віднести до обох областей, тобто до двох класів процесів. У тих випадках, коли в процесі функціонування об'єкт істотно змінює режим своєї роботи, кількість спостережуваних класів процесів може бути і більше двох.

Отже, необхідно, щоб нейронна мережа могла визначати кілька можливих рішень або виділяти послідовність рішень, що змінюють один одного. Для цього в архітектуру нейронної мережі АРТ- 2Д вводиться шар реєструючих нейронів (рис. 4.3).

Нейронна мережа АРТ-2Д та АРТ-2Д s у режимі навчання функціонують аналогічно, при цьому використовується алгоритм навчання, описаний у [140, 156]. У режимі розпізнавання їхня функціонування трохи відрізняється, тому розглянемо лише відмінності алгоритму роботи нейронної мережі АРТ-2Д s в режимі розпізнавання.

При цьому в алгоритмі роботи мережі АРТ-2Д прийняті такі ж позначення, що і в алгоритмі навчання АРТ-2Д.

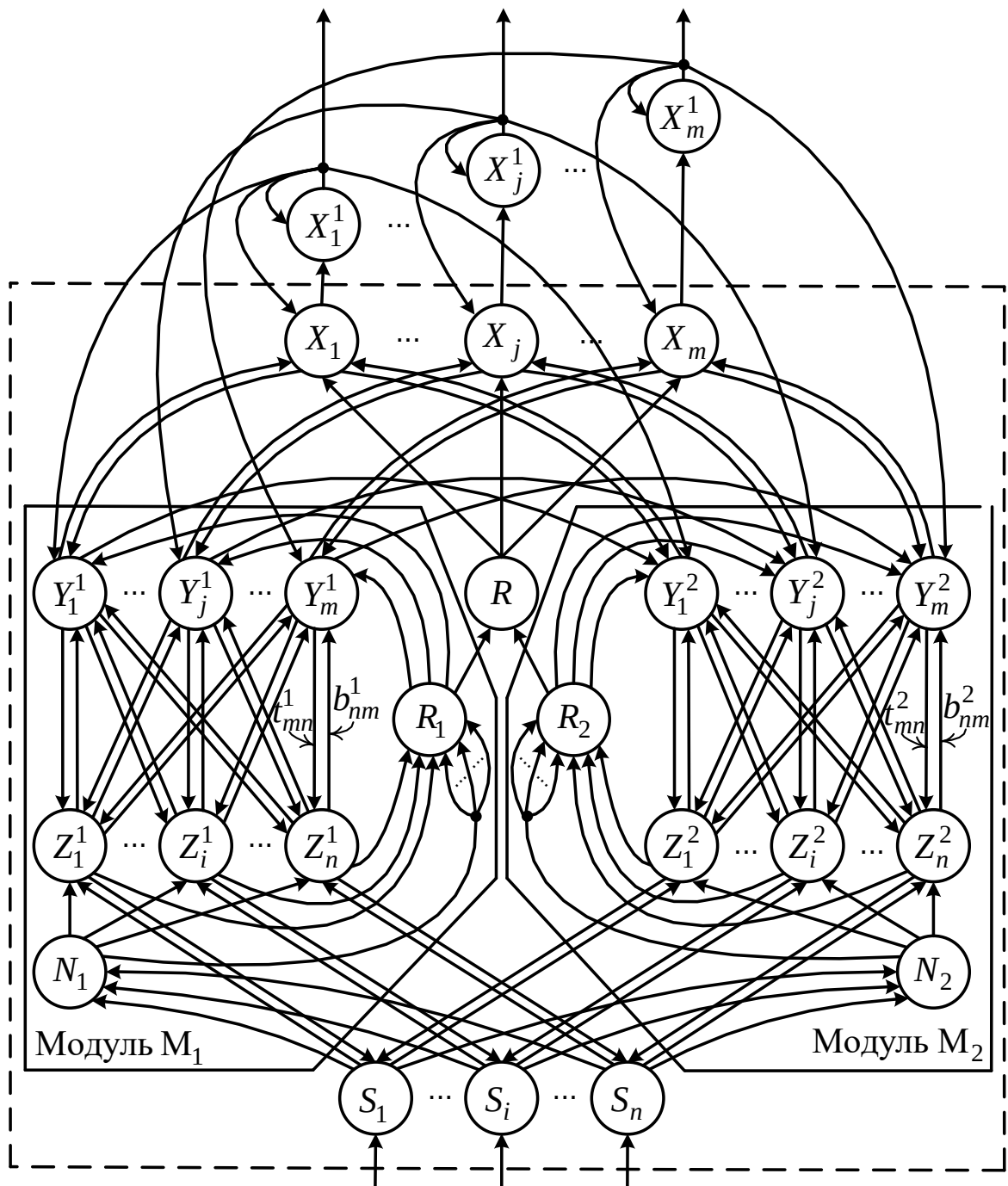


Рис. 4.3. Архітектура нейронної мережі АРТ-2Дс для пошуку кількох рішень

Алгоритм роботи мережі в режимі розпізнавання передбачає виконання наступних кроків:

Крок 1. Ініціюються параметри та ваги зв'язків мережі. Визначаються нульові вихідні сигнали всіх нейронів.

Крок 2. На вхід нейронної мережі подається вхідне зображення $S^* = (s_1^*, \dots, s_n^*)$, що відповідає l -му режиму функціонування об'єкта і для нього починається виконання кроків 3 – 19 алгоритму.

Крок 3. Вхідним вектором S^* визначаються вхідні та вихідні сигнали нейронів S -шару:

$$U_{\text{вх}S_i} = S_i^*; U_{\text{вих}S_i} = U_{\text{вх}S_i}, i = 1, \dots, n.$$

Далі виконуються кроки 4 – 17, які повністю аналогічні крокам алгоритму роботи нейронної мережі АРТ- 2Д в режимі розпізнавання [140, 156].

Крок 18. За обчисленими значеннями параметрів подібності p_1, p_2 для обох модулів мережі перевіряється відповідність процесів $I_k(t_i), k = 1, \dots, K, t_i = 0, 1, \dots, T$ зображення S^* областям D_k^l ($k = 1, \dots, K$) l -го режиму функціонування динамічного об'єкта: $p \leq p_1 + p_2 - 1$. Якщо умова виконується, вхідне зображення S^* розпізнається як l -й режим функціонування об'єкта. На це вказуватиме одиничний вихідний сигнал нейрона X_J , який переводиться в активний стан одиничними вихідними сигналами нейронів Y_J^1, Y_J^2, R . Сигнал $U_{\text{вих}R} = 1$ з'являється лише за трьох умов: $p_1 \geq p, p_2 \geq p, p \leq p_1 + p_2 - 1$. Якщо умова $p \leq p_1 + p_2 - 1$ не виконується, перехід до кроку 8 алгоритму.

Крок 19. Одиничний вихідний сигнал нейрона X_J переводить в активний стан елемент X_J^1 реєструючого шару нейронів: $U_{\text{вих}X_J^1} = 1$. Сигнал $U_{\text{вих}X_J^1}$ з ланцюга зворотного зв'язку фіксує активний стан нейрона X_J^1 . Цей сигнал загальмовує нейрони Y_J^1, Y_J^2 і X_J .

Крок 20. Перевіряється умова зупинки: $U_{\text{вих}Y_k^1} = -1, k = 1, \dots, q$, де q – кількість розподілених нейронів, що розпізнають. Якщо умова зупинки роботи алгоритму не виконується, перехід до кроку 8 алгоритму. Інакше – перехід до наступного кроку алгоритму.

Крок 21. Зупин.

В результаті роботи алгоритму на виходах нейронів реєструючого X^1 шару може не бути жодного, один або кілька одиничних сигналів.

У першому випадку вхідне зображення несе нову інформацію і не схоже за величиною параметра подібності на жодне з зображень, що зберігаються в пам'яті мережі.

У другому та третьому випадках у пам'яті мережі є відповідно одне або кілька зображень, що підходять вхідному зображенню за величиною параметра подібності.

Таким чином, розроблена безперервна нейронна мережа АРТ-2Дс для вирішення завдань, що мають одне, два або більше рішень.

У роботах [157, 158] описана архітектура та алгоритми функціонування безперервної ДАП, розробленої на основі двох модулів M_1 і M_2 , кожен з яких являє собою безперервну нейронну мережу АРТ-2Д. Заміна нейронних мереж АРТ-2Д на описані раніше мережі АРТ-2Дс дозволить безперервний ДАП визначати кілька рішень (рис. 4.4). Алгоритм навчання у цій мережі такий самий, як і у ДАП на основі АРТ-2Д [157, 158], а алгоритм роботи мережі трохи відрізняється.

Відмінності стосуються тільки тієї частини алгоритму, яка відрізняє роботу мереж АРТ-2Дс від мереж АРТ-2Д.

Проте, дискретні нейронні мережі АРТ мають і певні недоліки [132 – 134]:

- результати її навчання класичним алгоритмом [135] у загальному випадку залежать від порядку проходження зображень в навчальній послідовності;

- міра близькості зображень, що зберігаються у пам'яті мережі і що надходять її входи, визначається з допомогою параметра подібності: $p = \|Z\|/\|S\|$, де $\|Z\|$ -норма вектора, що зберігається в пам'яті мережі, яка обчислюється як сума його одиничних компонентів;

$\|S\|$ – норма вектора вхідних сигналів. З визначення параметра подібності випливає, що близькість чорно-білих зображень визначається лише розташуванням їх поодиноких (чорних) компонентів.

Наприклад, якщо два зображення Z , S містять по 100 компонентів, з яких у кожного зображення є лише по 10 одиничних компонентів, причому, в обох зображеннях однаково розташовані тільки п'ять одиничних компонентів, то параметр подібності в цьому випадку дорівнює $p = \|Z\|/\|S\| = 5/10 = 0,5$.

Таке значення параметра подібності вказує на те, що зображення Z та S істотно відрізняються один від одного. Однак, використання інших заходів близькості цих зображень, наприклад, з використанням відстані Хеммінгу, вказує на певну близькість цих зображень.

Дійсно, відстань Хеммінга в цьому випадку дорівнює 10 (десять двійкових компонент зображень, що не збігаються), а відношення числа збігаються компонент до їх загального числа дорівнює 0,9.

Таким чином, зображення відрізняються лише 10% своїх компонентів, що вказує на суттєву схожість порівнюваних зображень.

У зв'язку з цим виникає необхідність розробки нової архітектури нейронної мережі, яка, з одного боку, зберегла б у собі позитивні властивості стабільно-пластичних дискретних нейронних мереж АРТ [136], здатних розпізнавати нову інформацію, донавчатися в процесі свого функціонування і визначати кілька рівноцінних рішень, а з іншого боку, використовувала в процесі свого функціонування міру близькості на відстані Хеммінга, тобто параметр подібності між вхідним та еталонними зображеннями, що враховує всі компоненти бінарних векторів, в яких вони збігаються, що значно підвищить точність її функціонування [137, 138].

З урахуванням описаних вище особливостей, розробимо стабільно-пластичну нейронну мережу Хеммінга, здатну розпізнавати нову інформацію, донавчатись і визначати кілька рівноцінних рішень при класифікації зображень, що знаходяться на мінімальній відстані Хеммінга від одного, двох або трьох еталонних зображень, що зберігаються у вагах зв'язків нейронної мережі.

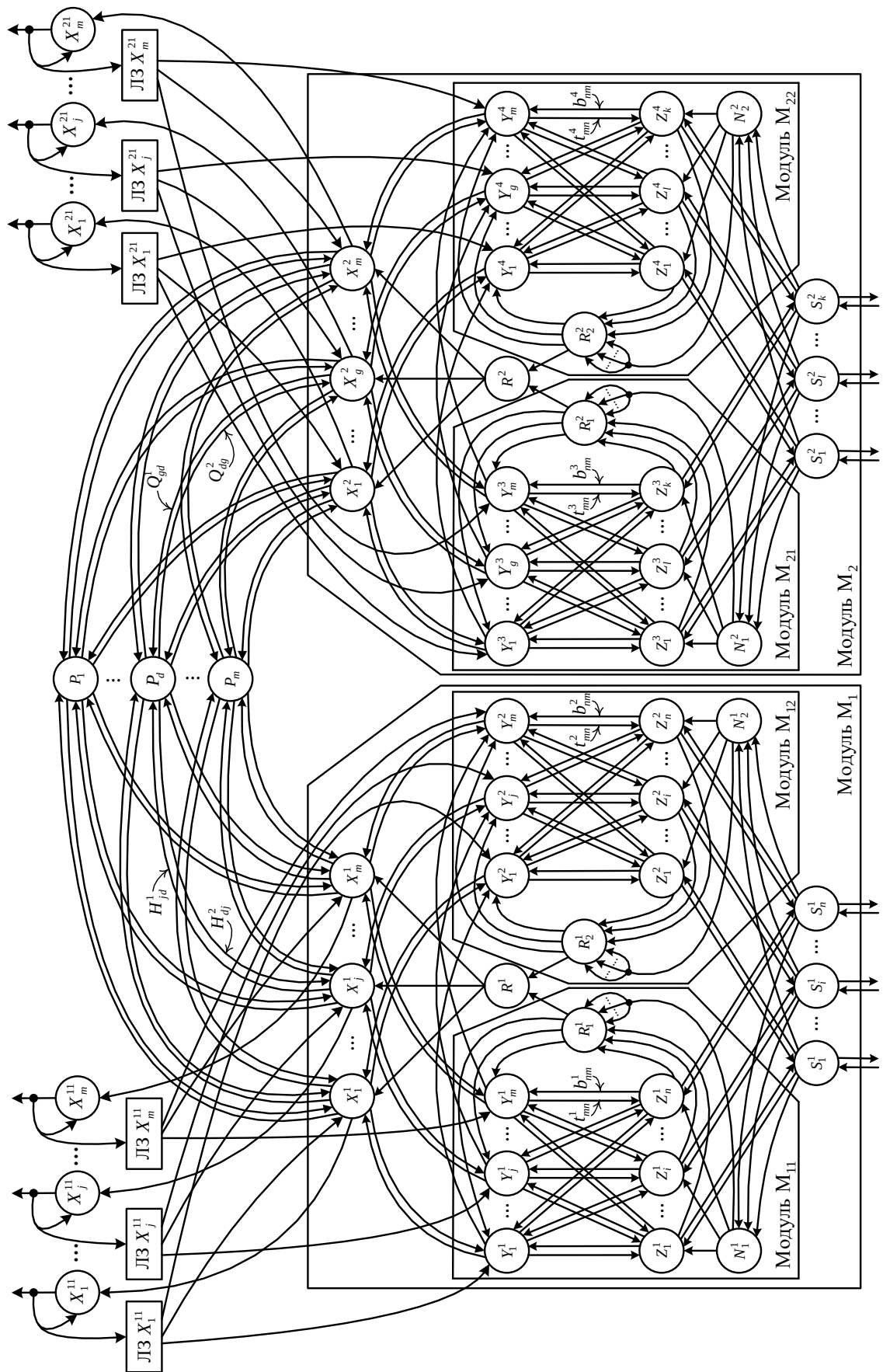


Рис. 4.4. Схема безперервної ДАП на основі мереж АРТ-2Дс, що дозволяють визначати декілька рішень

4.2. Стабільно-пластичні нейронні мережі Хеммінга, Хебба та мережі на основі перцептрону здатні розпізнавати нову інформацію, донавчатись та визначати декілька рішень

Одна з основних переваг, описаних вище безперервних стабільно-пластичних нейронних мереж АРТ-2s і АРТ-2ms – можливість донавчатись або можливість запам'ятовувати нову інформацію без спотворення мережі, що вже зберігається в пам'яті. Ця здатність всіх нейронних мереж АРТ забезпечується наявністю додаткових нейронів, куди й записується нова інформація. Принцип функціонування розпізнаючих нейронів полягає в тому, що частина нейронів Y -шару зберігає інформацію (еталонні зображення) про відомі класи зображень, а Y -нейрони, що залишилися, можуть використовуватися для запису нової інформації. При цьому кожен Y -нейрон зберігає, або зберігатиме, у своїх вагах зв'язків інформацію лише про одне зображення. Подібний шар нейронів має мережу Хеммінга (рис. 4.5), де кожен Z -нейрон у вагах своїх зв'язків зберігає інформацію про одне зображення, що є представником свого класу. Якщо в шар Z -нейронів мережі Хеммінга ввести додаткові Z -нейрони (і відповідні їм A - і Y -нейрони), здатні запам'ятовувати нову інформацію (еталонні зображення нових класів), то така мережа також зможе донавчатись і матиме властивості стабільності та пластичності, тобто властивостями нейронних мереж АРТ [139, 140].

Ще одна перевага нейронних мереж АРТ – можливість виділяти нову інформацію. Це досягається тим, що вхідне зображення порівнюється за величиною параметра подібності з еталонними зображеннями, що зберігаються у вагах зв'язків нейронів, що розпізнають. Якщо вхідне зображення відноситься до нового класу, то при порівнянні з будь-яким еталонним зображенням, що зберігається у вагах зв'язків розподілених нейронів, що розпізнають, виходить параметр подібності менше мінімально допустимого. Тому в результаті такого порівняння всі розподілені Y -нейрони, що розпізнають, будуть загальмовані, що і є ознакою того, що вхідне зображення несе нову інформацію, якої немає в пам'яті нейронної мережі АРТ [141].

У нейронної мережі Хеммінга порівняння зображень (або біполярних векторів) виконується за кількістю компонентів, в яких вхідне та еталонне зображення збігаються: $a = n - R_x$, де n – кількість компонентів зображення; R_x – відстань Хеммінгу між зображеннями. Тому за аналогією з нейронними мережами АРТ можна задати мінімально допустиме значення числа

збігаються компонент $a_{\min}$, при яких можуть порівнюватися вхідне та еталонне зображення, а при $a < a_{\min}$ вхідне зображення та еталонне незрівнянні або, іншими словами, вхідне зображення несе нову інформацію порівняно із зображенням, що зберігається у вагах зв'язків нейронної мережі.

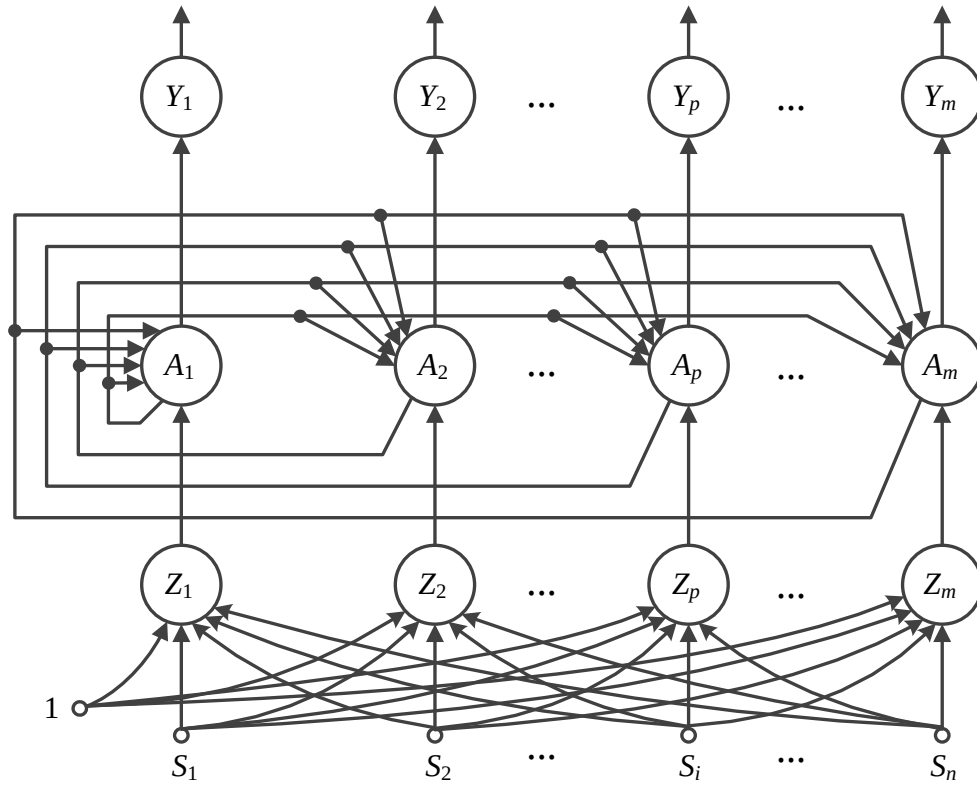


Рис. 4.5. Нейронна мережа Хеммінгу

Врахувати значення $a_{\min}$ в архітектурі нейронної мережі нескладно - достатньо ввести додаткове зміщення на нейрони Z-шару (точніше - змінити величину зміщення $n/2$). При цьому вихідні сигнали Z-нейронів будуть описуватись модифікованим співвідношенням:

$$U_{\text{вих}Z_p} = \frac{n}{2} - a_{\min} + 1 + \sum_{i=1}^n W_{ip} U_{\text{вих}S_i} = a - a_{\min} + 1, \quad p=1, \dots, q, \quad (4.1)$$

де q – кількість Z-нейронів, що зберігають еталонні зображення.

З (4.1) випливає:

$$U_{\text{вих}Z_p} = \begin{cases} 0, & \text{якщо } a < a_{\min}, \\ 1, & \text{якщо } a = a_{\min}, \\ U_{\text{вих}Z_p} > 1, & \text{якщо } a > a_{\min}. \end{cases}$$

Таким чином, якщо на виході всіх розподілених Z -нейронів вихідні сигнали дорівнюють нулю ($U_{\text{вих}Z_p} = 0, p = 1, \dots, q$), то вхідне зображення за прийнятим критерієм близькості зображень не є схожим на жодне з відомих еталонних зображень і несе нову інформацію. Для апаратного визначення новизни вхідного зображення в архітектуру нейронної мережі Хеммінга (або мережі Хеммінга, що розпізнає зображення на межах декількох класів) достатньо ввести один нейрон Σ , що підсумовує вихідні сигнали всіх нейронів Z -шару. Якщо після пред'явлення вхідного зображення на виході нейрона Σ нульовий вихідний сигнал, це означає, що вхідне зображення на відстані Хеммінга знаходиться далеко від еталонних зображень, що зберігаються у вагах зв'язків нейронів Z -шару, і є представником нового класу зображень. Якщо після пред'явлення вхідного зображення вихідний сигнал нейрона Σ позитивний, це означає, що вхідне зображення є представником відомого класу зображень, що у пам'яті нейронної мережі.

Ще одним істотним недоліком мережі Хеммінга є те, що вона не виділяє два або більше еталонних зображень, що мають з пред'явленим зображенням однакові максимальні заходи близькості. Це з особливістю функціонування нейронів A -шару.

Шар A -нейронів функціонує циклічно, динаміка елементів описується ітераційним виразом.

$$U_{\text{вих} A_p}(t+1) = q_A(U_{\text{вих} A_p}(t) - \varepsilon \sum_{j=1, j \neq p}^m U_{\text{вих} A_j}(t)), \quad (4.2)$$

$$p = 1, \dots, m, \quad t = 0, 1, 2, \dots,$$

за початкових умов

$$U_{\text{вих} A_p}(0) = U_{\text{вих} Z_p}, \quad p = 1, \dots, m. \quad (4.3)$$

Якщо серед вхідних сигналів нейронів $A_1, \dots, A_m$ виявиться один найбільший сигнал $U_{\text{вих} A_p}$, то в результаті ітераційного процесу (4.2) тільки один A -нейрон залишиться з вихідним сигналом, більшим за нуль. Оскільки вихідні сигнали A -елементів надходять на входи Y -нейронів, то в результаті на виході мережі Хеммінга лише один нейрон Y_p виявиться з одиничним вихідним сигналом. Одиничний вихід цього нейрона і нульові виходи всіх інших і будуть вказувати на те, що пред'явлене зображення S^q найближче, у сенсі відстані Хеммінга, до еталонного зображення, що зберігається у вагах зв'язків нейрона Z_p . В іншому випадку, коли на вході A -нейронів виявиться

не один, а кілька сигналів з однаковим найбільшим значенням, мережа не зможе виділити єдиний максимальний сигнал і в результаті її функціонування на виходах всіх A -і Y -нейронів з'являться нульові сигнали.

Архітектура стабільно-пластичної нейронної мережі Хеммінга наведена на рис. 4.4, у якій кожен нейрон S_i ($i = 1, \dots, n$) пов'язаний із входом кожного елемента Z_p ($p = 1, \dots, m$) зв'язками з вагами W_{ip} . Ваги зв'язків $W_{1p}, \dots, W_{np}$ містять інформацію про p -му еталонному зображенні $V^p = (V_1^p, \dots, V_n^p)$: $W_{1p} = V_1^p / 2, \dots, W_{np} = V_n^p / 2$.

При пред'явленні вхідного зображення $S^* = (S_1^*, \dots, S_m^*)$ кожен Z -нейрон розраховує свій вхідний та вихідний сигнали. Вихідні сигнали $U_{\text{вих } Z_1}, \dots, U_{\text{вих } Z_m}$ Z - елементів, є вхідними сигналами A -нейронів – $a_1, \dots, a_m$.

Мережа функціонує циклічно, динаміка нейронів описується ітераційним співвідношенням (4.2) за початкових умов (4.3). Вихідні сигнали нейронів у результаті ітераційної процедури поступово зменшуються.

Якщо серед вхідних сигналів $a_1, \dots, a_m$ нейронів $A_1, \dots, A_m$ є один найбільший сигнал a_p ($p \in \{1, 2, \dots, m\}$), то результаті ітераційного процесу лише один нейрон A_p залишиться с вихідним сигналом, великим нуля. Якщо максимальних сигналів два або більше, то на виходах всіх нейронів у результаті ітераційного процесу будуть нульові вихідні сигнали. Для подолання нестачі мережі Хеммінга необхідно до закінчення ітераційного процесу виділяти однакові максимальні вихідні сигнали за допомогою додаткових нейронів.

Архітектура пропонованої нейронної мережі (рис. 4.6) відрізняється від архітектури відомої мережі Хеммінга (рис. 4.5), наявністю двох додаткових шарів нейронів: X -шару та Σ -шару [142, 143].

Нейрони X - і Σ -шару мають функцію активації виду:

$$g(U_{\text{вх}}) = \begin{cases} 1, & \text{якщо } U_{\text{вх}} > 0, \\ 0, & \text{якщо } U_{\text{вх}} \leq 0, \end{cases} \quad (4.4)$$

де $U_{\text{вх}}$ – вхідний сигнал нейрона, що має функцію активації $g(U_{\text{вх}})$.

Вхідні сигнали $U_{\text{вх } X_p}$ ($p = 1, \dots, m$), нейронів X -шару описуються наступним виразом:

$$U_{\text{вх}X_p} = U_{\text{вх}X_p} W_{X_p X_p} + U_{\text{вх}Y_p} W_{Y_p X_p} + \sum_{i=0}^3 W_{\Sigma_i X_p} U_{\text{вх}\Sigma_i} + W_{0p}^3 \cdot 1, \quad (4.5)$$

де $U_{\text{вх}X_p}, U_{\text{вх}Y_p}$ ($p=1, \dots, m$) – відповідно вихідні сигнали нейронів X - та Y -шару; $W_{X_p X_p}$ – вага зворотного зв'язку нейрона X_p ($p=1, \dots, m$); $W_{Y_p X_p}$ – вага зв'язку з виходу нейрона Y_p на вхід нейрона X_p ($p=1, \dots, m$); $W_{\Sigma_i X_p}$ – вага зв'язку від нейрона Σ_i ($i=0, 1, 2, 3$) до нейрона X_p ($p=1, \dots, m$); $U_{\text{вх}\Sigma_i}$ ($i=0, 1, 2, 3$) – вихідні сигнали нейронів Σ -шару; W_{0p}^3 – вага зв'язку сигналу зміщення нейрона X_p ($p=1, \dots, m$).

Вхідні сигнали нейронів Σ -шару описуються співвідношеннями:

$$U_{\text{вх}\Sigma_0} = \sum_{p=1}^m U_{\text{вх}Y_p} W_{Y_p \Sigma_0}; \quad (4.6)$$

$$U_{\text{вх}\Sigma_1} = \sum_{p=1}^m U_{\text{вх}Y_p} W_{Y_p \Sigma_1} + U_{\text{вх}\Sigma_0} W_{\Sigma_0 \Sigma_1} + W_{01}^4 \cdot 1; \quad (4.7)$$

$$U_{\text{вх}\Sigma_2} = \sum_{p=1}^m U_{\text{вх}Y_p} W_{Y_p \Sigma_2} + U_{\text{вх}\Sigma_1} W_{\Sigma_1 \Sigma_2} + U_{\text{вх}\Sigma_0} W_{\Sigma_0 \Sigma_2} + W_{02}^4 \cdot 1; \quad (4.8)$$

$$U_{\text{вх}\Sigma_3} = \sum_{p=1}^m U_{\text{вх}Y_p} W_{Y_p \Sigma_3} + U_{\text{вх}\Sigma_2} W_{\Sigma_2 \Sigma_3} + U_{\text{вх}\Sigma_1} W_{\Sigma_1 \Sigma_3} + U_{\text{вх}\Sigma_0} W_{\Sigma_0 \Sigma_3} + W_{03}^4 \cdot 1; \quad (4.9)$$

де $U_{\text{вх}Y_p}$ – вихідний сигнал нейрона Y_p , $p=1, \dots, m$; $W_{Y_p \Sigma_j}$ – $p=1, \dots, m$, вага зв'язку від нейрона Y_p до Σ_j нейрона $W_{Y_p \Sigma_j} = -1$ $j=0, 1, 2, 3$; $U_{\text{вх}\Sigma_j}$ – вихідний сигнал нейрона Σ_j , $j=0, 1, 2, 3$; $W_{\Sigma_k \Sigma_{k+1}}$ – вага зв'язку від нейрона Σ_k до нейрона Σ_{k+1} ; $k=0, 1, 2$ W_{0j}^4 – вага зв'язку сигналу зміщення нейрона Σ_j , $j=1, 2, 3$, $W_{0j}^4 = j$.

Якщо на виходах чотирьох або більшого числа A -нейронів є позитивні вихідні сигнали, які викликають поодинокі вихідні сигнали на виходах відповідних Y -нейронів, то сигнали $U_{\text{вх } \Sigma_1}$, $U_{\text{вх } \Sigma_2} - U_{\text{вх } \Sigma_3}$ негативні.

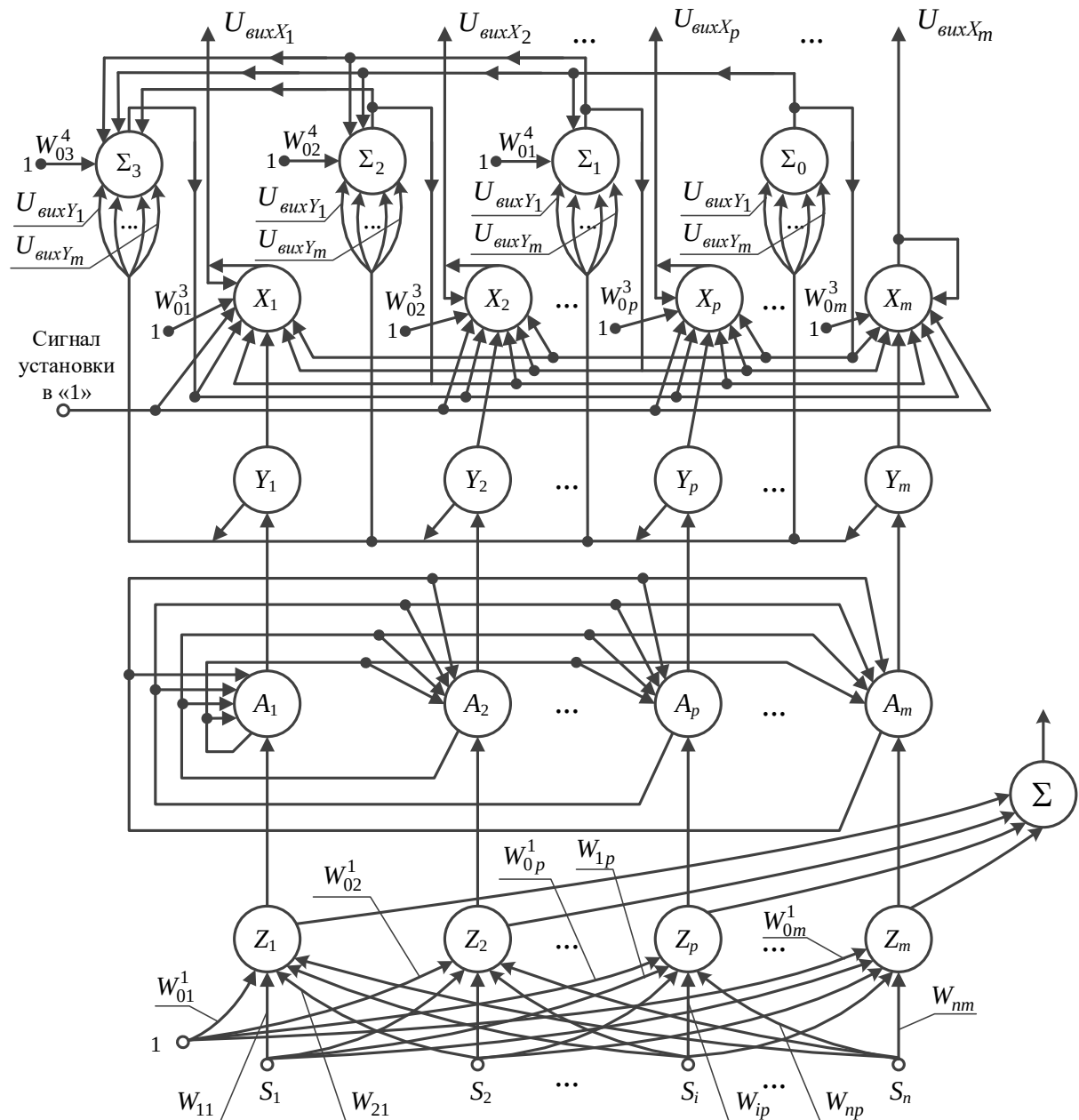


Рис. 4.6. Нейронна мережа, яка використовує відстань Хеммінга та класифікує зображення, що знаходяться на мінімальній відстані від одного, двох або трьох еталонних зображень

Відповідно до функції активації (4.4) на виходах нейронів $\Sigma_1, \Sigma_2, \Sigma_3$ будуть нульові вихідні сигнали. Якщо виходах лише трьох A -нейронів будуть

позитивні сигнали, наприклад, у нейронів A_{p1} , A_{p2} і A_{p3} , тоді відповідно до виразом (4.9) маємо: $U_{\text{вх } \Sigma_3} = 0$.

При нульовому вхідному сигналі $U_{\text{вх } \Sigma_3} = 0$ та функції активації нейрона Σ_3 виду (4.9) на виході нейрона з'явиться одиничний вихідний сигнал $U_{\text{вих } \Sigma_3} = 1$ який надійде на входи всіх нейронів X -шару. Відповідно до виразу (4.5) на входах X -нейронів будуть наступні вхідні сигнали: $U_{\text{вх } X_p} = -1, p = 1, \dots, m, p \neq p_1, p_2, p_3; U_{\text{вх } X_p} = 0, p = p_1, p_2, p_3$.

Таким чином, на виходах нейронів $X_p (p = 1, \dots, m, p \neq p_1, p_2, p_3)$ будуть нульові вихідні сигнали, а на виходах нейронів X_{p1}, X_{p2}, X_{p3} будуть одиничні вихідні сигнали.

При появі на виходах нейронів X_{p1} , одиничних X_{p2} сигналів X_{p3} ці сигнали по ланцюгу зворотного зв'язку з вагою $W_{X_p X_p} = 2 (p = p_1, p_2, p_3)$ надходять на входи цих нейронів. Сигнали зворотного зв'язку цих нейронів будуть підтримувати невід'ємні вхідні сигнали навіть тоді, коли виконуватимуться умови $U_{\text{вих } \Sigma_3} = 0; U_{\text{вих } Y_{p1}} = U_{\text{вих } Y_{p2}} = U_{\text{вих } Y_{p3}} = 0$. Таким чином, якщо вхідне зображення знаходиться на однаковій мінімальній відстані Хеммінга від трьох еталонних зображень, що зберігаються у вагах зв'язків нейронів Z_{p1}, Z_{p3} то Z_{p2} вихідні сигнали нейронів A_{p1} одночасно A_{p2} стають A_{p3} рівними нулю. При цьому $U_{\text{вих } A_{p1}} = U_{\text{вих } A_{p2}} = U_{\text{вих } A_{p3}} = U_{\text{вих } \Sigma_3} = 0$ і $U_{\text{вих } X_{p1}} = U_{\text{вих } X_{p2}} = U_{\text{вих } X_{p3}} = 1$. Отже, на виході нейронної мережі залишаються поодинокі сигнали нейронів, що вказують від яких трьох зображень, знаходиться вхідне зображення на мінімальній відстані.

Якщо сигнали на виходах A -нейронів не одночасно стають рівними нулю, наприклад, спочатку на виході одного нейрона $A_p (p = p_1, p_2, p_3)$ з'являється нульовий сигнал, наприклад, $U_{\text{вих } A_{p3}} = 0$ тоді одиничний сигнал на виході нейрона X_{p3} повинен бути скинутий в нуль. Це досягається так:

1. Відповідно до виразу (4.8) спрацьовує нейрон Σ_2 : $U_{\text{вх } \Sigma_2} = 0$ і $U_{\text{вих } \Sigma_2} = 1$.

2. Вихідний сигнал нейрона Σ_2 загальмовує нейрон Σ_3 , оскільки за співвідношенням (4.9) $W_{\Sigma_2 \Sigma_3} = -4$ маємо $U_{\text{вх } \Sigma_3} = -3$ і $U_{\text{вих } \Sigma_3}(-3) = 0$.

3. Відповідно до виразу (4.5) вхідний сигнал нейрона X_{p3} буде негативним, а вихідний – нульовим.

4. Відповідно до виразу (4.5) вхідні сигнали нейронів X_{p1} будуть X_{p2} невід’ємними, а вихідні – одиничними.

5. Якщо сигнали $U_{вихA_{p1}}$ і $U_{вихA_{p2}}$ одночасно стануть нульовими, то на виходах нейронів X_{p1} залишаться X_{p2} поодинокі вихідні сигнали, що вказують на те, що вхідне зображення знаходиться на однаковій відстані Хеммінга від еталонних зображень, що зберігаються у вагах зв’язків нейронів $Z_{p1} \cdot Z_{p2}$.

Якщо сигнали $U_{вихA_{p1}}$ і $U_{вихA_{p2}}$ не звертаються одночасно в нуль, а спочатку, наприклад, стає нульовим сигнал $U_{вихA_{p2}}$, то в цьому випадку одиничний сигнал залишиться тільки на виході нейрона X_{p1} , вказуючи, що вхідне зображення знаходиться на мінімальній відстані від Хеммінга еталонного зображення, що зберігається у вагах зв’язків нейрона Z_{p1} . Справді, у цьому випадку маємо:

$$U_{вихA_{p1}} \neq 0; \dots U_{вихY_p} = 0, p = 1, \dots, m, p \neq p_1;$$

$$U_{вх \sum 0} = \sum_{p=1}^m U_{вихY_p} W_{Y_p \sum 0} + U_{вихY_{p1}} W_{Y_{p1} \sum 0} = 1 \cdot -(1) = -1;$$

$$U_{вх \sum 0} = g(U_{вх \sum 0} = -1) = 0;$$

$$U_{вх \sum 1} = \sum_{p=1}^m U_{вихY_p} W_{Y_p \sum 1} + U_{вих \sum 0} W_{\sum 0 \sum 1} + W_{01}^4 \cdot 1 = 0;$$

$$U_{вих \sum 1} = g(U_{вх \sum 1} = 0) = 1;$$

$$U_{вх \sum 2} = \sum_{p=1}^m U_{вихY_p} W_{Y_p \sum 2} + U_{вих \sum 1} W_{\sum 1 \sum 2} + U_{вих \sum 0} W_{\sum 0 \sum 2} + W_{02}^4 \cdot 1 = -1;$$

$$U_{вих \sum 2} = g(U_{вх \sum 2} = -1) = 0;$$

$$U_{вх \sum 3} = \sum_{p=1}^m U_{вихY_p} W_{Y_p \sum 3} + U_{вих \sum 2} W_{\sum 2 \sum 3} + U_{вих \sum 1} W_{\sum 1 \sum 3} +$$

$$+ U_{вих \sum 0} W_{\sum 0 \sum 3} + W_{03}^4 \cdot 1 = -1;$$

$$U_{вих \sum 3} = g(U_{вх \sum 3} = -1) = 0;$$

$$U_{\text{вх}X_p}_{p \neq p_1} = \sum_{i=0}^3 U_{\text{вх}\sum i} W_{\sum iX_p} + U_{\text{вх}X_p} W_{X_pX_p} + U_{\text{вх}Y_{p_1}} W_{Y_{p_1}X_p} + W_{0p_1}^3 \cdot 1 = 2;$$

$$U_{\text{вх}X_p}_{p \neq p_1} = g(U_{\text{вх}X_p} = -1) = 0;$$

$$U_{\text{вх}X_{p_1}} = \sum_{i=0}^3 U_{\text{вх}\sum i} W_{\sum iX_{p_1}} + U_{\text{вх}X_{p_1}} W_{X_{p_1}X_{p_1}} + U_{\text{вх}Y_{p_1}} W_{Y_{p_1}X_{p_1}} + W_{0p_1}^3 \cdot 1 = 2;$$

$$U_{\text{вх}X_p}_{p \neq p_1} = g(U_{\text{вх}X_{p_1}} = 2) = 1.$$

де $W_{\Sigma_0\Sigma_1} = -2$; $W_{\Sigma_0\Sigma_2} = -3$; $W_{\Sigma_0\Sigma_3} = -4$; $W_{\Sigma_1\Sigma_2} = -2$; $W_{\Sigma_1\Sigma_3} = -3$.

Отже, в цьому випадку тільки на виході одного нейрона Х-шару буде одиничний вихідний сигнал, що вказує на те, що вхідне зображення знаходиться на мінімальній відстані Хеммінга від еталонного зображення, що зберігається у вагах нейрона зв'язків Z_{p_1} .

Таким чином, розроблена нова стабільно-пластична нейронна мережа, що використовує відстань Хеммінга при розпізнаванні чорно-білих зображень і здатна розпізнавати зображення, що знаходяться на мінімальній відстані від одного, двох або трьох еталонних зображень Хеммінга, що зберігаються у вагах зв'язків нейронної мережі. Розроблена нейронна мережа Хеммінга, здатна розпізнавати нову інформацію, донавчатися і визначати кілька рівноцінних рішень. На архітектуру та алгоритми функціонування нейронної мережі отримано патент України на винахід [143].

Результати, отримані по мережі Хеммінгу, можуть бути узагальнені інші нейронні мережі. Проілюструємо це з прикладу нейронної мережі Хебба [138, 142]. Для забезпечення стабільності в нейронних мережах АРТ при запам'ятовуванні нової інформації використовуються додаткові нейрони, введення яких дозволяє запам'ятовувати нову інформацію, і не руйнувати вже наявну. Покажемо, що цей ефект може бути досягнутий і в нейронній мережі Хебба при введенні додаткових нейронів, що розпізнають. Продемонструємо це на конкретному прикладі.

Нехай задано нейронну мережу Хебба, наведену на рис. 4.7. Потрібно запам'ятати зображення (S^1, S^2, S^3) за допомогою трьох нейронів Y_1, Y_2, Y_3 .

Для навчання нейронної мережі зображеннями S^1, S^2, S^3 необхідно виконати наступні кроки :

Крок 1. Задається множина $M = \{(S^1, t^1), (S^2, t^2), (S^3, t^3)\} = \{((1, -1, 1, 1, 1, 1, -1, -1, 1), (1, -1, -1)), ((1, 1, 1, 1, -1, 1, 1, -1, 1), (-1, 1, -1)), ((1, 1, 1, -1, 1, -1, -1, 1, -1), (-1, -1, 1))\}$. Задаються нульові вихідні сигнали всіх Y -нейронів і нульові значення ваги всіх зв'язків, задається початковий момент часу:

$$U_{\text{вих } Y_j} = 0, j = 1, \dots, 8;$$

$$W_{ij} = 0, i = 0, 1, \dots, 9, j = 1, \dots, 8.$$

$$t = t_0.$$

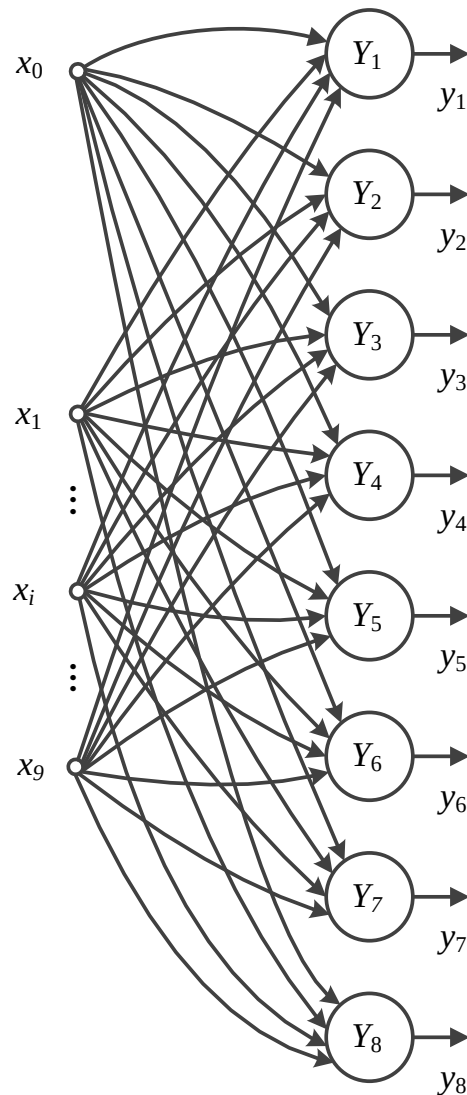


Рис. 4.7 . Нейронна мережа Хебба з додатковими нейронами, що запам'ятовують

Крок 2. Починається навчання нейронної мережі парою (S^1, t^1) .

Крок 3. Ініціюється множина входів нейронної мережі зображенням S^1 :

$$x_0 = 1, x_1 = 1, x_2 = -1, x_3 = 1, x_4 = 1, x_5 = 1, x_6 = 1, x_7 = -1, x_8 = -1, x_9 = 1.$$

Крок 4. Ініціюється множина вихідних нейронів мережі вектором необхідних вихідних сигналів t^1 пари (S^1, t^1) :

$$U_{\text{вых } Y_1} = y_1 = t_1^1 = 1;$$

$$U_{\text{вых } Y_2} = y_2 = t_2^1 = -1;$$

$$U_{\text{вых } Y_3} = y_3 = t_3^1 = -1.$$

Крок 5. Визначаються ваги зв'язків нейронів Y_1, Y_2, Y_3 мережі за правилом Хебба:

$$W_{01}(t_1) = W_{01}(t_0) + x_0 y_1 = 0 + 1 \cdot 1 = 1;$$

$$W_{11}(t_1) = W_{11}(t_0) + x_1 y_1 = 0 + 1 \cdot 1 = 1;$$

$$W_{11}(t_1) = W_{31}(t_1) = W_{41}(t_1) = W_{51}(t_1) = W_{61}(t_1) = W_{91}(t_1) = 1;$$

$$W_{21}(t_1) = W_{21}(t_0) + x_2 y_1 = 0 + (-1) \cdot 1 = -1;$$

$$W_{21}(t_1) = W_{71}(t_1) = W_{81}(t_1) = -1;$$

$$W_{02}(t_1) = W_{02}(t_0) + x_0 y_2 = 0 + 1 \cdot (-1) = -1;$$

$$W_{12}(t_1) = W_{12}(t_0) + x_1 y_2 = 0 + 1 \cdot (-1) = -1;$$

$$W_{12}(t_1) = W_{32}(t_1) = W_{42}(t_1) = W_{52}(t_1) = W_{62}(t_1) = W_{92}(t_1) = -1;$$

$$W_{22}(t_1) = W_{22}(t_0) + x_2 y_2 = 0 + (-1) \cdot (-1) = 1;$$

$$W_{22}(t_1) = W_{72}(t_1) = W_{82}(t_1) = 1;$$

$$W_{03}(t_1) = W_{02}(t_1) = -1;$$

$$W_{13}(t_1) = W_{33}(t_1) = W_{43}(t_1) = W_{53}(t_1) = W_{63}(t_1) = W_{93}(t_1) = W_{12}(t_1) = -1;$$

$$W_{23}(t_1) = W_{73}(t_1) = W_{83}(t_1) = W_{22}(t_1) = 1.$$

Потім повинні виконуватися кроки алгоритму, пов'язані з пред'явленням зображень S^2 та S^3 . У табл. 4.1 наведено результати цих розрахунків.

У табл. 4.2 представлені результати пред'явлення навченої нейронної мережі зображень $S^1, \dots, S^9$. Результати отримані для випадку, коли Y – нейрони мають наступну функцію активації:

$$U_{\text{вих } Y_j} = \begin{cases} 1, & \text{якщо } U_{\text{вх } Y_j} \geq 0, \\ -1, & \text{якщо } U_{\text{вх } Y_j} < 0, \end{cases}$$

де $U_{\text{вих } Y_j}$ і $U_{\text{вх } Y_j}$ – відповідно вихідні та вхідні сигнали нейронів Y_j , $j = 1, 2, 3$.

Таблиця 4.1

Результати розрахунків ваги зв'язків мережі Хебба після пред'явлення зображень S^1 , S^2 , S^3 .

Ваги зв'язків	Початковий момент часу t_0	Момент часу t_1 (після пред'явлення зображення S^1)	Момент часу t_2 (після пред'явлення зображення S^2)	Момент часу t_3 (після пред'явлення зображення S^3)
W_{01}	0	1	0	-1
W_{11}	0	1	0	-1
W_{21}	0	-1	-2	-3
W_{31}	0	1	0	-1
W_{41}	0	1	0	1
W_{51}	0	1	2	1
W_{61}	0	1	0	1
W_{71}	0	-1	-2	-1
W_{81}	0	-1	0	-1
W_{91}	0	1	0	1
W_{02}	0	-1	0	-1
W_{12}	0	-1	0	-1
W_{22}	0	1	2	1
W_{32}	0	-1	0	-1
W_{42}	0	-1	0	1
W_{52}	0	-1	-2	-3
W_{62}	0	-1	0	1
W_{72}	0	1	2	3
W_{82}	0	1	0	-1
W_{92}	0	-1	0	-1

Ваги зв'язків	Початковий момент часу t_0	Момент часу t_1 (після пред'явлення зображення S^1)	Момент часу t_2 (після пред'явлення зображення S^2)	Момент часу t_3 (після пред'явлення зображення S^3)
W_{03}	0	-1	-2	-1
W_{13}	0	-1	-2	-1
W_{23}	0	1	0	1
W_{33}	0	-1	-2	-1
W_{43}	0	-1	-2	-3
W_{53}	0	-1	0	1
W_{63}	0	-1	-2	-3
W_{73}	0	1	0	-1
W_{83}	0	1	2	3
W_{93}	0	-1	-2	-3

З аналізу табл. 4.1 випливає, що вхідні зображення $S^1, S^2, S^3, S^4, S^8, S^9$ викликають реакцію мережі, у якій при пред'явленні будь-якого із зображень на виході нейронної мережі спостерігається один позитивний одиничний сигнал і два негативні одиничні сигнали, тобто мережа відносить вхідне зображення до одного з відомих класів. У табл. 4.2 наведені результати розпізнавання зображень $S^1, \dots, S^9$

Таблиця 4.2

Результати розпізнавання зображень $S^1, \dots, S^9$

Нейрони	Вихідні сигнали нейронів при пред'явленні зображень								
	S^1	S^2	S^3	S^4	S^5	S^6	S^7	S^8	S^9
Y_1	1	-1	-1	-1	1	1	1	1	-1
Y_2	-1	1	-1	1	-1	1	-1	-1	-1
Y_3	-1	-1	1	-1	1	1	1	-1	1
Результат розпізнавання	+	+	+	+	-	-	-	+	+

Аналіз даних табл. 4.2 та зображень показує, що відбулося правильне розпізнавання всіх шести зображень, незважаючи на те, що три з них мають дефекти (S^4, S^8, S^9).

Неважко побачити, що при віднесенні вхідного зображення до одного з трьох класів, представники яких зберігаються у вагах зв'язків нейронів Y_1, Y_3 сумарний Y_2 вихідний сигнал цих нейронів дорівнює мінус одиниці:

$$\sum_{j=1}^3 U_{\text{вих}Y_j} = -1.$$

Якщо вхідне зображення не належить до класів зображень що зберігаються у вагах зв'язків нейронів Y_1, Y_2, Y_3 , то маємо $\sum_{j=1}^3 U_{\text{вих}Y_j} \neq -1$, що

може бути ознакою нової інформації (зображень) на вхідному шарі нейронів і необхідності навчання наступної групи Y -нейронів розпізнавати цю вхідну інформацію. При цьому навчені нейрони, що розпізнають, повинні бути заблоковані в режимі розпізнавання і заблоковані або ігноруватися в режимі навчання.

Нейрони Y_4, Y_5, Y_6 нескладно навчити розпізнаванню зображень S^5, S^7, S^6 алгоритмом Хебба. Результат навчання наведено у табл. 4.3. При цьому множина M_1 з повчальних пар задавали наступним чином:

$$M_1 = \{(S^5, t^5), (S^6, t^6), (S^7, t^7)\} = \{((-1, -1, 1, -1, 1, -1, 1, -1, -1), (1, -1, -1)), ((-1, -1, -1, -1, -1, -1, 1, 1, 1), (-1, 1, -1)), ((1, -1, -1, -1, 1, -1, -1, 1, 1), (-1, -1, 1))\}.$$

У табл. 4.4 наведено результати розпізнавання зображень S^5, S^6, S^7, S^{10} та S^{11} .

Таблиця 4.3

Результати розрахунків ваг зв'язків нейронів Y_4, Y_5, Y_6 після пред'явлення зображень S^5, S^6, S^7

Ваги зв'язків	Початковий момент часу t_0	Момент часу t_1 (після пред'явлення зображення S^5)	Момент часу t_2 (після пред'явлення зображення S^6)	Момент часу t_3 (після пред'явлення зображення S^7)
W_{04}	0	1	0	-1
W_{14}	0	-1	0	-1

Ваги зв'язків	Початковий момент часу t_0	Момент часу t_1 (після пред'явлення зображення S^5)	Момент часу t_2 (після пред'явлення зображення S^6)	Момент часу t_3 (після пред'явлення зображення S^7)
W_{24}	0	-1	0	1
W_{34}	0	1	2	3
W_{44}	0	-1	0	1
W_{54}	0	1	2	1
W_{64}	0	-1	0	1
W_{74}	0	1	0	1
W_{84}	0	-1	-2	-3
W_{94}	0	-1	-2	-3
W_{05}	0	-1	0	-1
W_{15}	0	1	0	-1
W_{25}	0	1	0	1
W_{35}	0	-1	-2	-1
W_{45}	0	1	0	1
W_{55}	0	-1	-2	-3
W_{65}	0	1	0	1
W_{75}	0	-1	0	1
W_{85}	0	1	2	1
W_{95}	0	1	2	1
W_{06}	0	-1	-2	-1
W_{16}	0	1	2	3
W_{26}	0	1	2	1
W_{36}	0	-1	0	-1
W_{46}	0	1	2	1
W_{56}	0	-1	0	1
W_{66}	0	1	2	1
W_{76}	0	-1	-2	-3
W_{86}	0	1	0	1

Ваги зв'язків	Початковий момент часу t_0	Момент часу t_1 (після пред'явлення зображення S^5)	Момент часу t_2 (після пред'явлення зображення S^6)	Момент часу t_3 (після пред'явлення зображення S^7)
W_{96}	0	1	0	1

З аналізу табл. 4.4 слід, що нейрони Y_4, Y_5, Y_6 відносять зображення S^5, S^6, S^7 до відомих класів, зразки яких зберігаються у вагах зв'язків цих нейронів. Зображення S^{10} і S^{11} нейронами Y_4, Y_5, Y_6 розпізнаються як такі, що не належать до цих класів, це ж спостерігається і при пред'явленні зображень S^{10}, S^{11} і першій групі нейронів Y_1, Y_2, Y_3 . Таким чином, для розпізнавання зображень S^{10}, S^{11} необхідно навчити ще два Y -нейрони: Y_7, Y_8 .

Нейрони Y_7, Y_8 будуть розпізнавати вказані зображення після того, як при спробі їх розпізнавання будуть заблоковані спочатку нейрони Y_1, Y_2, Y_3 , а потім нейрони Y_4, Y_5, Y_6 . Результати навчання наведено у табл. 4.5. При цьому множина M_2 з повчальних пар (вхідне зображення – необхідний вихідний вектор) ставилося таким чином:

$$M_2 = \{(S^{10}, t^{10}), (S^{11}, t^{11})\} = \{((1, -1, -1, -1, -1, 1, 1, -1, -1), (1, -1)), ((-1, 1, 1, 1, -1, -1, -1, 1, -1), (-1, 1))\}.$$

Таблиця 4.4

Результати розпізнавання зображень S^5, S^6, S^7, S^{10} та S^{11} .

Нейрони	Вихідні сигнали нейронів при пред'явленні зображень				
	S^5	S^6	S^7	S^{10}	S^{11}
Y_4	1	-1	-1	1	1
Y_5	-1	1	-1	1	1
Y_6	-1	-1	1	-1	-1
Результат розпізнавання	+	+	+	-	-

Неважко перевірити, що після пред'явлення зображення S^{10} на виходах нейронів Y_7, Y_8 буде вектор сигналів $(1, -1)$, а після пред'явлення зображення S^{11} – вектор $(-1, 1)$.

Узагальним результати прикладу на випадок, коли спочатку нейронна мережа Хебба навчається розпізнаванню множини з n_0 ($n_0 \geq 3$) зображень $M_0 = \{S^1, \dots, S^{n_0}\}$, кожне з яких кодується на виходах Y -нейронів ($Y_1^0, \dots, Y_{n_0}^0$) одним поодиноким сигналом і $(n_0 - 1)$ сигналами «-1». Сумарний вихідний сигнал нейронів $Y_1^0, \dots, Y_{n_0}^0$, що правильно розпізнають одне з зображень, що відносяться до множини M_0 , в цьому випадку дорівнює:

$$\sum_{i=1}^{n_0} U_{\text{вых } Y_i^0} = -(n_0 - 2). \quad (4.10)$$

Таблиця 4.5

Результати розрахунків ваги зв'язків нейронів Y_7, Y_8 після пред'явлення зображень S^{10}, S^{11} .

Ваги зв'язків	Початковий момент часу t_0	Момент часу t_1 (після пред'явлення зображення S^{10})	Момент часу t_2 (після пред'явлення зображення S^{11})
W_{07}	0	1	0
W_{17}	0	1	2
W_{27}	0	-1	-2
W_{37}	0	-1	-2
W_{47}	0	-1	-2
W_{57}	0	-1	0
W_{67}	0	1	2
W_{77}	0	1	2
W_{87}	0	-1	-2
W_{97}	0	-1	0
W_{08}	0	-1	0
W_{18}	0	-1	-2
W_{28}	0	1	2
W_{38}	0	1	2

W_{48}	0	1	2
W_{58}	0	1	0
W_{68}	0	-1	-2
W_{78}	0	-1	-2
W_{88}	0	1	2
W_{98}	0	1	0

Якщо при пред'явленні нейронної мережі зображення S^* співвідношення (4.10) не виконується, це ознакою появи на вході нейронної мережі нової інформації (представника нового класу зображень). При накопиченні деякої множини таких зображень $M_1 = \{S^{n_0+1}, S^{n_0+2}, \dots, S^{n_0+n_1}\}$, де $n_1 \geq 3$, можуть бути навчені за допомогою алгоритму Хебба наступні n_1 нейрони мережі. Ознаком того, що деяке вхідне зображення S^* відноситься до багатьох M_1 є співвідношення:

$$\sum_{i=1}^{n_0} U_{\text{вх} Y_i^0}(S^*) > -(n_0 - 2); \quad \sum_{i=1}^{n_1} U_{\text{вх} Y_i^1}(S^*) = -(n_1 - 2). \quad (4.11)$$

Поява зображень, для яких не виконуються співвідношення (4.10) і (4.11) вказує на необхідність наступного навчання нейронної мережі. Число N кроків донавчання практично не обмежене. Однак при великому N і апаратній реалізації нейронної мережі мережа Хебба з донавчанням буде програвати швидкодії мережі Хебба, навченої на всій множини зображень, що розпізнаються. В останньому випадку розпізнавання вхідного зображення вимагає однієї спроби (визначаються вхідні та вихідні сигнали нейронів вхідного шару та шару нейронів, що розпізнають). У разі нейронної мережі, яка донавчається N разів, вдала спроба розпізнавання в гіршому випадку може бути здійснена тільки з $(N + 1)$ -го разу.

На рис. 4.8 наведено архітектуру нейронної мережі Хебба, яка може донавчатися N разів.

Мережа складається з шару вхідних нейронів $x_1, \dots, x_n$ і Y -шару нейронів, що розпізнають [138, 142]. Нейрони Y -шару розбиті на $(N + 1)$ групу, кожна з яких може містити різне число нейронів (але не менше трьох) і формуватися у процесі функціонування мережі.

Перша група нейронів $Y_1^0, \dots, Y_{n_0}^0$ використовується для запам'ятовування вихідної інформації у вигляді множини зображень M_0 . Друга та наступні групи нейронів $(Y_1^1, \dots, Y_{n_1}^1), \dots, (Y_1^N, \dots, Y_{n_N}^N)$ використовуються для навчання нейронної мережі в міру накопичення нової інформації та послідовного запам'ятовування множин зображень $M_1, M_2, \dots, M_N$.

У кожній групі нейронів вихідні сигнали Y -нейронів надходять на входи керуючого нейрона, що має функцію активації виду:

$$U_{\text{вих } \Sigma_d} = \begin{cases} 0, & \text{якщо } U_{\text{вх } \Sigma_d} = \sum_{k=1}^{n_d} U_{\text{вих } Y_k^d} = -(n_d - 2), \\ 1, & \text{якщо } U_{\text{вх } \Sigma_d} \neq -(n_d - 2), \end{cases} \quad d = 0, 1, \dots, N, \quad (4.12)$$

де $U_{\text{вих } \Sigma_d}$, $U_{\text{вх } \Sigma_d}$ – відповідно вихідний та вхідний сигнал нейрона Σ_d ($d = 0, 1, \dots, N$); $U_{\text{вих } Y_k^d}$ – вихідний сигнал нейрона Y_k^d ($d = 0, 1, \dots, N; k = 1, \dots, n_d$); n_d – кількість нейронів у групі $Y_1^d, \dots, Y_{n_d}^d$.

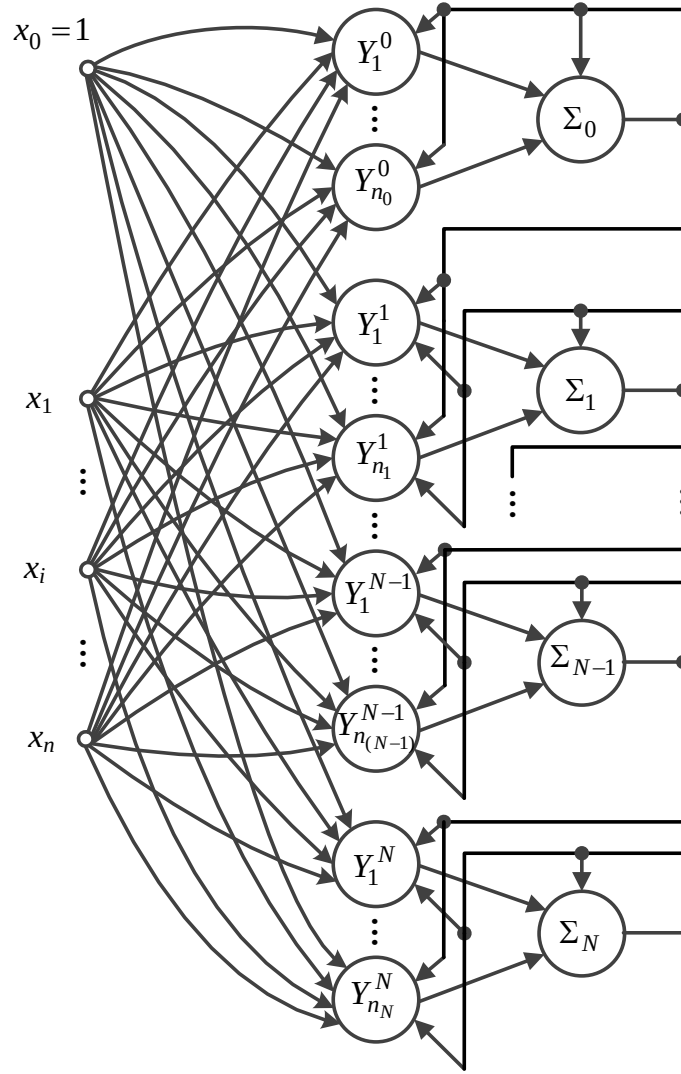


Рис. 4.8. Архітектура мережі Хебба, яка може донавчатися N разів

На початку режиму розпізнавання обнулюються вихідні сигнали Σ нейронів і блокується робота нейронів $Y_1^1, Y_2^1, \dots, Y_{n_N}^N$.

При подачі на вхід нейронної мережі, яка донавчалася L разів ($1 < L < N$), деякого зображення S^* спочатку активуються нейрони першої групи $Y_1^0, \dots, Y_{n_0}^0$, вихідні сигнали яких надходять на входи нейрона, що управляє Σ_0 . Якщо виконується співвідношення:

$$U_{\text{вих } \Sigma_0} = \sum_{k=1}^{n_0} U_{\text{вих } Y_k^0} = -(n_0 - 2), \quad (4.13)$$

де $U_{\text{вих } \Sigma_0} = 0$ й вхідне зображення S^* відноситься до множини зображень M_0 , а конкретний клас зображень визначають вихідні сигнали нейронів $Y_1^0, \dots, Y_{n_0}^0$.

Якщо співвідношення (4.12) не виконується, то $U_{\text{вих } \Sigma_0} = 1$ що вказує на те, що вхідне зображення S^* не належить множини M_0 . Одиничний вихідний сигнал нейрона Σ_0 по ланцюгу зворотний зв'язок фіксує одиничний вихідний сигнал нейрона Σ_0 і надходить на входи нейронів першої групи, блокуючи їх. Одночасно цей одиничний сигнал управляючого нейрона надходить на входи нейронів $Y_1^1, \dots, Y_{n_1}^1$ другої групи, що розпізнають, і переводить їх в активний стан. Вихідні сигнали нейронів $Y_1^1, \dots, Y_{n_1}^1$ надходять на входи управляючого нейрона Σ_1 , за допомогою якого визначається належність зображення S^* до множини M_1 . Якщо виконується співвідношення:

$$U_{\text{вих } \Sigma_1} = \sum_{k=1}^{n_1} U_{\text{вих } Y_k^1} = -(n_1 - 2), \quad (4.14)$$

то зображення S^* належить множині M_1 , а конкретний клас зображень визначають вихідні сигнали нейронів $Y_1^1, \dots, Y_{n_1}^1$. Якщо рівність (4.14) не виконується, то зображення S^* не належить до множини M_1 і $U_{\text{вих } \Sigma_1} = 1$. Сигнал $U_{\text{вих } \Sigma_1}$ блокує нейрони $Y_1^1, \dots, Y_{n_1}^1$ та підключає до розпізнавання нейрони третьої групи і т.д. В результаті цього процесу вхідне зображення або буде віднесено до одного з відомих множин зображень $M_0, M_1, M_2, \dots, M_L$, або буде сприйнято як нове зображення, яке необхідно запам'ятати на $(L + 1)$ нейроні нейронної мережі.

Таким чином, розроблені стабільно-пластичні нейронні мережі Хебба, які, на відміну від класичних аналогів, здатні розпізнавати нову інформацію і донавчатися в процесі свого функціонування.

Розроблений підхід для навчання нейронної мережі Хебба може бути узагальнений і на інші нейронні мережі, зокрема, на перцептрони з нейронами, що мають безперервні функції активації, наприклад, біполярні, сигмоїдальні функції активації:

$$U_{\text{вих}} = 2 / (1 + e^{-\tau U_{\text{вих}}}) - 1,$$

де τ – константа.

При таких функціях активації отримати на виходах нейронів шару, що розпізнає, вихідні сигнали, точно рівні «1» або «-1», неможливо. Отже, утруднено і безпосереднє використання співвідношень виду (4.10) і (4.11), якщо перцептрон з n_0 вихідними нейронами використовувати як і мережу Хебба для запам'ятовування лише n_0 різних зображень, задаючи кожне з них одним сигналом, близьким до одиниці, тільки на виході одного нейрона, а інші вихідні сигнали перцептрону задавати сигналами, близькими до «-1». Однак такі безперервні сигнали можна округлити до цілих значень і використовувати надалі біполярні сигнали.

Архітектуру мережі умовно можна розбити на $(N+1)$ однотипних блоків (рис. 4.9), кожен з яких зберігає у вагах своїх зв'язків множина зображень $M_l = \{S^{l1}, S^{l2}, \dots, S^{ln_l}\}$, $l = 0, 1, \dots, N$.

Будь-який l -й ($l = 0, 1, \dots, N$) блок містить k_l A -нейронів прихованого шару: $A_1^l, A_2^l, \dots, A_{k_l}^l$, n_l Y -нейронів розпізнає або вихідного шару: $Y_1^l, Y_2^l, \dots, Y_{n_l}^l$, і стільки ж D -нейронів ($D_1^l, D_2^l, \dots, D_{n_l}^l$).

D -нейрони мають функцію активації виду:

$$U_{\text{вих } D} = \begin{cases} 1, & \text{якщо } (1 - \delta) \leq U_{\text{вх } D} < 1, \\ 0, & \text{якщо } (-1 + \delta) < U_{\text{вх } D} < 1 - \delta, \\ -1, & \text{якщо } -1 < U_{\text{вх } D} \leq -1 + \delta, \end{cases} \quad (4.15)$$

де $U_{\text{вих } D}$ – $U_{\text{вх } D}$ відповідно вихідний і вхідний сигнал D -нейрона; δ – максимально припустима помилка наближення сигналів «1» та «-1» за допомогою нейронів з біполярною функцією активації сигмоїдальної.

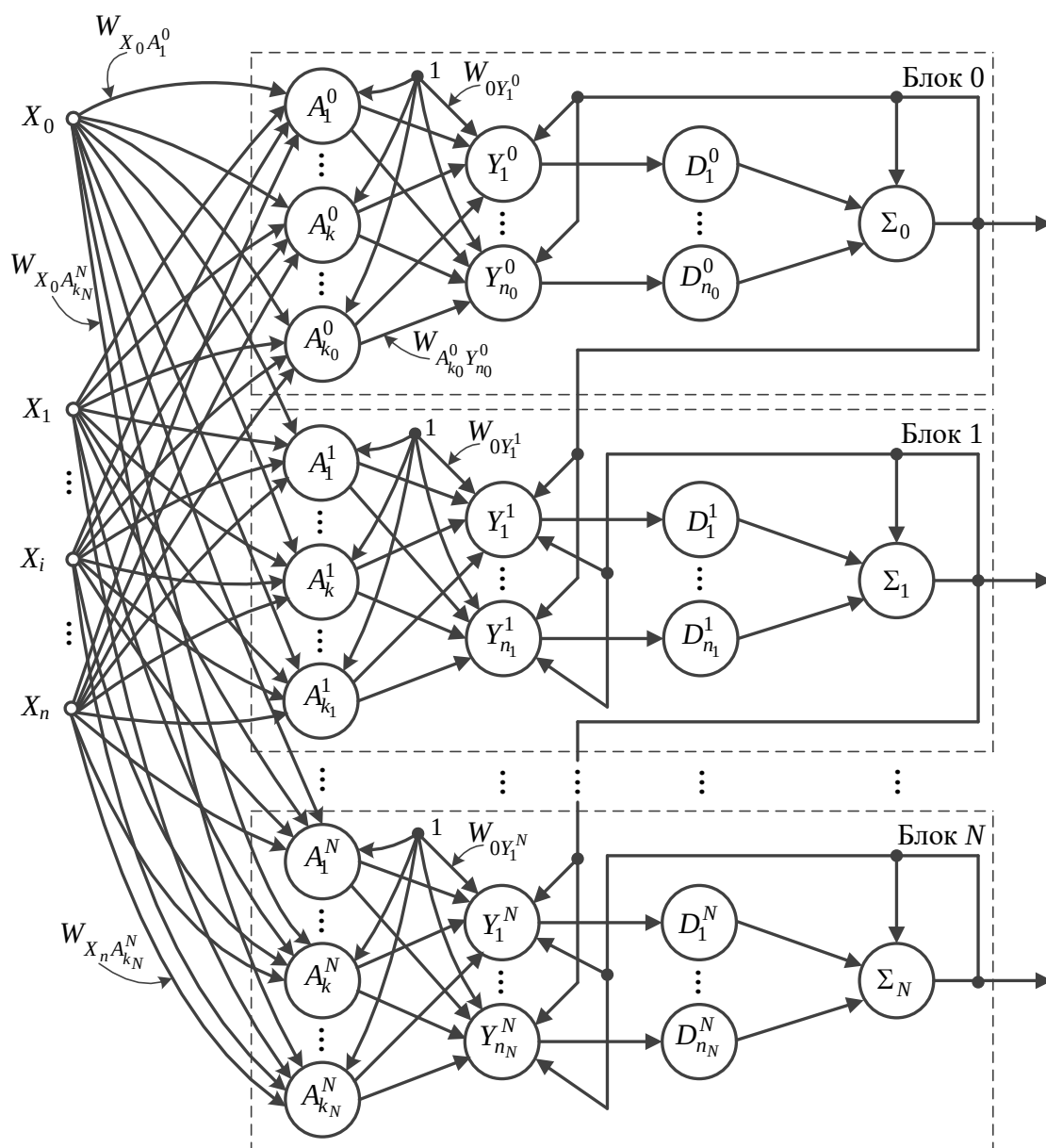


Рис. 4.9. Архітектура тришарового перцептрону, який може довчатися N разів

Кожен блок нейронної мережі містить також керуючий Σ -нейрон, що виконує такі ж функції, що і керуючі нейрони в мережі Хебба, здатної донавчати. Входи A -нейронів всіх $(N+1)$ блоку мережі з'єднані з виходами сенсорних нейронів $X_1, X_2, \dots, X_n$.

Нейрони $A_1^0, \dots, A_{k_0}^0, Y_1^0, \dots, Y_{n_0}^0$ нульового блоку використовуються для запам'ятовування вихідної інформації у вигляді множини зображень M_0 . Блок 1 та наступні блоки нейронної мережі використовуються для навчання перцептрону в міру накопичення нової інформації та послідовного запам'ятовування множин зображень $M_1, M_2, \dots, M_N$. У кожному блоці вихідні сигнали Y -нейронів надходять на входи D -нейронів, що мають

функцію активації виду (4.15) і перетворюють безперервні сигнали Y -нейронів на дискретні сигнали: 1, 0 і -1 . У кожному блоці нейронів сигнали D -нейронів надходять на входи керуючого нейрона, що має функцію активації виду:

$$U_{\text{вих } \Sigma_d} = \begin{cases} 0, & \text{якщо } U_{\text{вх } \Sigma_d} = \sum_{k=1}^{n_d} U_{\text{вих } D_k^d} = -(n_d - 2), \\ 1, & \text{якщо } U_{\text{вх } \Sigma_d} \neq -(n_d - 2), \quad d = 0, 1, \dots, N, \end{cases} \quad (4.16)$$

де $U_{\text{вих } \Sigma_d}$ – $U_{\text{вх } \Sigma_d}$ відповідно вихідний і вхідний сигнал Σ_d нейрона; $d = 0, 1, \dots, N$ $U_{\text{вих } D_k^d}$ – вихідний сигнал нейрона D_k^d ($d = 0, 1, \dots, N$; $k = 1, \dots, n_d$); n_d – кількість Y та D нейронів у блоці d ($d = 0, 1, \dots, N$).

Якщо $U_{\text{вих } \Sigma_d} = 0$, це ознакою, що вхідне зображення належить множини M_d , яке конкретний клас визначається комбінацією вихідних сигналів D -нейронів. Якщо $U_{\text{вих } \Sigma_d} = 1$, це означає, що вхідне зображення не належить множини M_d . У цьому випадку вихідний сигнал $U_{\text{вих } \Sigma_d}$ ланцюга зворотного зв'язку фіксує одиничний вихідний сигнал нейрона Σ_d , блокує нейрони $Y_1^d, \dots, Y_{n_d}^d$ і підключає до розпізнавання нейрони групи $(d + 1)$.

Розглянемо укрупнені алгоритми навчання перцептронів, здатного донавчатись :

Крок 1. Задаються:

- множина M_0 з n_0 навчальних пар (вхідне зображення - заданий вихідний вектор мережі);
- максимальна кількість N можливих донавчень нейронної мережі;
- початкові ваги зв'язків нейронної мережі;
- нульові вихідні сигнали нейронів блоку 0 нейронної мережі;
- початкове значення параметра l , за допомогою якого підраховується число донавчання мережі, $l = 0$;
- початкове значення параметра r за допомогою якого підраховується число нерозпізнаних вхідних зображень;

Блокується робота Y -нейронів всіх блоків мережі, крім нульового.

Крок 2. Одним з алгоритмів методу зворотного поширення помилки блок 0 навчається розпізнаванню усіх зображень з множини M_0 .

Крок 3. Нейронна мережа переводиться в режим розпізнавання або класифікації вхідної інформації, задається початкове значення параметра $r = 0$. Формується множина $M_{l+1} = \{S_1^{(l+1)}, S_2^{(l+1)}, \dots, S_{n(l+1)}^{(l+1)}\}$ вхідних зображень, інформація про які немає в пам'яті нейронної мережі та є представниками нових класів зображень. При записі до множини M_{l+1} нового зображення $S_k^{(l+1)}$ параметр r збільшується на одиницю і перевіряється умова необхідності донавчання нейронної мережі (наприклад, за величиною параметра r і числом донавчень нейронної мережі). Якщо умова не виконується, мережа продовжує функціонувати в заданому режимі, інакше – перехід на наступний крок алгоритму.

Крок 4. Одним із алгоритмів методу зворотного розповсюдження помилки блок $(l + 1)$ навчається розпізнаванню всіх зображень з множини M_{l+1} . Число l збільшується на одиницю: $l = l + 1$. Перевіряється умова закінчення роботи алгоритму, якщо вона виконується, то перехід крок 3 алгоритму, інакше – перехід останній крок алгоритму.

Крок 5. Зупинка.

Можлива архітектура мережі та алгоритм навчання, коли число груп нейронів та число нейронів у кожній групі не задається заздалегідь, а формується у процесі навчання.

Розглянемо укрупнений алгоритм функціонування перцептрону, здатного донавчати, в режимі розпізнавання:

Крок 1. Ініціюються ваги зв'язків та обнулюються вихідні сигнали всіх нейронів нейронної мережі. Задається число L ($1 < L < N$) донавчання нейронної мережі. Задається число l ($l = 0$), з допомогою якого підраховується число блоків, які можна використовувати для розпізнавання вхідного зображення. Блокується робота Y -нейронів всіх блоків, крім нульового.

Крок 2. На вхід мережі подається деяке зображення $S^* = (S_1^*, S_2^*, \dots, S_n^*)$.

Крок 3. Визначаються вхідні та вихідні сигнали нейронів X -шару:

$$U_{\text{вх}X_i} = S_i^*, \quad U_{\text{вих}X_i} = U_{\text{вх}X_i}, \quad i = 1, \dots, n.$$

Крок 4. Визначаються вхідні та вихідні сигнали нейронів прихованого шару нульового блоку:

$$U_{\text{вх}A_k^0} = 1 \cdot W_{X_0A_k^0} + \sum_{i=1}^n U_{\text{вих}X_i} W_{X_iA_k^0}, \quad k = 1, \dots, k_0;$$

$$U_{\text{вих}A_k^0} = f_{A_k^0}(U_{\text{вх}A_k^0}), \quad k = 1, \dots, k_0,$$

де $U_{\text{вх } A_k^0}$, $U_{\text{вих } A_k^0}$, $k=1, \dots, k_0$ - відповідно вхідні та вихідні сигнали нейронів прихованого A^0 -шару;

$W_{X_0 A_k^0}$, $k=1, \dots, k_0$ - ваги зв'язків для сигналу зміщення на нейрони $A_1^0, \dots, A_{k_0}^0$;

$W_{X_i A_k^0}$, $i=1, \dots, n$; $k=1, \dots, k_0$ - ваги зв'язків від нейронів вхідного шару до нейронів прихованого шару;

$f_{A_k^0}$ - функція активації нейронів A^0 -шару.

Крок 5. Визначаються вхідні та вихідні сигнали нейронів, що розпізнають, нульового блоку:

$$U_{\text{вх } Y_p^0} = 1 \cdot W_{0Y_p^0} + \sum_{k=1}^{k_0} U_{\text{вих } A_k^0} W_{A_k^0 Y_p^0}, \quad p=1, \dots, n_0;$$

$$U_{\text{вих } Y_p^0} = f_{Y_p^0}(U_{\text{вх } Y_p^0}), \quad p=1, \dots, n_0,$$

де $U_{\text{вх } Y_p^0}$, $U_{\text{вих } Y_p^0}$, $p=1, \dots, n_0$ - відповідно вхідні та вихідні сигнали нейронів Y -шару;

$W_{0Y_p^0}$, $p=1, \dots, n_0$ - ваги зв'язків для сигналу зміщення на нейрони $Y_1^0, \dots, Y_{n_0}^0$;

$W_{A_k^0 Y_p^0}$, $k=1, \dots, k_0$, $p=1, \dots, n_0$ - ваги зв'язків від елементів A -шару до нейронів Y -шару;

$f_{Y_p^0}$ - функція активації нейронів Y -шару.

Крок 6. Визначаються вхідні та вихідні сигнали D -нейронів нульового блоку:

$$U_{\text{вх } D_p^0} = U_{\text{вих } Y_p^0}, \quad p=1, \dots, n_0;$$

$$U_{\text{вих } D_p^0} = \begin{cases} 1, & \text{якщо } (1-\delta) \leq U_{\text{вх } D_p^0} < 1, \\ 0, & \text{якщо } (-1+\delta) < U_{\text{вх } D_p^0} < 1-\delta, \\ -1, & \text{якщо } -1 < U_{\text{вх } D_p^0} \leq -1+\delta, \end{cases}$$

нейронів D -шару нульового блоку;

δ – максимально припустима помилка наближення сигналів «1» та «-1» за допомогою нейронів з біполярною функцією активації.

Крок 7. Визначаються вхідні та вихідні сигнали управляючого нейрона Σ_0

$$U_{\text{вих } \Sigma_0} = \begin{cases} 0, & \text{якщо } U_{\text{вх } \Sigma_0} = \sum_{p=1}^{n_0} U_{\text{вих } D_p^0} = -(n-2), \\ 1, & \text{якщо } U_{\text{вх } \Sigma_0} = \sum_{p=1}^{n_0} U_{\text{вих } D_p^0} \neq -(n-2). \end{cases}$$

Якщо $U_{\text{вих } \Sigma_0} = 0$ за допомогою вихідних сигналів D^0 -нейронів визначається клас, до якого відноситься вхідне зображення. Потім здійснюється перехід крок 1 алгоритму. Якщо $U_{\text{вих } \Sigma_0} = 1$, то вхідне зображення не належить множині M_0 . У цьому випадку ланцюгом зворотного зв'язку фіксується одиничний вихідний сигнал нейрона Σ_0 . Цей сигнал блокує нейрони $Y_1^0, \dots, Y_{n_0}^0$ та підключає до розпізнавання нейрони першої групи.

Крок 8. Число l збільшується на одиницю: $l = l + 1$. Визначаються вхідні та вихідні сигнали нейронів шарів A , Y , D блоку l :

$$\begin{aligned} U_{\text{вх } A_k^l} &= 1 \cdot W_{X_0 A_k^l} + \sum_{i=1}^{n_l} U_{\text{вих } X_i} W_{X_i A_k^l}, \quad k = 1, \dots, k_l; \\ U_{\text{вих } A_k^l} &= f_{A_k^l}(U_{\text{вх } A_k^l}), \quad k = 1, \dots, k_l; \\ U_{\text{вх } Y_p^l} &= 1 \cdot W_{0 Y_p^l} + \sum_{k=1}^{k_l} U_{\text{вих } A_k^l} W_{A_k^l Y_p^l}, \quad p = 1, \dots, n_l; \\ U_{\text{вих } Y_p^l} &= f_{Y_p^l}(U_{\text{вх } Y_p^l}), \quad p = 1, \dots, n_l; \\ U_{\text{вх } D_p^l} &= U_{\text{вих } Y_p^l}, \quad p = 1, \dots, n_l; \\ U_{\text{вих } D_p^l} &= \begin{cases} 1, & \text{якщо } (1-\delta) \leq U_{\text{вх } D_p^l} < 1, \\ 0, & \text{якщо } (-1+\delta) < U_{\text{вх } D_p^l} < 1-\delta, \\ -1, & \text{якщо } -1 < U_{\text{вх } D_p^l} \leq -1+\delta, \end{cases} \end{aligned}$$

де $U_{\text{вх } A_k^l}, U_{\text{вих } A_k^l} (k=1, \dots, k_l), U_{\text{вх } Y_p^l}, U_{\text{вих } Y_p^l}, U_{\text{вх } D_p^l}, U_{\text{вих } D_p^l} (p=1, \dots, n_l)$ – відповідно вхідні та вихідні сигнали нейронів A^l -шару, Y^l -шару та D^l -шару блоку l нейронної мережі;

$W_{X_0 A_k^l} (k=1, \dots, k_l), W_{0 Y_p^l} (p=1, \dots, n_l)$ – ваги зв'язків для сигналів зміщення відповідно на нейрони A^l та Y^l шарів;

$W_{X_i A_k^l}, W_{A_k^l Y_p^l} (i=1, \dots, n; k=1, \dots, k_l; p=1, \dots, n_l)$ – відповідно ваги зв'язків від нейронів вхідного шару до нейронів прихованого A^l -шару і від нейронів A^l -шару до нейронів Y^l -шару.

Крок 9. Визначаються вхідний $U_{\text{вх } \Sigma_l}$ і вихідний $U_{\text{вих } \Sigma_l}$ сигнали управляючого нейрона Σ_l :

$$U_{\text{вх } \Sigma_l} = \sum_{p=1}^{n_l} U_{\text{вих } D_p^l}; \quad U_{\text{вих } \Sigma_l} = \begin{cases} 0, & \text{якщо } U_{\text{вх } \Sigma_l} = -(n_l - 2), \\ 1, & \text{якщо } U_{\text{вх } \Sigma_l} \neq -(n_l - 2). \end{cases}$$

Якщо $U_{\text{вих } \Sigma_l} = 0$ за допомогою вихідних сигналів D^l -нейронів визначається клас, до якого відноситься вхідне зображення. Потім здійснюється перехід крок 1 алгоритму.

Якщо $U_{\text{вих } \Sigma_l} = 1$ і $l = L$, то – перехід на крок 1 алгоритму, оскільки вхідне зображення не належить множині M_l і в пам'яті мережі відсутній клас зображень, до якого може належати вхідне зображення. Воно сприймається як представник нового класу зображень, який необхідно запам'ятати на $(L+1)$ -му донавченні нейронної мережі в $(L+1)$ -му блоці.

Якщо $U_{\text{вих } \Sigma_l} = 1$ і $l < L$, то вхідне зображення не належить множині M_l , але може належати множині M_{l+1} . Сигнал з виходу нейрона Σ_l ланцюгом зворотного зв'язку фіксує свій одиничний вихідний сигнал, блокує роботу нейронів $Y_1^l, \dots, Y_{n_l}^l$ і підключає до розпізнавання нейрони групи $(l+1)$.

Крок 10. Перевіряються умови припинення роботи алгоритму. Якщо вони виконуються, то перехід крок 11 алгоритму, інакше – перехід крок 8 алгоритму.

Крок 11. Зупинка.

Таким чином, розроблено архітектуру та алгоритми функціонування тришарового перцептрону, здатного донавчатись у процесі свого функціонування. Отримані результати нескладно узагальнити і перцептрони,

що мають більше трьох шарів нейронів [144].

4.3. Багатоспрямовані баз знань побудовані на моделях асоціативної пам'яті, що дозволяють донавчатись та визначати кілька рішень

Проблема, характерна для класичної двонаправленої асоціативної пам'яті, яка не має можливості одночасного відновлення зі своєї пам'яті множини асоціативних один одному зображень, вирішується завдяки тому, що її архітектура перебудовується шляхом введення в неї додаткових $(N - 1)$ сенсорних шарів нейронів (рис. 4.10) які пов'язані з першим шаром сенсорних елементів парами двонаправлених зважених зв'язків з відповідними ваговими коефіцієнтами.

В результаті додавання в структуру нейронної мережі вищезгаданих сенсорних шарів нейронів досягається можливість зберігання та відновлення з пам'яті множинних асоціацій. Це стає можливим завдяки тому, що вхідний сенсорний шар нейронів пов'язаний з N шарами елементів, що дозволяє одному вхідному зображенню асоціювати N вихідних. Пам'ять (рис. 4.7) складається з вхідного сенсорного шару нейронів X_i ($i = \overline{1, n}$) та N вихідних шарів Y_{q1}^1 ($q1 = \overline{1, g1}$), Y_{q2}^2 ($q2 = \overline{1, g2}$), ..., Y_{qN}^N ($qN = \overline{1, gN}$), елементи яких пов'язані з відповідними ним нейронами вхідного сенсорного X -шару парами двонаправлених зважених зв'язків з ваговими $W_{i,q1}^{11}$, $W_{q1,i}^{12}$ ($i = \overline{1, n}$; $q1 = \overline{1, g1}$) коефіцієнтами $W_{i,q2}^{21}$, $W_{q2,i}^{22}$ ($i = \overline{1, n}$; $q2 = \overline{1, g2}$), ..., $W_{i,qN}^{N1}$, $W_{qN,i}^{N2}$ ($i = \overline{1, n}$; $qN = \overline{1, gN}$). Верхні індекси матриць вагових коефіцієнтів показують: перший індекс, що нейрони вхідного X -шару з'єднані з нейронами відповідного вихідного шару, другий індекс: 1, коли матриця зв'язків передає сигнали нейронів X -шару нейронам відповідного вихідного шару, і 2, навпаки, коли матриця зв'язків передає сигнали вихідного шару нейронам X -шару. Перші нижні індекси вказують на нейрони, що видають сигнали, а другі – на нейрони, що приймають сигнали [145].

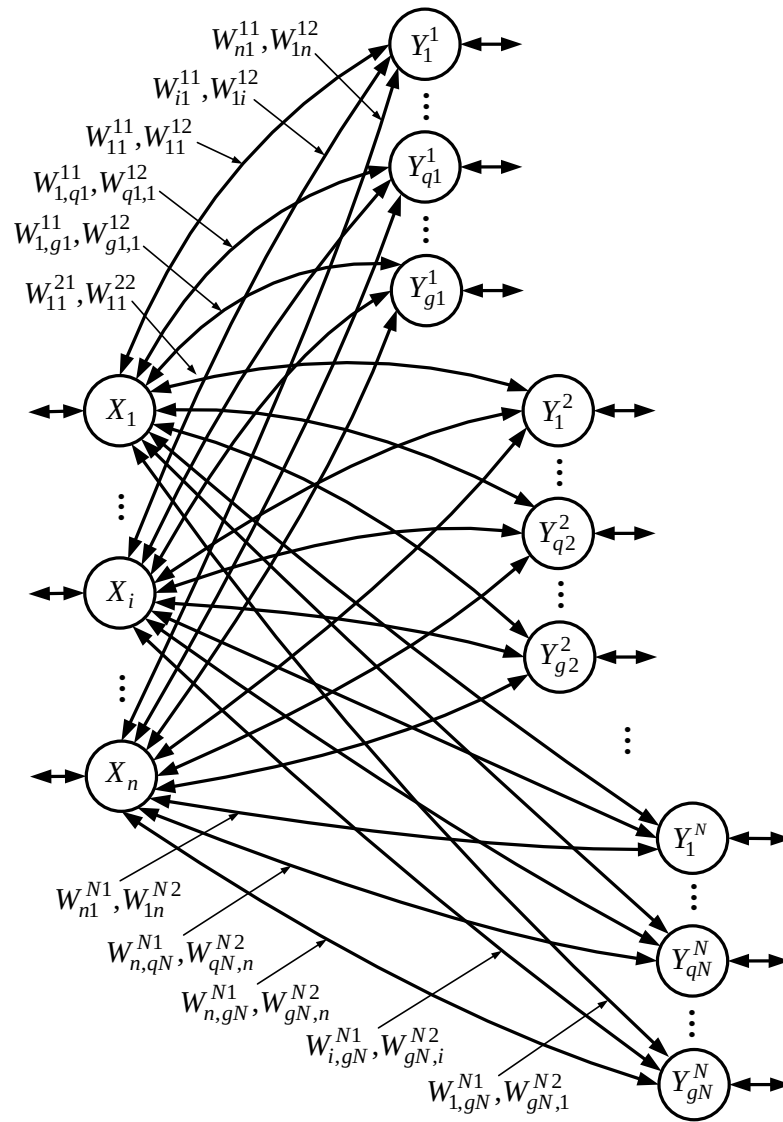


Рис. 4.10. Архітектура N -спрямованої асоціативної пам'яті

Розроблена асоціативна пам'ять функціонує відповідно до двох алгоритмів: навчання та функціонування. Алгоритм навчання зводиться до визначення навчального набору з наборів r наборів зображень:

$$(S_1, S_1^1, S_1^2, \dots, S_1^N), (S_2, S_2^1, S_2^2, \dots, S_2^N), \dots, (S_r, S_r^1, S_r^2, \dots, S_r^N), \quad (4.17)$$

які запам'ятовуються N -спрямованою асоціативною пам'яттю, і матриць ваги зв'язків $W^{11}, W^{12}, W^{21}, W^{22}, \dots, W^{N1}, W^{N2}$ між нейронами вхідного шару і шарами вихідних нейронів: X і Y^1 , X та Y^2 , ..., X і Y^N .

Матриці ваг зв'язків W^{d1}, W^{d2} ($d = \overline{1, N}$) визначаються за допомогою співвідношень, де W^{d1} – матриця ваг зв'язків, яка передає сигнали з виходів

нейронів X -шару на входи нейронів Y^d -шару, $d = \overline{1, N}$; W^{d2} – матриця ваг зв'язків, яка передає сигнали з виходів нейронів Y^d -шару на входи нейронів X -шару, матриця W^{d2} виходить шляхом транспонування матриці W^{d1} ($d = \overline{1, N}$);

r – кількість груп зображень, що використовуються для навчання нейронної мережі; S_{pi} ($i = \overline{1, n}$) – компоненти p -го вхідного зображення $S_p = (S_{p1}, S_{p2}, \dots, S_{pn})$; S_{pj}^d ($j = \overline{1, gd}$) – компоненти зображення $S_p^d = (S_{p1}^d, S_{p2}^d, \dots, S_{p,gd}^d)$, які мають бути на виходах нейронів Y^d -шару при подачі на вхід нейронної мережі зображення S_p :

$$W^{d1} = \begin{bmatrix} W_{11}^d & \dots & W_{1j}^d & \dots & W_{gd}^d \\ \dots & \dots & \dots & \dots & \dots \\ W_{i1}^d & \dots & W_{ij}^d & \dots & W_{i,gd}^d \\ \dots & \dots & \dots & \dots & \dots \\ W_{n1}^d & \dots & W_{nj}^d & \dots & W_{n,gd}^d \end{bmatrix}, \quad W^{d2} = (W^{d1})^T, \quad W_{ij}^d = \sum_{p=1}^r S_{pi} S_{pj}^d, \quad (4.18)$$

Оскільки будь-яка пара верств X і Y^d ($d = \overline{1, N}$) має архітектуру двоспрямованої асоціативної пам'яті, їх навчання аналогічно класичному алгоритму навчання ДАП [146]. Послідовне застосування класичного алгоритму навчання ДАП до шарів нейронів X та Y^1, X і $Y^2, \dots, X$ і Y^N дозволяє запам'ятати всі множини груп асоціативних зображень (4.17).

В алгоритмі функціонування N -спрямованої асоціативної пам'яті в режимі визначення асоціативних зображень прийняті такі позначення:

n – кількість бінарних компонентів у вхідному векторі;

gd – кількість бінарних компонентів в d -м вихідному векторі Y^d -шару ($d = \overline{1, N}$) нейронів;

r – кількість наборів асоціативних зображень, що запам'ятовуються;

$W_{i,qd}^{d1}, W_{qd,i}^{d2}$ ($i = \overline{1, n}; d = \overline{1, N}; qd = \overline{1, gd}$) – ваги зв'язків від елементів вхідного шару до елементів d -го вихідного шару, що містить нейрони $Y_1^d, Y_2^d, \dots, Y_{gd}^d$;

Крок 4. Ініціюються ваги зв'язків $W_{i,qd}^{d1}, W_{qd,i}^{d2}$ ($i = \overline{1, n}; qd = \overline{1, gd}$).
 Задається час: $t = t_0$. При цьому передбачається, що час буде змінюватися дискретно $(t_0, t_1, t_2, \dots)$ з деяким кроком Δt , крім того, передбачається, що час визначення вхідних сигналів нейронів буде значно меншим Δt , а час визначення вихідних сигналів нейронів за їх вхідними даними дорівнюватиме Δt .

Крок 5. Задаються вхідні сигнали нейронів X -шару мережі:

$$U_{\text{вх.}X_i}(t_0) = S_{pi}, \quad i = \overline{1, n}.$$

Обчислюються вихідні сигнали X -елементів:

$$U_{\text{вих.}X_i}(t_1) = f_i(U_{\text{вх.}X_i}(t_0)), \quad i = \overline{1, n}.$$

Визначається початкове значення допоміжної змінної: $b = 0$.

Крок 6. Поки не встановляться вихідні сигнали всіх X - і Y_{qd}^d нейронів, виконуються кроки 7 – 9 алгоритму.

Крок 7. Адаптується активність елементів Y^d шару. Обчислюються вхідні та вихідні сигнали Y_{qd}^d -елементів:

$$U_{\text{вх.}Y_{qd}^d}(t_{1+b}) = \sum_{i=1}^n W_{i,qd}^{d1} U_{\text{вих.}X_i}(t_{1+b}), \quad qd = \overline{1, gd};$$

$$U_{\text{вих.}Y_{qd}^d}(t_{2+b}) = f_{qd}(U_{\text{вх.}Y_{qd}^d}(t_{1+b})), \quad qd = \overline{1, gd}.$$

Вихідні сигнали Y_{qd}^d нейронів посилюються на вході елементів X шару.

Крок 8. Адаптується активність елементів X -шару. Обчислюються вхідні та вихідні сигнали X -елементів:

$$U_{\text{вх.}X_i}(t_{2+b}) = \sum_{qd=1}^{gd} W_{qd,i}^{d2} U_{\text{вих.}Y_{qd}^d}(t_{2+b}), \quad i = \overline{1, n};$$

$$U_{\text{вих.}X_i}(t_{3+b}) = f_i(U_{\text{вх.}X_i}(t_{2+b})), \quad i = \overline{1, n}.$$

Вихідні сигнали X -нейронів посилюються на вході елементів Y_{qd}^d -шару і обчислюються вхідні та вихідні сигнали Y_{qd}^d -елементів:

$$U_{\text{вх.}Y_{qd}^d}(t_{3+b}) = \sum_{i=1}^n W_{i,qd}^{d1} U_{\text{вих.}X_i}(t_{3+b}), \quad qd = \overline{1, gd};$$

$$U_{\text{вих.}Y_{qd}^d}(t_{4+b}) = f_{qd}(U_{\text{вх.}Y_{qd}^d}(t_{3+b})), \quad qd = \overline{1, gd}.$$

Крок 9. Перевіряється тест на збіжність. Порівнюються вихідні сигнали X -нейронів ($U_{\text{вих.}X_i}(t_3)$ і $U_{\text{вих.}X_i}(t_1)$, $i = \overline{1, n}$), а також Y_{qd}^d -нейронів ($U_{\text{вих.}Y_{qd}^d}(t_2)$ і $U_{\text{вих.}Y_{qd}^d}(t_4)$, $qd = \overline{1, gd}$), які були отримані відповідно на поточній та попередній ітераціях. Якщо не виконано хоча б одну рівність:

$$U_{\text{вих.}X_i}(t_{3+b}) = U_{\text{вих.}X_i}(t_{1+b}), \quad i = \overline{1, n};$$

$$U_{\text{вих.}Y_{qd}^d}(t_{2+b}) = U_{\text{вих.}Y_{qd}^d}(t_{4+b}), \quad qd = \overline{1, gd},$$

то змінюється допоміжна змінна: $b = b + 2$, і перевіряється умова досягнення допустимої кількості ітерацій, у своїй, якщо $b > b_{\max}$ то перехід до кроку 10 алгоритму з відповідним повідомленням, якщо ж допустима кількість ітерацій не перевищена ($b \leq b_{\max}$), то перехід до кроку 8 алгоритму. Якщо умови виконуються, то змінна d збільшується однією, і перевіряється умова $d + 1 \leq N$, у разі його блокуються ваги зв'язків $W_{i,qd}^{d1}$, $W_{qd,i}^{d2}$ ($i = \overline{1, n}$; $qd = \overline{1, gd}$), і перехід до кроку 4 алгоритму, інакше – до кроку 10 алгоритму.

Крок 10. Зупинка.

Таким чином, вперше на основі двоспрямованої асоціативної пам'яті запропонована архітектура та алгоритми функціонування N -спрямованої дискретної нейромережевої асоціативної пам'яті, яка здатна відновлювати по вхідному вектору множина N зображень, асоціативних до вхідної інформації. На архітектуру та алгоритми функціонування нейромережевої асоціативної пам'яті отримано патент України на винахід [146].

Друга проблема, характерна для класичної двонаправленої асоціативної пам'яті – відсутня можливість відновлювати за вхідною інформацією ланцюжки взаємопов'язаних асоціацій, вирішується завдяки тому, що її архітектура перебудовується шляхом заміни одного із сенсорних шарів нейронів, наприклад, шару Y -елементів, на N шарів (рис. 4.11), які послідовно

пов'язані один з одним парами двонаправлених зважених зв'язків. При цьому кожна пара сусідніх верств нейронів фактично є двонаправленою асоціативною пам'яттю. В результаті цього виникає можливість будь-якому вектору $Z_{\text{вх.}}^i = (Z_{1\text{вх.}}^i, Z_{2\text{вх.}}^i, \dots, Z_{q_i\text{вх.}}^i)$ деякого шару мережі Z^i ($i = \overline{1, N-1}$) поставити у відповідність асоціативний вектор $Z_{\text{вих.}}^{i+1}$ на виході шару Z^{i+1} , а вектор $Z_{\text{вх.}}^i$ розглядати як асоціацію вхідного вектора попереднього шару нейронної мережі. Тому вектор на вході X -шару мережі породжує ланцюжок їх N двоспрямованих асоціацій, де кожен вектор Z^i ($i = \overline{1, N-1}$) входить у дві асоціації [147, 148].

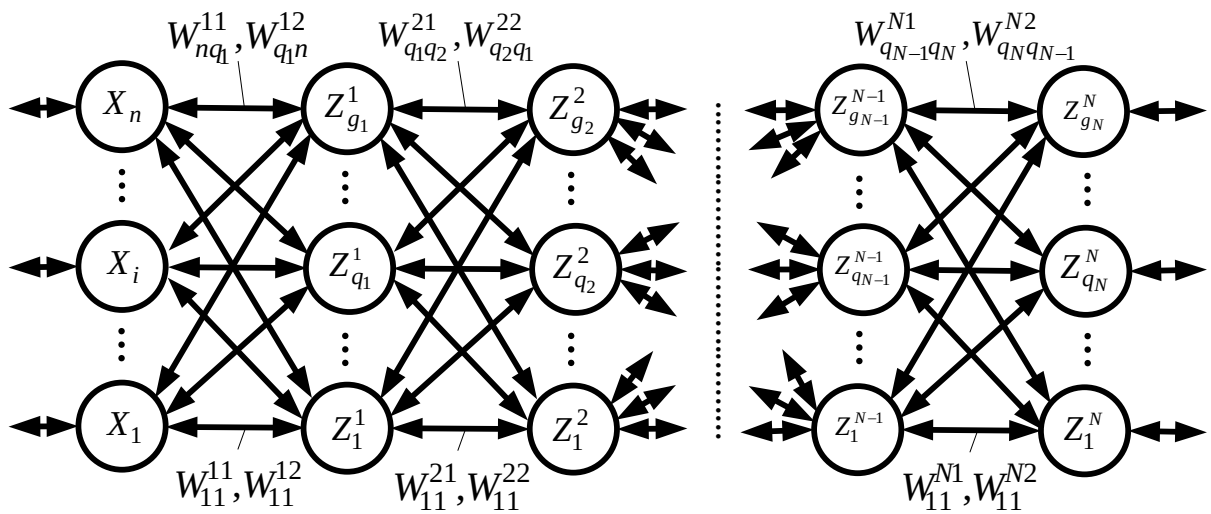


Рис. 4.11. Нейросітєва багатошарова асоціативна пам'ять

Пам'ять складається з сенсорного шару нейронів X_i ($i = \overline{1, n}$) та N шарів Z -елементів $Z^1(Z_1^1, \dots, Z_{q_1}^1), \dots, Z^N(Z_1^N, \dots, Z_{q_N}^N)$. Кожен нейрон вхідного шару X_i ($i = \overline{1, n}$) пов'язаний з кожним нейроном Z^1 -шару парами двонаправлених зважених зв'язків $W_{iq_1}^{11}, W_{q_1i}^{12}$ ($i = \overline{1, n}; q_1 = \overline{1, g_1}$), кожен нейрон Z^1 -шару пов'язаний з кожним нейроном Z^2 -шару парами двонаправлених зважених зв'язків $W_{q_1q_2}^{21}, W_{q_2q_1}^{22}$ ($q_1 = \overline{1, g_1}; q_2 = \overline{1, g_2}$). За аналогією, кожен Z^k шар мережі пов'язаний з попереднім шаром $Z^{(k-1)}$ ($k = \overline{3, N-1}$) парами двонаправлених зважених зв'язків $W_{q_{(k-1)}q_k}^{k1}, W_{q_kq_{k-1}}^{k2}$ ($q_{k-1} = \overline{1, g_{k-1}}; q_k = \overline{1, g_k}$), а також з наступним $Z^{(k+1)}$ шаром (за винятком Z^N шару мережі) парами

двонаправлених зважених зв'язків $W_{q_k q_{k+1}}^{(k+1)1}, W_{q_{(k+1)} q_k}^{(k+1)2} (q_k = \overline{1, g_k}; q_{k+1} = \overline{1, g_{k+1}})$.

Кожен нейрон вихідного шару $Z_{q_N}^N (q_N = \overline{1, g_N})$ пов'язаний з кожним нейроном $Z_{q_{N-1}}^{N-1}$ - шару парами двонаправлених зважених зв'язків $W_{q_N q_{N-1}}^{N1}, W_{q_{(N-1)} q_N}^{N2} (q_N = \overline{1, g_N}; q_{N-1} = \overline{1, g_{N-1}})$.

Розроблена мережа функціонує відповідно до двох алгоритмів: навчання та розпізнавання. Алгоритм навчання є процес визначення навчального набору зображень та визначення матриць ваг зв'язків між шарами нейронів: $X_i, Z^1, Z^2, \dots, Z^N$, з допомогою співвідношень виду (4.17). Оскільки будь-які два Z -шари нейронів Z^1 і Z^2, Z^2 і $Z^3, \dots, Z^{N-1}$ і Z^N , мають архітектуру двонаправленої асоціативної пам'яті, їх функціонування аналогічно класичному алгоритму функціонування ДАП. Послідовне застосування класичного алгоритму ДАП до шарів нейронів Z^1 і Z^2, Z^2 і $Z^3, \dots, Z^{N-1}$ і Z^N дозволяє отримувати весь ланцюжок асоціативних зображень $S^{V1}, S^{V2}, \dots, S^{VN}$. Запропонована багатошарова асоціативна пам'ять є двоспрямованою. Тому, якщо на входи Z^N нейронів подати зображення S^{VN} , то буде отримано ланцюжок асоціативних зображень $S^{V(N-1)}, S^{V(N-2)}, \dots, S^{V1}, S^V$. Процеси функціонування запропонованої нейронної мережі у разі аналогічні процесам функціонування мережі під час подачі зображення S^V на входи шару X - нейронів.

В алгоритмі функціонування багатошарової двонаправленої асоціативної пам'яті в режимі визначення ланцюжків асоціацій прийняті такі позначення:

n – число нейронів у сенсорному шарі нейронів;

$g_1, g_2, \dots, g_N$ – число елементів відповідно в шарах $Z^1, Z^2, \dots, Z^N$ нейронної мережі, $g_1 = g_2 = \dots = g_N$;

$S^V, S^{V1}, S^{V2}, \dots, S^{VN} (v = \overline{1, L})$ – ланцюжки асоціативних зображень;

L – число ланцюжків асоціативних зображень, що запам'ятовуються;

v – номер ланцюжка асоціативних зображень;

$t_0^1, t_1^1, t_2^1, \dots$ – послідовні моменти часу при отриманні асоціативних зображень, якщо $t_1^1 = t_0^1 + \Delta t$ або у загальному вигляді $t_k^1 = t_{(k-1)}^1 + \Delta t$;

Δt – час, необхідне отримання вихідного сигналу нейронів з допомогою функції активації;

f_v – функція активації v -го елемента.

Алгоритм роботи багат шарової двонаправленої асоціативної пам'яті при подачі зображення на перший сенсорний вхід передбачає виконання кроків, аналогічних крокам при функціонуванні ДАП:

Крок 1. Ініціюються ваги зв'язків $W_{iq_1}^{11}, W_{q_1i}^{12}$ ($i = \overline{1, n}; q_1 = \overline{1, g_1}$). Задається початковий час: $t = t_0^1$. Ініціюються нульовими вхідними сигналами всі нейрони мережі:

$$\begin{aligned} U_{\text{вх.} X_i}(0) &= 0; U_{\text{вих.} X_i}(0) = f_i(U_{\text{вх.} X_i}) = 0; i = \overline{1, n}; \\ U_{\text{вх.} Z_{q_1}^1}(0) &= 0; U_{\text{вих.} Z_{q_1}^1}(0) = f_{q_1}(U_{\text{вх.} Z_{q_1}^1}) = 0; q_1 = \overline{1, g_1}. \\ U_{\text{вх.} Z_{q_2}^2}(0) &= 0; U_{\text{вих.} Z_{q_2}^2}(0) = f_{q_2}(U_{\text{вх.} Z_{q_2}^2}) = 0; q_2 = \overline{1, g_2}; \\ &\dots\dots\dots \\ U_{\text{вх.} Z_{q_N}^N}(0) &= 0; U_{\text{вих.} Z_{q_N}^N}(0) = f_{q_N}(U_{\text{вх.} Z_{q_N}^N}) = 0; q_N = \overline{1, g_N}. \end{aligned}$$

Крок 2. Для зображення $S^V = (S_1^V, \dots, S_n^V)$ з довільного ланцюжка навчальних зображень $S^V, S^{V1}, S^{V2}, \dots, S^{VN}$ ($V = \overline{1, L}$) виконуються кроки 3 – 7.

Крок 3 Задаються вхідні сигнали нейронів X -шару мережі:

$$U_{\text{вх.} X_i}(t_0^1) = S_i^V, i = \overline{1, n}.$$

В інтервалі часу $[t_0, t_1^1 = t_0^1 + \Delta t]$ обчислюються вихідні сигнали X -елементів:

$$U_{\text{вих.} X_i}(t_1^1) = f_i(U_{\text{вх.} X_i}(t_0^1)), i = \overline{1, n}.$$

Крок 4. Поки не встановляться вихідні сигнали всіх X - і Z^1 нейронів, виконуються кроки 5 – 7.

Крок 5. Адаптується активність елементів Z^1 шару. Обчислюються вхідні та вихідні сигнали Z^1 -елементів:

$$U_{\text{вх.}Z_{q_1}^1}(t_1^1) = \sum_{i=1}^n W_{iq_1}^{11} U_{\text{вих.}X_i}(t_1^1), \quad i = \overline{1, n}; \quad q_1 = \overline{1, g_1};$$

$$U_{\text{вих.}Z_{q_1}^1}(t_2^1) = f_{q_1}(U_{\text{вх.}Z_{q_1}^1}(t_1^1)); \quad i = \overline{1, n}; \quad q_1 = \overline{1, g_1}.$$

Вихідні сигнали Z^1 нейронів посиляються на входи елементів X шару.

Крок 6. Адаптується активність елементів X -шару. Обчислюються вхідні та вихідні сигнали X -елементів:

$$U_{\text{вх.}X_i}(t_2^1) = \sum_{q_1=1}^{g_1} W_{q_1 i}^{12} U_{\text{вих.}Z_{q_1}^1}(t_2^1), \quad i = \overline{1, n}; \quad q_1 = \overline{1, g_1};$$

$$U_{\text{вих.}X_i}(t_3^1) = f_i(U_{\text{вх.}X_i}(t_2^1)), \quad i = \overline{1, n}.$$

Вихідні сигнали X -нейронів посиляються на входи елементів Z^1 шару:

$$U_{\text{вх.}Z_{q_1}^1}(t_3^1) = \sum_{i=1}^n W_{iq_1}^{11} U_{\text{вих.}X_i}(t_3^1), \quad q_1 = \overline{1, g_1}; \quad i = \overline{1, n};$$

$$U_{\text{вих.}Z_{q_1}^1}(t_4^1) = f_{q_1}(U_{\text{вх.}Z_{q_1}^1}(t_3^1)); \quad q_1 = \overline{1, g_1}; \quad i = \overline{1, n}.$$

Крок 7. Перевіряється тест на збіжність. Порівнюються вихідні сигнали X -нейронів $U_{\text{вих.}X_i}(t_3^1)$ та $U_{\text{вих.}X_i}(t_1^1)$, $i = \overline{1, n}$, а також вихідні сигнали Z^1 -нейронів $U_{\text{вих.}Z_{q_1}^1}(t_2^1)$ та $U_{\text{вих.}Z_{q_1}^1}(t_4^1)$, $q_1 = \overline{1, g_1}$, які отримані на поточній та попередній ітераціях. Якщо не виконано хоча б одну рівність:

$$U_{\text{вих.}X_i}(t_3^1) = U_{\text{вих.}X_i}(t_1^1), \quad i = \overline{1, n};$$

$$U_{\text{вих.}Z_{q_1}^1}(t_2^1) = U_{\text{вих.}Z_{q_1}^1}(t_4^1), \quad q_1 = \overline{1, g_1},$$

то перехід до кроку 5 алгоритму, інакше – на виході Z^1 шару отримано зображення S_1^{v1} , яке є вхідним зображенням для Z^2 шару асоціативної пам'яті і здійснюється перехід до кроку 8.

Для отримання наступних зображень виконуються кроки 8 – 15 алгоритму, коли кожному з k шарів Z -нейронів отримуємо одне зображення з ланцюжка асоціацій, де $k = \overline{1, N-1}$.

Крок 8. Ініціюються ваги зв'язків $W_{q_k q_{(k+1)}}^{k1}, W_{q_{(k+1)} q_k}^{k2}$ ($q_k = \overline{1, g_k}; q_{(k+1)} = \overline{1, g_{(k+1)}}$) і задається час: $t = t_0^{(1+k)}$.

Крок 9. Для заданого зображення $S_k^V = (S_{k1}^V, \dots, S_{kn}^V)$, отриманого на шарі Z^k нейронів, виконуються кроки 10 – 14.

Крок 10 Задається час $t = t_1^{(1+k)}$ і обчислюються вихідні сигнали Z^k -елементів:

$$U_{\text{вих.}Z_{q_k}^k}(t_1^{(1+k)}) = U_{\text{вих.}Z_{q_k}^k}(t_r^k); \quad q_k = \overline{1, g_k},$$

де t_r^k ($r \in \{4, 6, 8, \dots\}$) – момент часу отримання вихідного сигналу на шарі Z^k -елементів попередньої ітерації.

Крок 11 Поки не встановляться вихідні сигнали всіх Z^k і $Z^{(k+1)}$ нейронів, виконуються кроки 12 – 14.

Крок 12 Адаптується активність елементів $Z^{(k+1)}$ шару. Обчислюються вхідні та вихідні сигнали $Z^{(k+1)}$ -елементів:

$$U_{\text{вих.}Z_{q_{(k+1)}}^{(k+1)}}(t_1^{(1+k)}) = \sum_{q_k=1}^{g_k} W_{q_k q_{(k+1)}}^{k1} U_{\text{вих.}Z_{q_k}^k}(t_1^{(1+k)}), \quad q_{(k+1)} = \overline{1, g_{(k+1)}}; \quad q_k = \overline{1, g_k};$$

$$U_{\text{вих.}Z_{q_{(k+1)}}^{(k+1)}}(t_2^{(1+k)}) = f_{q_{(k+1)}}(U_{\text{вих.}Z_{q_{(k+1)}}^{(k+1)}}(t_1^{(1+k)})), \quad q_{(k+1)} = \overline{1, g_{(k+1)}}; \quad q_k = \overline{1, g_k}.$$

Вихідні сигнали $Z^{(k+1)}$ нейронів посилаються на входи елементів Z^k шару.

Крок 13. Адаптується активність елементів Z^k шару. Обчислюються вхідні та вихідні сигнали Z^k -елементів:

$$U_{\text{вих.}Z_{q_k}^k}(t_2^{(1+k)}) = \sum_{q_{(k+1)}=1}^{g_{(k+1)}} W_{q_{(k+1)} q_k}^{k2} U_{\text{вих.}Z_{q_{(k+1)}}^{(k+1)}}(t_2^{(1+k)}), \quad q_k = \overline{1, g_k}; \quad q_{(k+1)} = \overline{1, g_{(k+1)}};$$

$$U_{\text{вих.}Z_{q_k}^k}(t_3^{(1+k)}) = f_i(U_{\text{вих.}Z_{q_k}^k}(t_2^{(1+k)})), \quad q_k = \overline{1, g_k}; \quad q_{(k+1)} = \overline{1, g_{(k+1)}}.$$

Вихідні сигнали Z^k -нейронів посилаються на входи елементів $Z^{(k+1)}$ шару:

$$U_{\text{вх.}Z_{q(k+1)}^{(k+1)}}(t_3^{(1+k)}) = \sum_{q_k=1}^{g_k} W_{q_k q(k+1)}^{k1} U_{\text{вх.}Z_{q_k}^k}(t_3^{(1+k)}), \quad q_{(k+1)} = \overline{1, g_{(k+1)}}; \quad q_k = \overline{1, g_k};$$

$$U_{\text{вх.}Z_{q(k+1)}^{(k+1)}}(t_4^{(1+k)}) = f_{q(k+1)}(U_{\text{вх.}Z_{q(k+1)}^{(k+1)}}(t_3^{(1+k)})); \quad q_{(k+1)} = \overline{1, g_{(k+1)}}; \quad q_k = \overline{1, g_k}.$$

Крок 14. Перевіряється тест на збіжність. Порівнюються вихідні сигнали Z^k -нейронів $U_{\text{вх.}Z_{q_k}^k}(t_3^{(1+k)})$ та $U_{\text{вх.}Z_{q_k}^k}(t_1^{(1+k)})$, $q_k = \overline{1, g_k}$, а також $Z^{(k+1)}$ -нейронів $U_{\text{вх.}Z_{q(k+1)}^{(k+1)}}(t_2^{(1+k)})$ та $U_{\text{вх.}Z_{q(k+1)}^{(k+1)}}(t_4^{(1+k)})$, $q_{(k+1)} = \overline{1, g_{(k+1)}}$, які отримані на поточній та попередній ітераціях.

Якщо не виконано хоч одну рівність:

$$U_{\text{вх.}Z_{q_k}^k}(t_3^{(1+k)}) = U_{\text{вх.}Z_{q_k}^k}(t_1^{(1+k)}), \quad q_k = \overline{1, g_k};$$

$$U_{\text{вх.}Z_{q(k+1)}^{(k+1)}}(t_2^{(1+k)}) = U_{\text{вх.}Z_{q(k+1)}^{(k+1)}}(t_4^{(1+k)}), \quad q_{(k+1)} = \overline{1, g_{(k+1)}},$$

то перехід до кроку 12 алгоритму, якщо $k+1 < N$, те $k = k+1$ й перехід до кроку 8, інакше – кроку 15 алгоритму.

Крок 15. Зупинка.

Розроблено програмне забезпечення, що моделює архітектуру та алгоритми функціонування багатошарової дискретної двонаправленої асоціативної пам'яті [149]. Програма дозволяє в процесі роботи нейронної мережі відновлювати за вхідною інформацією, що подається на входи X - і Z^N нейронів ланцюжка асоціативних зображень. Таким чином, вперше на основі двонаправленої асоціативної пам'яті запропоновано архітектуру та алгоритми функціонування двонаправленої багатошарової дискретної нейронної мережі, яка здатна відновлювати за вхідною інформацією, що подається на будь-який з її двох входів, ланцюжки асоціативних зображень. На архітектуру та алгоритми функціонування мережі отримано патент України на винахід [148].

Для побудови багатошарової асоціативної пам'яті ДАП з керуючими нейронами, яка здатна відновлювати за вхідною інформацією ланцюжки взаємопов'язаних асоціацій і коригувати їх з урахуванням додаткової інформації, необхідна модифікація розробленої вище нейронної мережі, пов'язана з додаванням N керуючих шарів нейронів R^i ($i = \overline{1, N}$). При цьому

кожна пара сусідніх верств нейронів фактично є двонаправленою асоціативною пам'яттю (рис. 4.12). В результаті цього виникає можливість будь-якому вектору $Z_{\text{вх.}}^i = (Z_{1\text{вх.}}^i, Z_{2\text{вх.}}^i, \dots, Z_{q_i\text{вх.}}^i)$ деякого шару мережі Z^i ($i = \overline{1, N}$) поставити у відповідність асоціативний вектор $Z_{\text{вих.}}^{i+1}$ на виході Z^{i+1} шару, а вектор $Z_{\text{вх.}}^i$ розглядати як асоціацію вхідного вектора попереднього шару нейронної мережі. При цьому, за допомогою шарів нейронів, що управляють R^i ($i = \overline{1, N}$), можна здійснювати корекцію векторів Z^i ($i = \overline{1, N}$), що складають ланцюжок асоціативних зображень. Все це дає можливість говорити про те, що будь-який вектор на вході X -шару нейронної мережі породжує ланцюжок їх N двонаправлених асоціацій, де кожен вектор Z^i ($i = \overline{1, N-1}$) входить у дві асоціації, які можна коригувати за допомогою відповідних управляючих нейронів [150, 151].

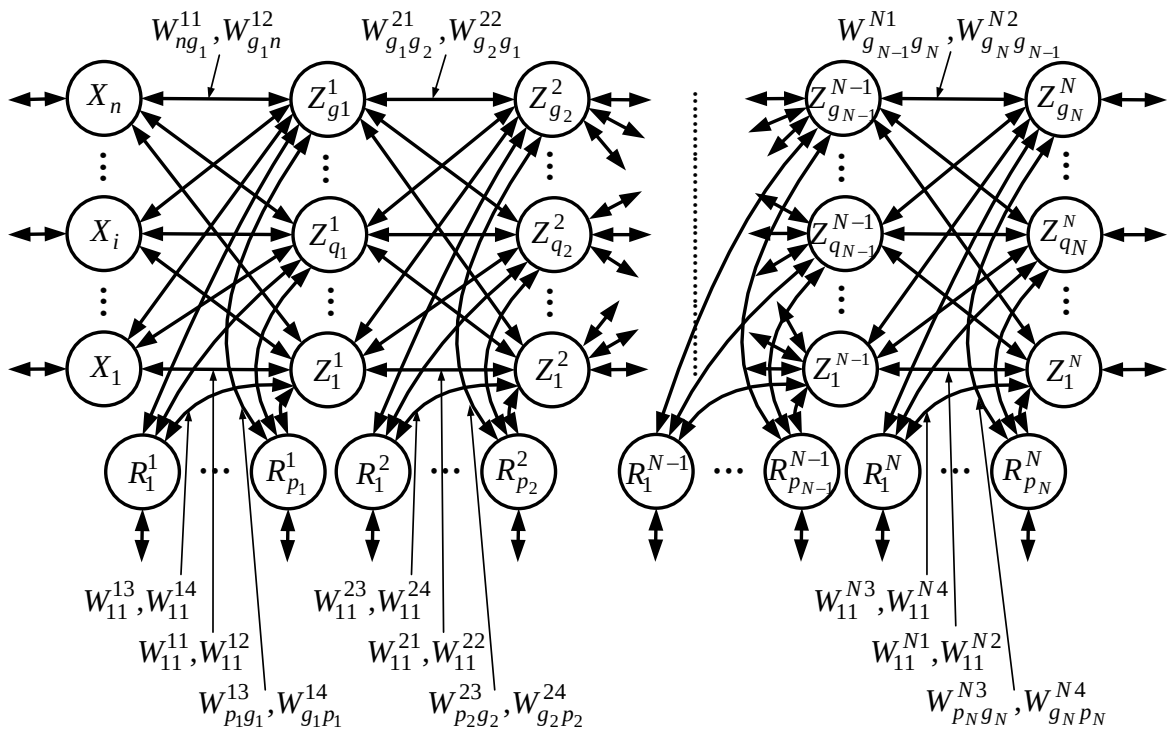


Рис. 4.12. Нейросітєва багатошарова асоціативна пам'ять

При цьому нова пам'ять складається з сенсорного шару нейронів X_i ($i = \overline{1, n}$) та N шарів Z -елементів $Z^1(Z^1_1, \dots, Z^1_{g_1}), \dots, Z^N(Z^N_1, \dots, Z^N_{g_N})$ з керуючими шарами нейронів R^i ($i = \overline{1, N}$). Кожен нейрон вхідного шару X_i ($i = \overline{1, n}$) пов'язаний з кожним нейроном Z^1 -шару парами двонаправлених

зважених зв'язків з ваговими коефіцієнтами $W_{iq_1}^{11}$, $W_{q_1 i}^{12}$ ($i = \overline{1, n}$; $q_1 = \overline{1, g_1}$), кожен нейрон Z^1 -шару пов'язаний з кожним нейроном Z^2 -шару парами двонаправлених зважених зв'язків з ваговими коефіцієнтами $W_{q_1 q_2}^{21}$, $W_{q_2 q_1}^{22}$ ($q_1 = \overline{1, g_1}$; $q_2 = \overline{1, g_2}$) і з кожним нейроном з керуючого R^1 -шару парами двонаправлених зв'язків $R_{h_1}^1$ ($h_1 = \overline{1, p_1}$) з коефіцієнтами $W_{h_1 q_1}^{13}$, $W_{q_1 h_1}^{14}$ ($h_1 = \overline{1, p_1}$; $q_1 = \overline{1, g_1}$). За аналогією кожен Z^k -шар мережі ($k = \overline{3, N}$) пов'язаний з попереднім шаром Z^{k-1} парами двонаправлених зважених зв'язків з ваговими коефіцієнтами $W_{q_{k-1} q_k}^{k1}$, $W_{q_k q_{k-1}}^{k2}$ ($q_{k-1} = \overline{1, g_{k-1}}$; $q_k = \overline{1, g_k}$) і з нейронами $R_{h_{k-1}}^{k-1}$ ($h_{k-1} = \overline{1, p_{k-1}}$) з керуючого шару R^{k-1} парами двонаправлених зважених зв'язків з ваговими коефіцієнтами $W_{h_{k-1} q_{k-1}}^{(k-1)3}$, $W_{q_{k-1} h_{k-1}}^{(k-1)4}$ ($h_{k-1} = \overline{1, p_{k-1}}$; $q_{k-1} = \overline{1, g_{k-1}}$). Кожен Z^k -шар ($k = \overline{2, N-1}$) пов'язаний з наступним $Z^{(k+1)}$ шаром парами двоспрямованих зважених зв'язків $W_{q_k q_{k+1}}^{(k+1)1}$, $W_{q_{k+1} q_k}^{(k+1)2}$ ($q_k = \overline{1, g_k}$; $q_{k+1} = \overline{1, g_{k+1}}$). Кожен нейрон вихідного шару $Z_{q_N}^N$ ($q_N = \overline{1, g_N}$) пов'язаний з кожним нейроном $Z_{q_{N-1}}^{N-1}$ -шару парами двонаправлених зважених зв'язків $W_{q_{N-1} q_N}^{N1}$, $W_{q_N q_{N-1}}^{N2}$ ($q_{N-1} = \overline{1, g_{N-1}}$; $q_N = \overline{1, g_N}$) і з нейронами $R_{h_N}^N$ ($h_N = \overline{1, p_N}$) з керуючого шару R^N парами двонаправлених зважених зв'язків з ваговими коефіцієнтами $W_{h_N q_N}^{N3}$, $W_{q_N h_N}^{N4}$ ($h_N = \overline{1, p_N}$; $q_N = \overline{1, g_N}$).

Розроблена мережа функціонує відповідно до двох алгоритмів: навчання та розпізнавання. Алгоритм навчання цієї нейронної мережі аналогічний алгоритму навчання багатошарової дискретної двонаправленої асоціативної пам'яті. При цьому додавання в структуру нової багатошарової нейромережевої пам'яті N шарів нейронів, що управляють, дає можливість побудови асоціацій з урахуванням додаткової інформації. Це стає можливим завдяки тому, що керуючі нейрони пов'язані з відповідними шарами нейронної мережі і при появі інформації на входах шарів можуть її коригувати з урахуванням інформації на входах керуючих нейронів.

В алгоритмі функціонування багатошарової двонаправленої асоціативної пам'яті з керуючими нейронами прийнято позначення, як в алгоритмі навчання багатошарової ДАП, до яких додані такі позначення:

$SR^{V1}, SR^{V2}, ..., SR^{VN}$ ($V = \overline{1, L}$) - множина керуючих векторів;

SR^{Vk} – множина керуючих нейронів для k - шару Z -нейронів ($k = \overline{1, N}$).

Алгоритм роботи багатошарової двонаправленої асоціативної пам'яті при подачі зображення на перший сенсорний вхід передбачає виконання наступних кроків:

Крок 1. Ініціюються ваги зв'язків $W_{iq_1}^{11}, W_{q_1i}^{12}$ ($i = \overline{1, n}; q_1 = \overline{1, g_1}$). Задається початковий час: $t = t_0^1$. Ініціюються нульовими вхідними сигналами всі нейрони мережі:

$$\begin{aligned} U_{\text{вх.}X_i}(0) &= 0; U_{\text{вих.}X_i}(0) = f_i(U_{\text{вх.}X_i}) = 0; i = \overline{1, n}; \\ U_{\text{вх.}Z_{q_r}^r}(0) &= 0; U_{\text{вих.}Z_{q_r}^r}(0) = f_{q_r}(U_{\text{вх.}Z_{q_r}^r}) = 0; q_r = \overline{1, g_r}; r = \overline{1, N}; \\ U_{\text{вх.}R_{h_r}^r}(0) &= 0; U_{\text{вих.}R_{h_r}^r}(0) = f_i(U_{\text{вх.}R_{h_r}^r}) = 0; h_r = \overline{1, p_r}; r = \overline{1, N}. \end{aligned}$$

Крок 2. Для зображення $S^V = (S_1^V, ..., S_n^V)$ з довільного ланцюжка навчальних зображень $S^V, S^{V1}, S^{V2}, ..., S^{VN}$ ($V = \overline{1, L}$) виконуються кроки 3 – 7.

Крок 3 Задаються вхідні сигнали нейронів X -шару та керуючого R^1 -шару мережі:

$$\begin{aligned} U_{\text{вх.}X_i}(t_0^1) &= S_i^V, i = \overline{1, n}; \\ U_{\text{вх.}R_{h_1}^1}(t_0^1) &= SR_{h_1}^V, h_1 = \overline{1, p_1}. \end{aligned}$$

В інтервалі часу $[t_0, t_1^1 = t_0^1 + \Delta t]$ обчислюються вихідні сигнали нейронів X - і R^1 шару елементів:

$$\begin{aligned} U_{\text{вих.}X_i}(t_1^1) &= f_i(U_{\text{вх.}X_i}(t_0^1)), i = \overline{1, n}; \\ U_{\text{вих.}R_{h_1}^1}(t_1^1) &= f_i(U_{\text{вх.}R_{h_1}^1}(t_0^1)), h_1 = \overline{1, p_1}. \end{aligned}$$

Крок 4. Поки не встановляться вихідні сигнали всіх X – і Z^1 нейронів, виконуються кроки 5–7.

Крок 5. Адаптується активність елементів Z^1 шару. Обчислюються вхідні та вихідні сигнали Z^1 -елементів:

$$U_{\text{вх.}Z^1_{q_1}}(t_1^1) = \sum_{i=1}^n W_{iq_1}^{11} U_{\text{вих.}X_i}(t_1^1) + \sum_{h_1=1}^{p_1} W_{h_1q_1}^{13} U_{\text{вих.}R^1_{h_1}}(t_1^1),$$

$$i = \overline{1, n}; \quad q_1 = \overline{1, g_1}; \quad h_1 = \overline{1, p_1};$$

$$U_{\text{вих.}Z^1_{q_1}}(t_2^1) = f_{q_1}(U_{\text{вх.}Z^1_{q_1}}(t_1^1)); \quad q_1 = \overline{1, g_1}.$$

Вихідні сигнали Z^1 -нейронів посиляються на входи елементів X - і R^1 шарів.

Крок 6. Адаптується активність елементів X – і R^1 шарів. Обчислюються вхідні та вихідні сигнали нейронів X - та R^1 -шарів:

$$U_{\text{вих.}X_i}(t_2^1) = \sum_{q_1=1}^{g_1} W_{q_1i}^{12} U_{\text{вих.}Z^1_{q_1}}(t_2^1), \quad i = \overline{1, n}; \quad q_1 = \overline{1, g_1};$$

$$U_{\text{вих.}X_i}(t_3^1) = f_i(U_{\text{вих.}X_i}(t_2^1)), \quad i = \overline{1, n};$$

$$U_{\text{вих.}R^1_{h_1}}(t_2^1) = \sum_{q_1=1}^{g_1} W_{q_1h_1}^{14} U_{\text{вих.}Z^1_{q_1}}(t_2^1), \quad h_1 = \overline{1, p_1}; \quad q_1 = \overline{1, g_1};$$

$$U_{\text{вих.}R^1_{h_1}}(t_3^1) = f_{h_1}(U_{\text{вих.}R^1_{h_1}}(t_2^1)), \quad h_1 = \overline{1, p_1}.$$

Вихідні сигнали нейронів X - і R^1 шарів посиляються на входи елементів Z^1 шару:

$$U_{\text{вх.}Z^1_{q_1}}(t_3^1) = \sum_{i=1}^n W_{iq_1}^{11} U_{\text{вих.}X_i}(t_3^1) + \sum_{h_1=1}^{p_1} W_{h_1q_1}^{13} U_{\text{вих.}R^1_{h_1}}(t_3^1), \quad q_1 = \overline{1, g_1}; \quad i = \overline{1, n}; \quad h_1 = \overline{1, p_1};$$

$$U_{\text{вих.}Z^1_{q_1}}(t_4^1) = f_{q_1}(U_{\text{вх.}Z^1_{q_1}}(t_3^1)); \quad q_1 = \overline{1, g_1}.$$

Крок 7. Перевіряється тест на збіжність. Порівнюються вихідні сигнали нейронів X -шару $U_{\text{вих.}X_i}(t_3^1)$ і $U_{\text{вих.}X_i}(t_1^1)$ вихідні сигнали керуючих нейронів R^1 -шару $U_{\text{вих.}R_{h_1}^1}(t_3^1)$ і $U_{\text{вих.}R_{h_1}^1}(t_1^1)$, $i = \overline{1, n}$, а також вихідні сигнали нейронів Z^1 -шару $U_{\text{вих.}Z_{q_1}^1}(t_2^1)$ і $U_{\text{вих.}Z_{q_1}^1}(t_4^1)$, які $q_1 = \overline{1, g_1}$, отримані $h_1 = \overline{1, p_1}$, на поточній та попередній ітераціях. Якщо не виконано хоча б одну рівність:

$$\begin{aligned} U_{\text{вих.}X_i}(t_3^1) &= U_{\text{вих.}X_i}(t_1^1), \quad i = \overline{1, n}; \\ U_{\text{вих.}R_{h_1}^1}(t_3^1) &= U_{\text{вих.}R_{h_1}^1}(t_1^1), \quad h_1 = \overline{1, p_1}; \\ U_{\text{вих.}Z_{q_1}^1}(t_2^1) &= U_{\text{вих.}Z_{q_1}^1}(t_4^1), \quad q_1 = \overline{1, g_1}, \end{aligned}$$

то перехід до кроку 5 алгоритму, інакше – на виході Z^1 шару отримано зображення S_1^{V1} , яке є вхідним зображенням для Z^2 шару асоціативної пам'яті і здійснюється перехід до кроку 8.

Для отримання наступних зображень виконуються кроки 8 – 15 алгоритму, коли кожному з шарів Z -нейронів виходить одне зображення з ланцюжка асоціацій, де $k = \overline{1, N}$.

Крок 8. Ініціюються ваги зв'язків $W_{q_k q_{(k+1)}}^{k1}$, $W_{q_{(k+1)} q_k}^{k2}$ ($q_k = \overline{1, g_k}$; $q_{(k+1)} = \overline{1, g_{(k+1)}}$) і задається початковий час визначення зображення на виході Z^k -шару нейронів ($k > 1$): t_0^k .

Крок 9. Для зображення $S_k^V = (S_{k1}^V, \dots, S_{kn}^V)$, отриманого на шарі Z^k нейронів, виконуються кроки 10 – 14.

Крок 10. В інтервалі часу $[t_0^k, t_1^{(1+k)}]$ обчислюються вихідні сигнали нейронів Z^k - і R^k шару елементів:

$$\begin{aligned} U_{\text{вих.}Z_{q_k}^k}(t_1^{(1+k)}) &= U_{\text{вих.}Z_{q_k}^k}(t_r^k); \quad q_k = \overline{1, g_k}, \\ U_{\text{вих.}R_{h_k}^k}(t_1^{(1+k)}) &= U_{\text{вих.}R_{h_k}^k}(t_r^k), \quad h_k = \overline{1, p_k}. \end{aligned}$$

де t_r^k ($r \in \{4, 6, 8, \dots\}$) – момент часу отримання вихідного сигналу на шарі Z^k -елементів попередньої ітерації.

Крок 11 Поки не встановляться вихідні сигнали всіх Z^k і $Z^{(k+1)}$ нейронів, виконуються кроки 12 – 14.

Крок 12 Адаптується активність елементів $Z^{(k+1)}$ шару. Обчислюються вхідні та вихідні сигнали $Z^{(k+1)}$ -елементів:

$$U_{\text{вх.}Z_{q(k+1)}^{(k+1)}}(t_1^{(1+k)}) = \sum_{q_k=1}^{g_k} W_{q_k q(k+1)}^{k1} U_{\text{вих.}Z_{q_k}^k}(t_1^{(1+k)}) + \sum_{h_k=1}^{p_k} W_{h_k q(k+1)}^{k3} U_{\text{вих.}R_{h_k}^k}(t_1^{(1+k)}),$$

$$q_{(k+1)} = \overline{1, g_{(k+1)}}; \quad q_k = \overline{1, g_k}; \quad h_k = \overline{1, p_k};$$

$$U_{\text{вих.}Z_{q(k+1)}^{(k+1)}}(t_2^{(1+k)}) = f_{q(k+1)}(U_{\text{вх.}Z_{q(k+1)}^{(k+1)}}(t_1^{(1+k)})), \quad q_{(k+1)} = \overline{1, g_{(k+1)}}; \quad q_k = \overline{1, g_k}.$$

Вихідні сигнали $Z^{(k+1)}$ -нейронів посилаються на входи елементів Z^k - і $R^{(k+1)}$ шарів.

Крок 13. Адаптується активність елементів Z^k - і $R^{(k+1)}$ шарів. Обчислюються вхідні та вихідні сигнали нейронів Z^k та $R^{(k+1)}$ -шарів:

$$U_{\text{вх.}Z_{q_k}^k}(t_2^{(1+k)}) = \sum_{q(k+1)=1}^{g(k+1)} W_{q(k+1)q_k}^{k2} U_{\text{вих.}Z_{q(k+1)}^{(k+1)}}(t_2^{(1+k)}), \quad q_k = \overline{1, g_k}; \quad q_{(k+1)} = \overline{1, g_{(k+1)}};$$

$$U_{\text{вих.}Z_{q_k}^k}(t_3^{(1+k)}) = f_i(U_{\text{вх.}Z_{q_k}^k}(t_2^{(1+k)})), \quad q_k = \overline{1, g_k}; \quad q_{(k+1)} = \overline{1, g_{(k+1)}};$$

$$U_{\text{вх.}R_{h_k}^k}(t_2^{(1+k)}) = \sum_{q(k+1)=1}^{g(k+1)} W_{q(k+1)h_k}^{k4} U_{\text{вих.}Z_{q(k+1)}^{(k+1)}}(t_2^{(1+k)}),$$

$$h_k = \overline{1, p_k}; \quad q_{(k+1)} = \overline{1, g_{(k+1)}};$$

$$U_{\text{вих.}R_{h_k}^k}(t_3^{(1+k)}) = f_i(U_{\text{вх.}R_{h_k}^k}(t_2^{(1+k)})), \quad h_k = \overline{1, p_k}.$$

Вихідні сигнали нейронів Z^k - і R^k шарів посилаються на входи елементів $Z^{(k+1)}$ шару:

$$U_{\text{вх.}Z_{q(k+1)}^{(k+1)}}(t_3^{(1+k)}) = \sum_{q_k=1}^{g_k} W_{q_k q(k+1)}^{k1} U_{\text{вих.}Z_{q_k}^k}(t_3^{(1+k)}) + \sum_{h_k=1}^{p_k} W_{h_k q(k+1)}^{k3} U_{\text{вих.}R_{h_k}^k}(t_3^{(1+k)}),$$

$$q_{(k+1)} = \overline{1, g_{(k+1)}}; \quad q_k = \overline{1, g_k}; \quad h_k = \overline{1, p_k};$$

$$U_{\text{вих.}Z_{q(k+1)}^{(k+1)}}(t_4^{(1+k)}) = f_{q(k+1)}(U_{\text{вих.}Z_{q(k+1)}^{(k+1)}}(t_3^{(1+k)})); \quad q_{(k+1)} = \overline{1, g_{(k+1)}}; \quad q_k = \overline{1, g_k}.$$

Крок 14. Перевіряється тест на збіжність. Порівнюються вихідні сигнали нейронів Z^k -шару $U_{\text{вих.}Z_{q_k}^k}(t_3^{(1+k)})$ і $U_{\text{вих.}Z_{q_k}^k}(t_1^{(1+k)})$ вихідні сигнали управляючих нейронів R^k -шару $U_{\text{вих.}R_{h_k}^k}(t_3^{(1+k)})$ і, $h_k = \overline{1, p_k}$, а $U_{\text{вих.}R_{h_k}^k}(t_1^{(1+k)})$ також $q_k = \overline{1, g_k}$, вихідні сигнали нейронів $Z^{(k+1)}$ -шару $U_{\text{вих.}Z_{q(k+1)}^{(k+1)}}(t_2^{(1+k)})$ і $U_{\text{вих.}Z_{q(k+1)}^{(k+1)}}(t_4^{(1+k)})$, $q_{(k+1)} = \overline{1, g_{(k+1)}}$, які отримані на поточній та попередній ітераціях. Якщо не виконано хоча б одну рівність:

$$\begin{aligned} U_{\text{вих.}Z_{q_k}^k}(t_3^{(1+k)}) &= U_{\text{вих.}Z_{q_k}^k}(t_1^{(1+k)}), \quad q_k = \overline{1, g_k}; \\ U_{\text{вих.}R_{h_k}^k}(t_3^{(1+k)}) &= U_{\text{вих.}R_{h_k}^k}(t_1^{(1+k)}), \quad h_k = \overline{1, p_k}; \\ U_{\text{вих.}Z_{q(k+1)}^{(k+1)}}(t_2^{(1+k)}) &= U_{\text{вих.}Z_{q(k+1)}^{(k+1)}}(t_4^{(1+k)}), \quad q_{(k+1)} = \overline{1, g_{(k+1)}}, \end{aligned}$$

то перехід до кроку 12 алгоритму, якщо $k+1 < N$, те $k = k+1$ й перехід до кроку 8, інакше - до кроку алгоритму 15.

Крок 15. Зупинка.

Розроблено програмне забезпечення, що моделює архітектуру та алгоритми функціонування багатошарової дискретної двонаправленої асоціативної пам'яті з керуючими нейронами.

Програма дозволяє в процесі роботи нейронної мережі відновлювати за вхідною інформацією, що подається на входи X -або Z^N -нейронів ланцюжка асоціативних зображень. Програма також дозволяє коригувати асоціативні дані з урахуванням додаткової інформації, що зберігається в керуючих нейронах при відновленні ланцюжка зображень, асоціативних вхідної інформації з X шару нейронів.

Таким чином, вперше на основі двонаправленої асоціативної пам'яті запропонована архітектура та алгоритми функціонування нової двонаправленої багатошарової дискретної нейронної мережі, яка здатна відновлювати за вхідною інформацією, що подається на будь-який з її входів,

ланцюжки асоціативних зображень і змінювати ланцюжки асоціацій з урахуванням додаткової інформації керуючі нейрони.

На архітектуру та алгоритми функціонування нейромережевої пам'яті отримано патент України на винахід та корисні моделі [151–158].

Висновки за главою 4

Розроблено модифікації архітектур та алгоритмів функціонування двох безперервних нейронних мереж АРТ-2s та АРТ-2ms, які можуть вибирати та відновлювати зі своєї пам'яті кілька рівноцінних рішень.

Розроблено підхід, пов'язаний із введенням в архітектуру нейронної мережі шару додаткових реєструючих нейронів, що дозволяє додати можливість визначення кількох рівноцінних рішень для класу нейронних мереж, у яких у шарі, що розпізнає кожен з елементів дозволяє визначати тільки одне рішення.

На основі аналізу особливостей стабільно-пластичних нейронних мереж АРТ і мереж Хеммінга розглядається розробка архітектури та алгоритмів функціонування нових стабільно-пластичних нейронних мереж Хеммінга, які, на відміну від їх класичних аналогів не здатних донавчатися в процесі свого функціонування та визначати більше одного рішення та дискретних мереж АРТ, що здійснюють ідентифікацію між вхідним і еталонними зображеннями тільки по одиничним компонентами бінарних векторів в яких вони збігаються, здатні розпізнавати нову інформацію, донавчатися в процесі свого функціонування, і мають можливість визначати кілька рішень, використовуючи при цьому параметр подібності між вхідним і еталонними зображеннями, що враховує всі компоненти бінарних векторів, у яких вони збігаються, що дозволяє використовувати їх як альтернативу дискретним нейронним мережам АРТ.

Розроблено підхід, що узагальнює результати, отримані для мереж Хеммінга на архітектурі інших нейронних мереж. Зокрема, розроблено стабільно-пластичні нейронні мережі Хебба та мережі на основі перцептрону, які, на відміну від їх класичних аналогів, здатні розпізнавати нову інформацію та донавчатися у процесі свого функціонування.

У розділі розроблена N -спрямована нейромережева асоціативна пам'ять, яка, на відміну від існуючих дискретних нейронних мереж двонаправленої асоціативної пам'яті, здатних зберігати лише пару асоціативних один одному зображень, дозволяє відновлювати по вхідному вектору, множина N зображень, асоціативних між собою і до вхідної інформації. Крім того, розглянуто створення багат шарової нейромережевої асоціативної пам'яті з керуючими нейронами, яка, на відміну від класичних дискретних нейронних мереж двонаправленої

асоціативної пам'яті, не здатних за вхідною інформацією відновлювати з пам'яті мережі набори взаємопов'язаних асоціацій, може відновлювати за вхідною інформацією коригувати результати з урахуванням додаткової інформації, що подається на управляючі нейрони.

ГЛАВА 5

МОДЕЛІ УПРАВЛІННЯ ТРАФІКОМ ІНТЕГРАЛЬНИХ ПОТОКІВ ДАНИХ В ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖАХ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

5.1 Визначення статистичних характеристик точкового джерела еластичного трафіку

У [185] показано, що широкий діапазон швидкостей передачі – від декількох Кбіт/с до десятків Гбіт/с, істотний статистичний характер інформаційних потоків в інфокомунікаційних мережах, велика різноманітність мережевих конфігурацій значно ускладнюють опис трафіку в мультисервісних системах в порівнянні з класичними мережами зв'язку. У [172] обґрунтована вимога наявності можливості будь-якої зміни ширини смуги пропускання каналу між пунктами прийому і передачі, що забезпечується пакетною комутацією, причому плавно і практично на будь-яку величину, навіть до повного використання всіх можливих мережевих ресурсів.

Це робить у ряді випадків неприйнятним для аналізу характеристик реального мережевого трафіку інтегральних потоків даних використання класичного підходу [199], заснованого на марківських або напівмарківських моделях [176, 177], управлінні доступом на основі поняття ефективної пропускної спроможності [196] і припущеннях щодо пуассонівського характеру потоків [181, 182]. У зв'язку з цим останнім часом з'явилися роботи, в котрих аналіз характеристик трафіку проводиться на основі його статистичного характеру в системах з довготривало залежними процесами на вході [190, 195].

Проте, в загальному вигляді проблема отримання характеристик реального трафіку, створюваного інтегральними потоками даних (надалі – трафік ІПД), що дозволяють адекватно змодельовати його поведінку в інфокомунікаційних мережах, котрі використовують сучасні технології, на сьогодні не вирішена [177]. Зокрема, представляє інтерес дослідження характеристик еластичного трафіку, котрий доволі часто зустрічається у мультисервісних мережах та може в широких межах пристосовуватися до затримок і змін пропускної спроможності у мережі, але при цьому задовольняти потребам користувачьких та системних прикладень.

Розглянемо інфокомунікаційну мережу, що має i точкових джерел еластичного трафіку (ТДЕТ) [184]. припустимо, що i -те джерело ($i = \overline{1, I}$) характеризується випадковим процесом $V_i(t)$, котрий визначає сімейство випадкових функцій швидкості передачі інформації конкретних сеансів. даний стохастичний процес, що розглядається в перебігу деякого часового інтервалу $[0, T_i]$, можна охарактеризувати такими ключовими параметрами [184]:

$$V_i^{(\max)} = \max_{t \in [0, T_i]} V_i(t) - \text{піковою швидкістю передачі } i\text{-го ТДЕТ};$$

$$V_i^{(cp)} = \int_0^{T_i} V_i(t) dt - \text{середньою швидкістю передачі (математичним сподіванням) } i\text{-го ТДЕТ};$$

$$k_i^{(p)} = \frac{V_i^{(\max)}}{V_i^{(cp)}} - \text{коефіцієнтом пачковості [198], котрий визначає співвідношення між величинами пікової і середньої швидкості (величина, зворотна коефіцієнту пачковості, що називається коефіцієнтом можливого заповнення} - k_i^{(zap)} = \left(k_i^{(p)} \right)^{-1} \Big);$$

$$T_i^{(\max)} - \text{тривалістю пікового навантаження.}$$

Припустимо також, що об'єм інформації, переданої за час $t \in [0, T_i]$, характеризується випадковою величиною $W_i(t)$ з максимально можливим значенням $W_i^{(\max)} = V_i^{(\max)} \cdot T_i^{(\max)}$. тоді $V_i(t) = \frac{dW_i(t)}{dt}$. Розглянемо ймовірність досягнення пікової швидкості передачі трафіку i -го ТДЕТ на розглядаємому часовому інтервалі $[0, T_i]$: $p_i = P\left(V_i(t) = V_i^{(\max)} \right)$. дана ймовірність характеризує не тільки швидкість передачі інформації, але і її об'єми, що передаються:

$$V_i(t) = V_i^{(\max)} \Rightarrow \left(V_i(t) \cdot T_i^{(\max)} = V_i^{(\max)} \cdot T_i^{(\max)} \right) \equiv \left(W_i(t) = W_i^{(\max)} \right) \Rightarrow \\ \Rightarrow P_i = P \left(W_i(t) = W_i^{(\max)} \right).$$

Розіб'ємо часовий інтервал $[0, T_i]$ на дві підмножини вкладених інтервалів $\mathfrak{T}_i^{(1)}$ і $\mathfrak{T}_i^{(2)}$ таким чином (рис. 5.1):

$$\mathfrak{T}_i^{(1)} \cup \mathfrak{T}_i^{(2)} = [0, T_i]; \quad \mathfrak{T}_i^{(1)} \cap \mathfrak{T}_i^{(2)} = \emptyset;$$

$$\forall t^{(1)} \in [t_i^{(1)'}; t_i^{(1)''}] \subset \mathfrak{T}_i^{(1)} \Rightarrow V_i(t^{(1)}) = V_i^{(\max)};$$

$$\forall t^{(2)} \in [t_i^{(2)'}; t_i^{(2)''}] \subset \mathfrak{T}_i^{(2)} \Rightarrow V_i(t^{(2)}) < V_i^{(\max)}.$$

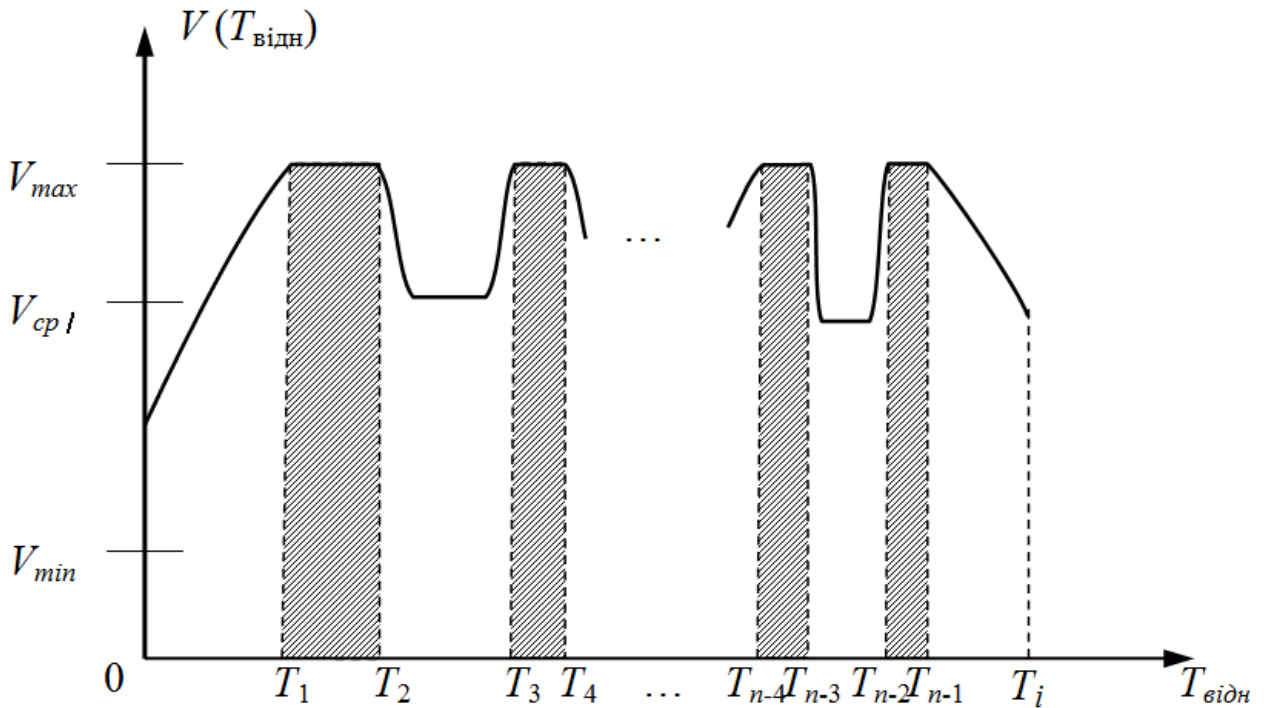


Рис. 5.1. Схема розбиття інтервалу

Дане розбиття дозволяє визначити тривалість пікового навантаження на заданому інтервалі, що дорівнює:

$$T_i^{(\max)} = \sum_{\left[t_i^{(1)}; t_i^{(1)} \right] \subset \mathfrak{Z}_i^{(1)}} \left| t_i^{(1)} - t_i^{(1)} \right|, \quad (5.1)$$

та знайти значення ймовірності досягнення пікової швидкості передачі трафіка i -го ТДЕТ на даному часовому інтервалі. для цього розрахуємо площі, що відповідають даним підмножинам $\mathfrak{Z}_i^{(1)}$ і $\mathfrak{Z}_i^{(2)}$:

$$\Theta_1 = \int_{\mathfrak{Z}_i^{(1)}} V_i(t) dt = V_i^{(\max)} \cdot T_i^{(\max)}; \quad \Theta_2 = \int_{\mathfrak{Z}_i^{(2)}} V_i(t) dt; \quad (5.2)$$

$$\Theta = \Theta_1 + \Theta_2 = V_i^{(\max)} \cdot T_i^{(\max)} + \Theta_2.$$

тоді шукана ймовірність дорівнює:

$$p_i = \frac{\Theta_1}{\Theta} = \frac{V_i^{(\max)} \cdot T_i^{(\max)}}{V_i^{(\max)} \cdot T_i^{(\max)} + \Theta_2}. \quad (5.3)$$

Використовуючи узагальнену інтегральну теорему про середнє (можливість застосування визначається еластичністю трафіка), визначимо, що:

$$\exists \eta \in [0, T_i] \mid \Theta_2 = V_i(\eta) \cdot (T_i - T_i^{(\max)}). \quad (5.4)$$

враховуючи, що:

$$\Theta = \Theta_1 + \Theta_2 = V_i^{(cp)} \cdot T_i,$$

а також значення для площ, що розраховані в (5.2), знайдемо значення Θ_2 :

$$\Theta_2 = \Theta - V_i^{(cp)} \cdot T_i = V_i^{(cp)} \cdot T_i - V_i^{(\max)} \cdot T_i^{(\max)}. \quad (5.5)$$

Відмітимо, що використовуючи вирази (5.4) і (5.5) можна розрахувати значення $V_i(\eta)$ таким чином:

$$V_i(\eta) = \frac{\Theta_2}{T_i - T_i^{(\max)}} = \frac{V_i^{(cp)} \cdot T_i - V_i^{(\max)} \cdot T_i^{(\max)}}{T_i - T_i^{(\max)}}.$$

Використовуючи вираз (5.3), отримуємо, що:

$$p_i = \frac{V_i^{(\max)} \cdot T_i^{(\max)}}{V_i^{(cp)} \cdot T_i} = k_i^{(p)} \cdot \frac{T_i^{(\max)}}{T_i}. \quad (5.6)$$

Оскільки розглядається джерело еластичного трафіку, то $\Theta_2 > 0$, тобто виходячи з виразу (5.5) отримуємо:

$$V_i^{(cp)} \cdot T_i - V_i^{(\max)} \cdot T_i^{(\max)} > 0; \quad \frac{V_i^{(\max)}}{V_i^{(cp)}} \cdot \frac{T_i^{(\max)}}{T_i} < 1 \Rightarrow k_i^{(p)} \cdot \frac{T_i^{(\max)}}{T_i} < 1,$$

що цілком узгоджується з виразом (5.6).

Знаючи ймовірність досягнення пікової швидкості, можна визначити ймовірність того, що пікова швидкість не буде досягнута, таким чином:

$$q_i = 1 - p_i = P\left(V_i(t) < V_i^{(\max)}\right).$$

Для подальшого аналізу необхідно знати величину розкиду можливих значень випадкової величини V_i на розглядаємому часовому інтервалі $[0, T_i]$. для цього визначимо щільність розподілу $f(V_i)$ даної випадкової величини, при котрій досягається $\sup D[V_i]$.

При відомій щільності ймовірності дисперсія розраховується таким чином:

$$D[V_i] = \int_{-\infty}^{\infty} V_i^2 f(V_i) dV_i - M^2[V_i] = \int_0^{V_i} V_i^2 f(V_i) dV_i - \left(\int_0^{V_i} V_i f(V_i) dV_i \right)^2. \quad (5.7)$$

Відмітимо, що аргумент V_i приймає значення в діапазоні від $V_i^{(\min)}$ до $V_i^{(\max)}$ $\left(0 \leq V_i^{(\min)} < V_i^{(\max)}\right)$. виходячи з цього проведемо апроксимацію

$D[V_i]$, поділивши відрізок $\Delta = [V_i^{(\min)}; V_i^{(\max)}]$ на n рівних частин

$$\Delta_j = [V_i^{(j-1)}; V_i^{(j)}] \text{ таким чином, що } \bigcup_{j=1}^n \Delta_j = \Delta; \quad \bigcap_{j=1}^n \Delta_j = \emptyset.$$

Тоді, вибравши усередині кожного відрізка Δ_j за теоремою про інтегральне середнє точку ξ_j , дисперсію можна представити, виходячи з (5.7), як:

$$D[V_i] = \sum_{o=1}^m \xi_j^2 \cdot \int_{V_i^{j-1}}^{V_i^j} f(V_i) dV_i - \left(\sum_{o=1}^m \xi_j \int_{V_i^{j-1}}^{V_i^j} f(V_i) dV_i \right)^2. \quad (5.8)$$

$$\text{Відмітивши, що } \int_{V_i^{j-1}}^{V_i^j} f(V_i) dV_i = p_j, \quad \sum_{j=1}^n p_j = 1, \quad \text{і позначивши}$$

$\vec{p} = (p_1, \dots, p_n)$ знайдемо екстремум дисперсії (5.8), використовуючи метод множників Лагранжа для вирішення задачі оптимізації:

$$\sum_{j=1}^n p_j \cdot \xi_j^2 - \left(\sum_{o=1}^n p_j \cdot \xi_j \right)^2 \rightarrow \text{extr} \quad (5.9)$$

при $\sum_{j=1}^n p_j = 1; p_j \geq 0$.

Складемо лагранжіан задачі (5.9):

$$L(\vec{p}, \lambda) = \sum_{j=1}^n p_j \cdot \xi_j^2 - \left(\sum_{j=1}^n p_j \cdot \xi_j \right)^2 - \lambda \left(\sum_{j=1}^n p_j - 1 \right)$$

і знайдемо його безумовний екстремум з такої системи рівнянь:

$$\begin{cases} \frac{\partial L}{\partial p_j} = 0, j = \overline{1, n}; \\ \frac{\partial L}{\partial \lambda} = 0 \end{cases} \Rightarrow \begin{cases} \xi_j^2 - 2\xi_j \left(\sum_{j=1}^n p_j \cdot \xi_j \right) - \lambda = 0; \\ \sum_{j=1}^n p_j - 1 = 0. \end{cases}$$

З першого рівняння системи знайдемо ξ_j :

$$\xi_j = \tilde{m}_\xi \pm \sqrt{\tilde{m}_\xi^2 + \lambda}, \text{ де } \tilde{m}_\xi = \sum_{j=1}^n p_j \cdot \xi_j$$

Тобто для множників Лагранжа, що задовольняють умові $\lambda > -\tilde{m}_\xi^2$, існує рівно два різні значення ξ_j : ξ_1 і ξ_2 , при цьому: $n = 2$; $p_1 = p_i$; $p_2 = 1 - p_1 = q_i$, тобто функція розподілу ймовірності має дискретний вигляд, а щільність розподілу $f(V_i) = p_i \delta(V_i - \xi_1) + q_i \delta(V_i - \xi_2)$, де $\delta(\cdot)$ – функція Дірака.

Тепер можна розрахувати математичне сподівання і дисперсію випадкової величини V_i :

$$M[V_i] = p_i \xi_1 + q_i \xi_2 = p_i \xi_1 + (1 - p_i) \xi_2; \quad (5.10)$$

$$\begin{aligned} D[V_i] &= p_i \xi_1^2 + (1 - p_i) \xi_2^2 - M^2[V_i] = p_i \xi_1^2 + (1 - p_i) \xi_2^2 - p_i^2 \xi_1^2 - \\ &- 2p_i \xi_1 \xi_2 (1 - p_i) - (1 - p_i)^2 \xi_2^2 = (1 - p_i) p_i (\xi_1 - \xi_2)^2. \end{aligned} \quad (5.11)$$

Очевидно, що $\sup D[V_i]$ досягається при максимальному значенні множника $(\xi_1 - \xi_2)^2$, тобто $\xi_1 = V_i^{(\max)}$; $\xi_2 = V_i^{(\min)}$, а, отже:

$$M[V_i] = p_i V_i^{(\max)} + (1 - p_i) V_i^{(\min)}. \quad (5.12)$$

але $M[V_i] = V_i^{(cp)}$, а значення $V_i^{(\min)}$ для реальних процесів з еластичним трафіком без обмеження спільності можна прирівняти до нуля. тому:

$$V_i^{(cp)} = p_i V_i^{(\max)} \Rightarrow p_i = \frac{V_i^{(cp)}}{V_i^{(\max)}} = \left(k_i^{(p)}\right)^{-1};$$

$$D[V_i] = (1 - p_i) p_i \left(V_i^{(\max)}\right)^2.$$

Знайдемо значення p_i , при якому досягається максимальне значення дисперсії V_i :

$$\frac{dD[V_i]}{dp_i} = \left(V_i^{(\max)}\right)^2 (-2p_i + 1) \Rightarrow p_i = 1/2,$$

тобто при $p_i = q_i = 1/2$ спостерігається максимальний розкид значень випадкової величини V_i .

Також відзначимо, що стосовно оцінки даного ТДЕТ, використовуючи (5.6), можна визначити максимальну тривалість пакету, котрий передається з піковою швидкістю $T_i^{(\max_d)}$:

$$k_i^{(p)} \cdot \frac{T_i^{(\max_d)}}{T_i} = \frac{1}{2} \Rightarrow T_i^{(\max_d)} = \frac{T_i}{2 \cdot k_i^{(p)}}. \quad (5.13)$$

Отже, запропонований підхід до визначення статистичних характеристик точкового джерела еластичного трафіку інфокомунікаційної

мережі дозволяє провести імовірнісну оцінку швидкості передачі інформації, використовуючи апроксимацію її функції щільності розподілу, і є базою для моделювання агрегованого трафіку від декількох джерел еластичного трафіка.

5.2. Математична модель еластичного трафіку

У більшості робіт для моделювання агрегованого трафіку декількох служб інфокомунікаційної мережі використовується класичний підхід, заснований на побудові адекватної динамічної моделі у вигляді систем звичайних диференціальних рівнянь, наприклад [166]. Проте для побудови такої моделі необхідне знання значного об'єму апіорної інформації про досліджуваний процес [168]. Окрім цього, обов'язковим є припущення про гаусовий характер окремих складових процесу [174]. Проте, докладний аналіз реального трафіку, створюваного ПІД інфокомунікаційної мережі, показує наявність в ній довготривалих залежностей, котрі призводять до розподілів з «важкими хвостами» [197]. А врахування фрактального характеру як сумарного трафіку, так і трафіку від окремих джерел (ОД) конкретних мережеских служб, не дозволяє побудувати класичну динамічну модель. Проте, застосування апарату сплайн-функцій з достатньо малими інтервалами розбиття для кожного окремого джерела дозволяє провести достатньо точну і швидко апроксимацію досліджуваної сесії [183].

5.2.1. Сплайн-інтерполяція еластичного трафіку

Розглянемо інфокомунікаційну мережу, котра має K служб, причому k -та служба $(k = \overline{1, K})$ обслуговує трафік, що надходить з L_k джерел. Нехай $W^{(k, \ell_k)}(t)$ – об'єм інформації, що надходить до k -ої служби від джерела $\ell_k (\ell_k = \overline{1, L_k})$ за досліджуємою сесією $t \in [t_0, T_c]$. Для аналізу характеру цієї функції використовуємо апарат локальних сплайнів [180], котрий дозволяє врахувати різний характер поведінки $W^{(k, \ell_k)}(t)$ на різних часових інтервалах сесії з найменшою помилкою апроксимації щодо норми в просторі $L_2[t_0, T_c]$. Для побудови локального $n^{(k, \ell_k)}$ -сплайна з вузлами інтерполяції $t_i^{(k, \ell_k)}$, де $i = \overline{0, n^{(k, \ell_k)}}$, $t_0^{(k, \ell_k)} = t_0$, $t_{n^{(k, \ell_k)}}^{(k, \ell_k)} = T_c$, необхідно на

кожному відрізку інтерполяції $\tau_i^{(k,\ell_k)} = [t_{i-1}^{(k,\ell_k)}, t_i^{(k,\ell_k)}]$ побудувати інтерполяційний поліном $P_{n^{(k,\ell_k)},i}^{(k,\ell_k)}(t)$. Тоді сплайн, що апроксимує $W^{(k,\ell_k)}(t)$, у загальному випадку можна представити як [167]:

$$S^{(k,\ell_k)}(t) = \sum_{i=1}^{n^{(k,\ell_k)}} \alpha_i^{(k,\ell_k)} \cdot P_{n^{(k,\ell_k)},i}^{(k,\ell_k)}(t), \quad (5.14)$$

де $\alpha_i^{(k,\ell_k)}$ – набір постійних коефіцієнтів в незалежному функціональному базисі $\left\{ P_{n^{(k,\ell_k)},i}^{(k,\ell_k)} \right\}$, який істотно залежить від характеру поведінки функцій $W^{(k,\ell_k)}(t)$ на розглядаємому інтервалі $\tau_i^{(k,\ell_k)}$. Так, якщо:

$$W^{(k,\ell_k)}(t) \in C^\beta(\tau_i), \quad (5.15)$$

то апроксимуючий поліном може мати ступінь не вище $2\beta + 1$, а апроксимувати при $W^{(k,\ell_k)}(t) \in C^\infty(\tau_i)$ можна тригонометричними сплайнами [186].

Розглянемо побудову кусково-поліноміального сплайна на інтервалі τ_i при виконанні умови (5.15). Задамо вузли $t_{j,i}^{(k,\ell_k)} \left(j = 0, n_i^{(k,\ell_k)} \right)$ та визначимо значення функції $W^{(k,\ell_k)}(t)$ в них: $W^{(k,\ell_k)}(t_{j,i}^{(k,\ell_k)})$.

В якості міри апроксимуючого полінома будемо розглядати число $\gamma = \overline{0, \beta - 1}$. Для кожного j -го вузла побудуємо інтерполяційний поліном $P_\beta(t, W_{j,i}^{(k,\ell_k)})$, виходячи зі значень у вузлах $t_{j-\gamma,i}^{(k,\ell_k)}, \dots, t_{j-\gamma+\beta,i}^{(k,\ell_k)}$. Тоді відповідний кусочно-поліноміальний сплайн для інтервалу $\tau_i^{(k,\ell_k)}$ визначається як:

$$S_i^{(k,\ell_k)}(t, \beta) = Q_{2\beta+1}^{(k,\ell_k)}(t, j),$$

$$\begin{aligned} \text{де} \quad \frac{d^m}{dt^m} Q_{2\beta+1}^{(k, \ell_k)}(t, j) \Big|_{t=t_{j,i}^{(k, \ell_k)}} &= \frac{d^m}{dt^m} P_{\beta} \left(t, W_{j,i}^{(k, \ell_k)} \right) \Big|_{t=t_{j,i}^{(k, \ell_k)}} ; \\ \frac{d^m}{dt^m} Q_{2\beta+1}^{(k, \ell_k)}(t, j) \Big|_{t=t_{j+1,i}^{(k, \ell_k)}} &= \frac{d^m}{dt^m} P_{\beta} \left(t, W_{j,i}^{(k, \ell_k)} \right) \Big|_{t=t_{j+1,i}^{(k, \ell_k)}} ; \quad m = \overline{1, \beta}. \end{aligned}$$

Представимо $Q_{2\beta+1}^{(k, \ell_k)}(t, j)$ як $Q_{2\beta+1}^{(k, \ell_k)}(t, j) = P_{\beta} \left(t, W_{j,i}^{(k, \ell_k)} \right) + R_{2\beta+1}^{(k, \ell_k)}(t, j)$,

де останній член даного розкладання $R_{2\beta+1}^{(k, \ell_k)}(t, j)$ є поправкою до класичного інтерполяційного полінома (ІП) на інтервалі τ_i , котра при виконанні (5.15) розраховується як [169]:

$$R_{2\beta+1}^{(k, \ell_k)}(t, j) = (t_{j+1} - t_j)^{\beta+1} \cdot W_{2\beta+1}^{(k, \ell_k)}(t_{j-\gamma}, t_{j-\gamma+1}, \dots, t_{j-\gamma+\beta+1}) \cdot q_{2\beta+1}(\tilde{t}, j),$$

де $W_{2\beta+1}^{(k, \ell_k)}(t_{j-\gamma}, t_{j-\gamma+1}, \dots, t_{j-\gamma+\beta+1})$ – відношення порядку $2\beta+1$; $\tilde{t} = \frac{t - t_j}{t_{j+1} - t_j}$;

$$\begin{aligned} q_{2\beta+1}(\tilde{t}, j) &= \frac{t_{j+\beta-\gamma+1} - t_{j-\gamma}}{t_{j+1} - t_j} \cdot \sum_{r=0}^{\beta} \left(\left(\frac{d^2}{d\tilde{t}^2} \prod_{\xi=0}^{\beta} \left(\tilde{t} - \frac{t_{j-\gamma+\xi}}{t_{j+1} - t_i} \right) \right) \Big|_{\tilde{t}=1} \right) \cdot \theta_r(\tilde{t}) ; \\ \theta_r(\tilde{t}) &= \frac{\tilde{t}^{j+1} \cdot (\tilde{t} - 1)^r}{r! j!} \cdot \sum_{m=0}^{\beta-r} (-1)^m \frac{(\beta + m)!}{m!} (\tilde{t} - 1)^m. \end{aligned}$$

В якості інтерполяційного поліному (ІП) в даному випадку можна вибрати ІП Лагранжа ступеню β [162]:

$$\begin{aligned} P_{\beta} \left(t, W_{t_{j,i}}^{(k, \ell_k)} \right) &= \sum_{m=0}^{\beta} W^{(k, \ell_k)} \left(t_{m,i}^{(k, \ell_k)} \right) \times \\ &\times \frac{\prod_{m_1=0}^{\beta} \left(t - t_{m_1,i}^{(k, \ell_k)} \right)}{\prod_{m_2=0}^{m-1} \left(t_{m,i}^{(k, \ell_k)} - t_{m_2,i}^{(k, \ell_k)} \right) \cdot \prod_{m_3=m+1}^{\beta} \left(t_{m,i}^{(k, \ell_k)} - t_{m_3,i}^{(k, \ell_k)} \right)}. \end{aligned} \quad (5.16)$$

Відповідно до [161] можна оцінити погрішність (5.16) як норму значення

нев'язки $R_{\beta,i}^{(k,\ell_k)} = \|W^{(k,\ell_k)}(t) - S_i^{(k,\ell_k)}(t, \beta)\|_{L_2(\tau_i)}$, отже:

$$R_{\beta,j,i}^{(k,\ell_k)}(t) \leq \sup_{t \in \tau_{j,i}^{(k,\ell_k)}} \left| \frac{d^{n_i^{(k,\ell_k)}}}{dt n_i^{(k,\ell_k)}} W_{j,i}^{(k,\ell_k)}(t) \right| \cdot \frac{\prod_{m=0}^{\beta} (t - t_{m,i}^{(k,\ell_k)})}{(\beta + 1)!}, \quad (5.17)$$

тобто при збільшенні β росте точність інтерполяційного наближення, проте збільшується складність обробки.

Тому вибір значення $\beta^{(i)} \leq \beta$ для кожного інтервалу τ_i є окремим завданням, котре залежить від вимог до апроксимації $W^{(k,\ell_k)}(t)$. Окрім цього, необхідно розглянути питання адекватності запропонованої сплайн-інтерполяційної моделі агрегованого трафіку реальному процесу.

5.2.2. Ітераційний метод оцінки адекватності моделі трафіку

Використовуючи вирази (5.14) – (5.17) можна запропонувати ітераційний метод оцінки адекватності узагальненого сплайна

$$S = \bigcup_{k=1}^K \bigcup_{\ell_k=1}^{L_k} S^{(k,\ell_k)}(t) \text{ реальному трафіку на інтервалі } [t_o, T_c].$$

Представимо інтервал $[t_o, T_c]$ як об'єднання I часових інтервалів:

$$[t_o, T_c] = \bigcup_{i=1}^I [t_{i-1}, t_i], \quad t_i|_{i=0} = t_o; \quad t_i|_{i=I} = T_c,$$

на кожному з яких проводилася та кількість вимірювань, котра необхідна для побудови сплайн-полінома необхідного ступеня гладкості, а в якості критерію точності інтерполяції будемо використовувати $\varepsilon_i^{(k,\ell_k)}$ - обмежену нев'язку [160]:

$$\rho(W^{(k,\ell_k)}(t), S_m^{(k,\ell_k)}(t)) \leq \varepsilon_i^{(k,\ell_k)}, \quad (5.18)$$

де $t \in \tau_i = [t_{i-1}, t_i]$; m – ступінь інтерполюючого полінома, що дорівнює:

$$m = \arg \min_{m'} S_{m'}^{(k, \ell_k)}(t), \quad (5.19)$$

а відстань $\rho(\bullet)$ визначена в просторі $L_2[t_o, T_c]$, тобто:

$$\rho\left(W^{(k, \ell_k)}(t), S_m^{(k, \ell_k)}(t)\right) = \sup_{t \in \tau_i} \left| W^{(k, \ell_k)}(t) - S_m^{(k, \ell_k)}(t) \right|. \quad (5.20)$$

Ввівши позначення $\tilde{S}_m^{(k, \ell_k)} = \sup_{t \in \tau_i} \left| \frac{d^m S^{(k, \ell_k)}(t)}{dt^m} \right|$ і використовуючи вирази

(5.19), (5.20), критерій (5.18) можна записати таким чином:

$$\sup_{t \in \tau_i} \left| W^{(k, \ell_k)}(t) - S_m^{(k, \ell_k)}(t) \right| \leq \frac{\tilde{S}_{m+1}^{(k, \ell_k)}}{(m+1)!} \sup_{t \in \tau_i} \left| \prod_{r=0}^m (t - t_r) \right| \leq \varepsilon_i^{(k, \ell_k)}. \quad (5.21)$$

Тоді з виразу (5.21) для кожної пари (k, ℓ_k) можна знайти такі значення $\tilde{m}^{(k, \ell_k)}$ і $\tilde{S}_{\tilde{m}^{(k, \ell_k)}+1}^{(k, \ell_k)}$, при котрих буде забезпечена необхідна точність інтерполяції. Для цього необхідно вибирати $t_j^{(i)}$ і t_i таким чином, щоб ці значення співпадали із коренями полінома Чебишева:

$$t_j^{(i)} = \frac{t_{i-1} + t_i}{2} - \frac{t_{i+1} + t_i}{2} \cos\left(\frac{2j-1}{2m} \pi\right), \quad j \in \overline{1, m},$$

для використання відомої [163] верхньої оцінки:

$$\sup_{t \in \tau_i} \left| \prod_{r=0}^m (t^{(i)} - t_r^{(i)}) \right| \leq 2 \left(\frac{t_{i-1} - t_i}{4} \right)^m. \quad (5.22)$$

Оцінюючи з використанням виразів (5.18) – (5.22) адекватність сплайн-інтерполяції реальному трафіку, на кожному із кроків ітерації будемо проводити аналіз виразу (5.21) на ступінь невідповідності по всіх $k \in \overline{1, K}$ і $\ell = \overline{1, L}$ [189] і залежно від ступеня відхилення від $\varepsilon_i^{(k, \ell)}$ проводити нове

розбиття $[t_o, T_c]$. Згідно [188] даний інтегральний процес є швидкозбіжним і дозволяє визначити поліноміальну сплайн-інтерполяцію трафіку, таку, що надає високу точність апроксимації сумарного трафіку мережі $W(t)$ на часовому інтервалі $[t_o, T_c]$ типової сесії мережі.

Запропонований підхід можна використовувати при проведенні оцінки адекватності сплайнової інтерполяції трафіку інфокомунікаційної мережі. Для майже регулярного трафіку можлива реалізація методу в режимі реального часу з динамічним уточненням постійних коефіцієнтів сплайна (5.14). Відсутність швидкої збіжності описаного вище ітераційного процесу свідчатиме про неможливість інтерполяції сплайна, котра викликана наявністю великої кількості нерегулярних складових, обумовлених фрактальним характером трафіку. Розглянута математична модель використана для синтезу двовимірної динамічної моделі еластичного трафіку інтегрального потоку даних, що базується на оперативній статистичній інформації про проходження потоку, припускає близькість трафіку ІПД до еластичного і наявності вимірювань по декількох сесіях.

5.3 Синтез двовимірної динамічної моделі трафіку ІПД

Ключовими характеристиками трафіку ІПД, котрі найбільш доступні для аналізу при роботі користувачів мережі, є об'єм переданої інформації і швидкість передачі даних [187]. Процес зміни швидкості передачі є випадковим [194], відповідними імовірнісними характеристиками котрого можуть бути безумовна і сумісна щільність розподілу випадкових величин, вибраних у якості точкових функцій процесу у фіксовані моменти часу, на основі аналізу яких зазвичай будуються моделі мережевого трафіку [193].

Проте, знаходження відповідних імовірнісних характеристик реального трафіку у багатьох випадках є проблематичним, а у разі частої зміни швидкості передачі робить неможливим процес оперативного перепланування мережевих ресурсів. тому необхідно синтезувати таку модель мережевого трафіку, котра б дозволила б оперативно визначати межі варіювання його основних характеристик, виходячи із статистичного матеріалу, що накопичується.

Розглянемо інформаційно-телекомунікаційну мережу, характер поведінки мережевого трафіку в котрій невідомий, проте передбачається, що часовий інтервал проведення чергової сесії можна розбити на кінцеве число

підінтервалів, на кожному трафік є близьким до еластичного, а для аналізу його параметрів і синтезу адекватної моделі використовуються статистичні оцінки, отримані при обробці даних, накопичених за деяке число сесій. При цьому, на відміну від існуючих моделей, поведінку процесу будемо вважати залежною не тільки від часу, але і від початкових умов (зокрема від початкової швидкості передачі інформації в кожній сесії).

Нехай $\{W^{(k,\ell_k)}(t)\}$ – сімейство динамічних функцій, котрі характеризують об'єм інформації від джерела ℓ_k , що оброблюється k -ою службою ($k = \overline{1, K}$) мультисервісної мережі з середньою швидкістю $V^{(k,\ell_k)}(t) = \frac{dW^{(k,\ell_k)}(t)}{dt}$, що описується залежністю $V^{(k,\ell_k)}(t) = \Psi(W^{(k,\ell_k)}, t)$, причому:

$$V^{(k,\ell_k)}(t_0) = \left. \frac{dW^{(k,\ell_k)}(t)}{dt} \right|_{t=t_0} = V_0^{(k,\ell_k)}; \quad t \in [t_0^{(k,\ell_k)}, t_0^{(k,\ell_k)} + T^{(k,\ell_k)}], \quad (5.23)$$

де $t_0^{(k,\ell_k)}$ – нижня межа даного часового інтервалу, а $T^{(k,\ell_k)}$ – його довжина.

Проведемо R вимірювань в межах N різних сесій з початковими умовами $V_{0,n}^{(k,\ell_k)}$ ($n = \overline{0, N-1}$) в моменти часу $t_{r,n}^{(k,\ell_k)}$, $r = \overline{0, R-1}$.

Для завдання двовимірної області моделі в межах кожної сесії розглядатимемо відносний час (до реального часу додається $t_{0,n}^{(k,\ell_k)}$). Тоді у якості довжини інтервалу моделювання виберемо $T^{(k,\ell_k)} = \max_n T_n^{(k,\ell_k)}$ (рис. 5.2).

Тоді отримані вимірювання потрапляють в допустиму область моделі, що задається таким чином:

$$\mathfrak{Z}^{(k,\ell_k)} = \left[V_{\min}^{(k,\ell_k)}, V_{\max}^{(k,\ell_k)} \right] \times \left[0; T^{(k,\ell_k)} \right] \subset \mathfrak{R}^2, \quad (5.24)$$

де $V_{\min}^{(k,\ell_k)}, V_{\max}^{(k,\ell_k)}$ – мінімальна і максимальна межі варіювання перших

похідних функцій сімейства $\{W^{(k,\ell_k)}(t)\}$ в межах даних сесій.

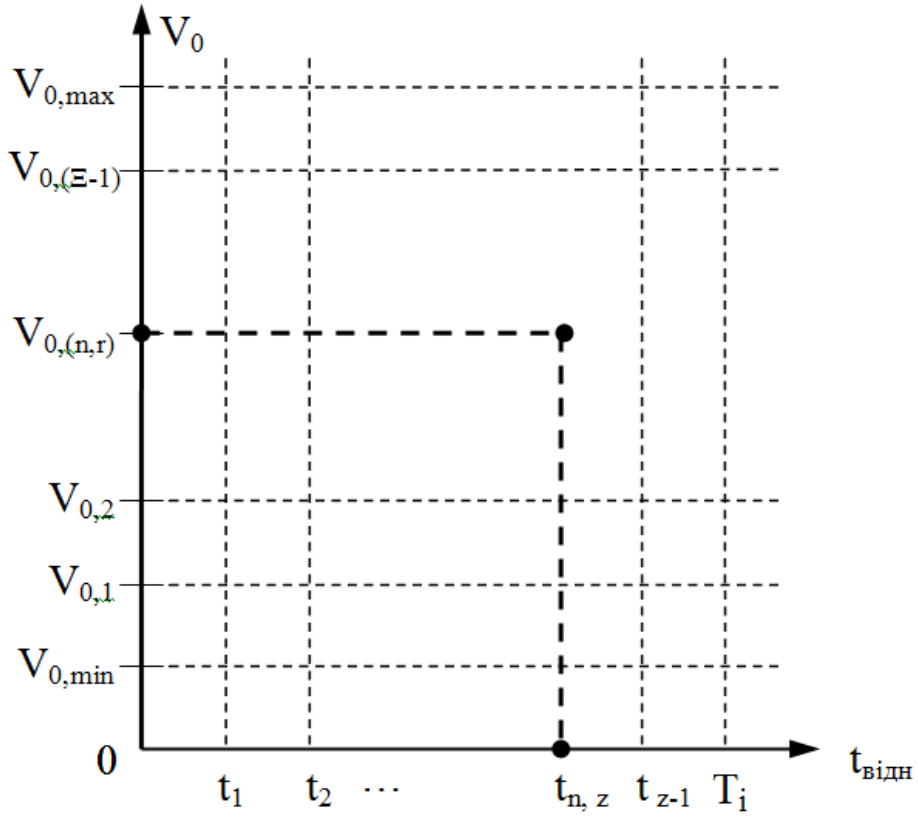


Рис.5.2. Схема області двовимірної інтерполяції

Тоді задача побудови динамічної моделі еластичного трафіку ІТМ може бути сформульована таким чином.

Сформувати сімейство сплайн-функцій, що задовольняють умові адекватності трафіку:

$$\begin{aligned} \rho\left(W^{(k,\ell_k)}\left(V_0^{(k,\ell_k)}, t\right), \tilde{W}^{(k,\ell_k)}\left(V_0^{(k,\ell_k)}, t\right)\right) &\leq \varepsilon^{(k,\ell_k)}; \\ \left(V_0^{(k,\ell_k)}, t\right) &\in \mathfrak{Z}^{(k,\ell_k)}, \end{aligned} \quad (5.25)$$

де $\tilde{W}(\bullet)$ – функція, що апроксимує $W(\bullet)$ за заданих початкових умов, а аргумент $\left(t, V_0^{(k,\ell_k)}\right)$ виділяє з сімейства $\{W^{(k,\ell_k)}(t)\}$ таку функцію, для якої виконана умова (5.23).

Оскільки $\mathfrak{Z}^{(k,\ell_k)} \subset \mathbb{R}^2$, то в (5.25) відстань $\rho(\bullet)$ є стандартною метрикою простору, тобто:

$$\max_{t, W_0^{(k, \ell_k)}} \left| W^{(k, \ell_k)} \left(V_0^{(k, \ell_k)}, t \right) - \tilde{W}^{(k, \ell_k)} \left(V_0^{(k, \ell_k)}, t \right) \right| \leq \varepsilon^{(k, \ell_k)} ; \quad (5.26)$$

$$\left(V_0^{(k, \ell_k)}, t \right) \in \mathfrak{Z}^{(k, \ell_k)} .$$

Для подальшої побудови моделі скористаємося результатом виконання збору статистичних даних реального трафіку, що дозволило побудувати таку множину вимірювань:

$$M^{(k, \ell_k)} = \left\{ m_{nr}^{(k, \ell_k)}, n = \overline{0, N-1}, r = \overline{0, R-1} \right\}, \quad (5.27)$$

де кожне вимірювання $m_{nr}^{(k, \ell_k)}$ можна представити як суму змодельованого вимірювання $\tilde{m}_{nr}^{(k, \ell_k)}$ і нев'язки $\delta \tilde{m}_{nr}^{(k, \ell_k)}$, пов'язаної з помилками вимірювань, причому, згідно [192], помилки некорельовані і мають нульове математичне сподівання.

Оскільки у вузлах передбачається локальна еластичність трафіку, то для синтезу математичної моделі можна розглянути узагальнений інтерполяційний поліном двовимірного сплайн-представлення функції $\tilde{W}^{(k, \ell_k)} \left(V_0^{(k, \ell_k)}, t \right)$ в базисі метричного простору L^2 над областю $\mathfrak{Z}^{(k, \ell_k)}$ [79]:

$$\begin{aligned} & \tilde{W}^{(k, \ell_k)} \left(V_0^{(k, \ell_k)}, t \right) = \\ & = \sum_{(\xi=\overline{0, R-1})}^{(\zeta=\overline{0, N-1})} \alpha_{\zeta, \xi}^{(k, \ell_k)} \times f_{\zeta, \Xi}^{(k, \ell_k)} \left(V_0^{(k, \ell_k)} \right) \phi_{\xi, Z}^{(k, \ell_k)} (t), \end{aligned} \quad (5.28)$$

де $f_{\zeta, \Xi}^{(k, \ell_k)} \left(V_0^{(k, \ell_k)} \right) \phi_{\xi, Z}^{(k, \ell_k)} (t)$ – базис інтерполяційного розкладання в L^2 , визначений над $\mathfrak{Z}^{(k, \ell_k)}$ відповідно до [191], в якому Ξ і Z визначають порядок сплайна по осях n і r відповідно; $\alpha_{\zeta, \xi}^{(k, \ell_k)}$ – невідомі коефіцієнти даного розкладання, а для підсумовування за декількома індексами використовується запропоноване в [200] позначення, еквівалентне

загальноприйнятому: $\sum_{i_1=1}^{I_1} \sum_{i_2=1}^{I_2} (\bullet)$.

Для виконання $\varepsilon^{(k,\ell_k)}$ -адекватності змодельованих значень із (5.28) необхідно при побудові сплайна накласти на елементи множини нев'язок $\delta\tilde{M}(\bullet)$ функцій $W^{(k,\ell_k)}(V_0^{(k,\ell_k)}, t)$ такі обмеження [159]:

$$\begin{aligned} \max_{t, V_0^{(k,\ell_k)}} \left| \delta\tilde{m}^{(k,\ell_k)}(V_0^{(k,\ell_k)}, t) \right| &\leq \varepsilon^{(k,\ell_k)} ; \\ \delta\tilde{m}^{(k,\ell_k)} &\in \delta\tilde{M}^{(k,\ell_k)}, \quad (V_0^{(k,\ell_k)}, t) \in \mathfrak{Z}^{(k,\ell_k)}, \end{aligned} \quad (5.29)$$

які дозволять відповідно до способу оцінки адекватності визначити значення порядків сплайнів.

При виконанні умови (5.29) невідомі коефіцієнти розкладання (5.28) знаходяться з такої системи алгебраїчних рівнянь:

$$\sum_{(\zeta=0, \overline{N-1})}^{(\zeta=0, \overline{R-1})} \alpha_{\zeta, \xi}^{(k,\ell_k)} \times f_{\zeta, \Xi}^{(k,\ell_k)}(V_{0,n}^{(k,\ell_k)}) \phi_{\xi, Z}^{(k,\ell_k)}(t_r) = m_{nr}. \quad (5.30)$$

Використання поліномів Лагранжа, як базисних функції інтерполяційного розкладання, в (5.28) і (5.30) приводить до такої моделі динамічного трафіку:

$$\begin{aligned} \tilde{W}^{(k,\ell_k)}(V_0^{(k,\ell_k)}, t) &= \sum_{(\xi=0, \overline{R-1})}^{(\zeta=0, \overline{N-1})} \alpha_{\zeta, \xi}^{(k,\ell_k)} \cdot L_{\zeta, \Xi}^{(k,\ell_k)}(V_0^{(k,\ell_k)}) \cdot L_{\xi, Z}^{(k,\ell_k)}(t) = \\ &= \sum_{(r=0, \overline{R-1})}^{(n=0, \overline{N-1})} m_{n,r}^{(k,\ell_k)} \cdot \sum_{\zeta=0}^Z \frac{\mathfrak{Z}_{\zeta}(V_0^{(k,\ell_k)})}{\mathfrak{Z}_{\zeta}(V_{0,\zeta}^{(k,\ell_k)})} \cdot \sum_{\xi=0}^{\Xi} \frac{\aleph_{\xi}(t)}{\aleph_{\xi}(t_{n,\xi})}, \end{aligned} \quad (5.31)$$

$$\text{де } \mathfrak{Z}_{\zeta}(V_0^{(k,\ell_k)}) = \prod_{i=0, i \neq \zeta}^Z (V_0^{(k,\ell_k)} - V_{0,i}^{(k,\ell_k)}); \quad \aleph_{\xi}(t) = \prod_{j=0, j \neq \xi}^{\Xi} (t - t_{n,j}).$$

Для виконання умови адекватності (5.29) необхідно вибрати кроки розбиття γ області $\mathfrak{Z}^{(k,\ell_k)}$ вузлами $(V_{0,n}^{(k,\ell_k)}, t)$, виходячи з умови мінімізації оцінки погрішності двовимірної інтерполяції [164]. Проведений аналіз показав, що при відносно невеликій кількості точок порушення еластичності

$W^{(k,\ell_k)}(V_0^{(k,\ell_k)}, t)$ розмірність розбиття γ є відносно невеликою і дозволяє провести оперативний аналіз якості функціонування мережі.

Запропонована математична модель дозволяє на основі накопичених статистичних даних синтезувати трафік, що створюється декількома джерелами за наявності даних вимірювань по декількох сесіях. Результати порівняння трафіку, змодельованого стандартними і запропонованою моделями, показали, що сумарне відхилення від реального трафіку зменшилося в середньому на 15%. Моделювання мережевого нееластичного трафіку, для якого не існує розбиття, що задовольняє умові (5.28), розглянуте в наступних підрозділах. При цьому необхідно враховувати складні взаємозв'язки між флуктуаціями робочого навантаження і різними мережними механізмами управління, що виникають в процесі конвергенції трафіку, а також характеристики викидів, пов'язаних з пульсуючим характером такого.

5.4. Конвергенція трафіку в мультисервісних мережах

Система комутації інфокомунікаційної мережі при обслуговуванні виклику, ініційованого ППД, залежно від виду інформації повинна сполучати між собою одночасно деяку кількість (i) каналів ($1 \leq i \leq V$, V – кількість каналів у напрямі зв'язку), що призводить до подальшого ускладнення механізмів управління мережею. Тому у разі перевантаження мережі може з'являтися додаткова нелінійність [165]. Важливо відзначити, що в подібних ситуаціях можуть виникати дуже складні взаємозв'язки між флуктуаціями робочого навантаження і різними мережевими механізмами управління. Ці взаємодії є потенційною причиною виникнення фрактальної структури трафіку в ІТМ [170]. Тому перед моделюванням трафіку, що має фрактальний характер, необхідно розглянути процес його конвергенції, при котрому одноканальні системи масового обслуговування типу $M/M/1/\infty$ об'єднуються в багатоканальну систему масового обслуговування.

Розглядатимемо процеси, що відбуваються в ІТМ при одночасному обслуговуванні великої, але скінченної кількості каналів і споживачів. Для проведення таких досліджень розглядатимемо ефекти об'єднання одноканальних систем масового обслуговування (СМО) типу $M/M/1/\infty$ в багатоканальну систему. Добре відомі моделі телекомунікаційного трафіку, створені на основі теорії масового обслуговування з пріоритетами [171]. Ці

моделі дозволяють враховувати деякі специфічні особливості фрактального трафіку, такі як існування кластеризації і непостійність характеристик у всіх часових масштабах. Крім того, фрактальний трафік добре описується поволі затухаючими розподілами (наприклад, розподіли Парето, Вейбулла, логонормальний, гіперекспоненціальний). У даному підрозділі для спрощення будуть розглянуті лише такі стохастичні моделі, функціонування котрих описується дискретними марківськими процесами, що дозволить скористатися відомими формулами для стаціонарних розподілів процесу загибелі і народження, а також мультиплікативною теоремою для мереж Джексоновського типу. Проведемо дослідження системи масового обслуговування, отриманої з декількох одноканальних СМО типу $M/M/1/\infty$ шляхом їхнього об'єднання в багатоканальну СМО.

Об'єднуючи рівнопотужні одноканальні СМО типу $M/M/1/\infty$, побудуємо СМО, у котрої стаціонарна довжина черги і час релаксації є істотно меншими, ніж у її складових.

Проведемо дослідження впливу способу комутації на показники ефективності сконструйованих систем, виявляючи конвергенційні ефекти.

Нехай $X_1, X_2, \dots$ – послідовність незалежно працюючих систем масового обслуговування типу $M/M/1/\infty$, що мають інтенсивність вхідного потоку λ і інтенсивність обслуговування, μ а також задовольняють умові ергодичності $\rho = \frac{\lambda}{\mu} < 1$. Побудуємо із заданих n елементів послідовності таку

систему обслуговування S , в котрій стаціонарна довжина черги $a(S)$ і характерний час релаксації (встановлення стаціонарного режиму) $\tau(S)$ задовольняють нерівностям $a(S) \leq A$; $\tau(S) \leq T$, де A, T – числа, що менші ніж аналогічні показники $a(X_i), \tau(X_i)$ елементів початкової послідовності.

Розглянемо об'єднання n незалежних однолінійних систем масового обслуговування $X_1, \dots, X_n$ в багатолінійну систему S_n типу $M/M/n/\infty$, надану на рис. 5.3.

На рис. 5.3 стрілки зображають вхідні і початкові потоки, вузли – обслуговуючі прилади з чергами, прямокутник – багатоканальну систему із загальною чергою.

Операцію комутації, яка задана в цьому випадку, запишемо у вигляді формули $S_n = X_1 \oplus \dots \oplus X_n$. Оскільки виконані умови ергодичності систем,, то

при деяких позитивних C і α стаціонарна середня довжина черги $a(S_n)$ в системі S_n задовольняє нерівності $a(S_n) \leq Ce^{-\alpha n}$.

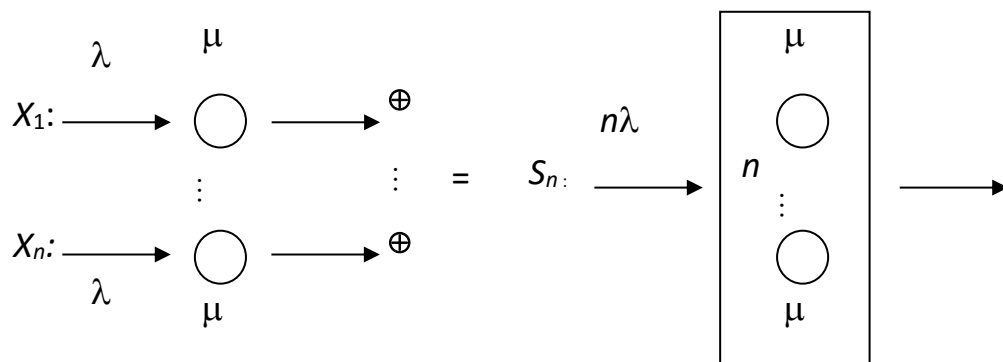


Рис. 5.3. Конвергенція незалежних однолінійних СМО в багатолінійну систему

Розглянемо тепер об'єднання систем $X_1, \dots, X_n$ в наступну систему Σ_n типу М/м/1/є, зображену на рис. 5.4.

Задану в цьому випадку операцію комутації зобразимо у вигляді формули

$$\Sigma_n = X_1 \otimes \dots \otimes X_n.$$

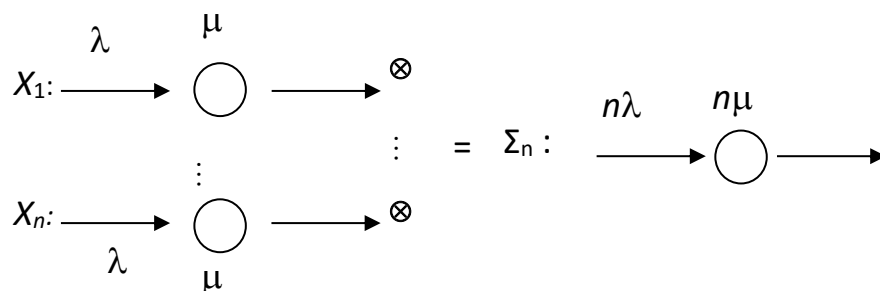


Рис. 5.4. Конвергенція незалежних однолінійних СМО в систему типу М/м/1/є

При виконанні наведених вище умов стаціонарна середня довжина черги $a(\Sigma_n)$ в системі Σ_n задовольняє такому співвідношенню:

$$a(\Sigma_n) \equiv a(X_1) < \infty.$$

З'ясуємо, як впливає тип комутації на час релаксації.

З аналізу часу релаксації $\tau(S_n)$ системи S_n виходить, що при наведених обмеженнях комутація систем $X_1, \dots, X_n$ за типом « $\oplus$ » призводить до

геометричної збіжності до нуля стаціонарної середньої довжини черги при $n \rightarrow \infty$, а комутація за типом « $\otimes$ » впливу на середню довжину черги не надає.

Справедливо і зворотне: комутація систем $X_1, \dots, X_n$ за типом « $\oplus$ », по суті, на час релаксації не впливає, а комутація $X_1, \dots, X_n$ за типом « $\otimes$ » призводить до убування часу релаксації до нуля із швидкістю порядку біля $1/n, n \rightarrow \infty$.

Якщо система обслуговування S_n^m синтезована з $N = nm$ систем типу М/М/1/∞, то маючи достатньо велику кількість N початкових систем обслуговування і використовуючи способи комутації « $\oplus$ », « $\otimes$ », можна синтезувати з них таку систему, в котрій і час релаксації, і стаціонарна середня довжина черги будуть достатньо малими.

Характерною особливістю трафіку інтегральних потоків даних є збільшення середнього часу очікування заявки в черзі (середньої довжини черги) із зростанням завантаження системи.

У нашому випадку, коли із зростанням кількості екземплярів n систем М/М/1/∞, що об'єднуються в систему S_n , завантаження росте, характер поведінки системи нагадує за своєю суттю фазовий перехід у фізичних системах.

Припустимо тепер, що об'єднувані системи (для простоти – в двоканальному) мають різні швидкості обслуговування.

Позначимо через X', X'' інтенсивності вхідних потоків, μ', μ'' – інтенсивності обслуговування в початкових одноканальних системах.

Тоді інтенсивність вхідного потоку λ дорівнює $\lambda' + \lambda''$.

Коефіцієнти завантаження дорівнюють $\rho = \lambda'/\mu' = \lambda''/\mu'' = \lambda/\mu$.

Неважко довести [107], що при $\rho < 1$ марківський процес $i(t)$ має граничний розподіл, який задовольняє системі лінійних рівнянь:

$$\begin{cases} \lambda p(0) = \mu' p(1') + \mu'' p(1''); \\ (\lambda + \mu') p(1') = \lambda' p(0) + \mu'' p(2); \\ (\lambda + \mu'') p(1'') = \lambda'' p(0) + \mu' p(2); \\ (\lambda + \mu) p(2) = \lambda (p(1') + p(1'')) + \mu p(3); \\ (\lambda + \mu') p(i) = \lambda p(i-1) + \mu p(i+1); \quad i = 3, 4, \dots; \\ p(0) + p(1') + p(1'') + p(2) + p(3) + \dots = 1. \end{cases} \quad (5.32)$$

Введемо наступні позначення:

$$\alpha = \mu' / \mu = \lambda' / \lambda; \quad \beta = \alpha(1 - \alpha); \quad A = p(1') / P(1'')$$

і проведемо дослідження системи рівнянь (5.32). Величина A характеризує відмінність в стаціонарній ймовірності завантаження окремих каналів, а B – стаціонарну ймовірність відсутності очікування для заявки, що знову поступила до об'єднаної системи. При цьому при фіксованому α , $1/2 < \alpha < 1$, є вірною монотонна збіжність:

$$A \downarrow (1 - \alpha^2) / (\alpha(2 - \alpha)) \text{ при } p \uparrow 1,$$

а при фіксованому p , $0 < p < 1$, є вірною збіжність $A \rightarrow 0$ при $\alpha \rightarrow 1$.

Іншими словами, в об'єднаній двоканальній системі більш потужніший канал є менш завантаженим, чим інший. Цей ефект посилюється при збільшенні коефіцієнта завантаження r і при наближенні коефіцієнта α до одиниці. Таким чином, стаціонарна ймовірність B відсутності очікування збільшується при зменшенні різниці потужності каналів. Використовуємо отримані результати при моделюванні трафіку ПД, при котрому можна говорити про сильну взаємодію між об'єднуваними окремими процесами, а конвергований трафік володіє властивостями довготривалої залежності (гіперболічна залежність основних параметрів об'єднаного трафіку) і масштабної інваріантності, тобто має фрактальний характер.

5.5. Визначення характеристик викидів агрегованого трафіку

При конвергенції трафіку від окремих джерел і отриманні агрегованого трафіку кількість викидів істотно збільшується, що ускладнює його сплайн-апроксимацію. Тому при управлінні ПД необхідно знати характеристики викидів. Відзначимо, що швидкість передачі інформації, котра є доступною для ПД, є стохастичним процесом $\xi(t)$ і має імовірнісний опис, причому по фізичних причинах завжди існує обмеження максимальної швидкості передачі [179]: $\xi_{\max} = \max \xi(t)$. Середня швидкість передачі інформації за час сеансу дорівнює:

$$m = M[\xi(t)] = \frac{1}{T} \int_0^T \xi(t) dt.$$

У мультисервісних мережах однією з основних характеристик трафіку, котра дозволяє оцінити необхідну пропускну спроможність окремих ланок мережі зв'язку, є берстність або коефіцієнт пачковості [175]:

$$B = \tau_{\max} / m, \tau_{\max} = \max \xi(t).$$

Проте дана характеристика не дає можливості оцінити швидкість розвитку випадкового процесу $\xi(t)$ за часом, оскільки не пов'язана з його спектральними, а, отже, кореляційними властивостями. Щоб врахувати часовий масштаб випадкової функції для опису швидкості передачі інформації введена ще одна характеристика трафіку – середній час пікової швидкості T_p , що визначається тривалістю викидів, для розрахунку котрої необхідно вибрати рівень вимірювань тривалості піку, що дозволить однозначно визначити:

- необхідний об'єм буферної пам'яті;
- оцінити джитер, тобто частоту пульсацій часу затримки.

Основні теоретичні положення базуються на теорії викидів випадкових процесів [178].

На рис. 5.5 наведена реалізація випадкового процесу $\xi(t)$ тривалістю T (наприклад, тривалість сеансу зв'язку).

Реальні випадкові процеси є безперервними функціями часу з обмеженим спектром внаслідок інерційних властивостей як самого джерела повідомлення, так і пристроїв обробки, котрі можна розглядати як фільтр низьких частот. Зокрема, такі поняття, як короткі і тривалі повідомлення, а також паузи між ними, є відносними і залежать від швидкодії засобів реалізації системи комутації.

Джерело трафіку вважається пульсуючим, якщо сумарний час на встановлення і роз'єднання крізного каналу менше інтервалу появи наступного повідомлення. Це дає підставу надалі при виведенні основних формул користуватися параболічною апроксимацією. Такі функції мають кінцеве число максимумів і мінімумів на обмеженому інтервалі часу T . Реалізація процесу $\xi(t)$ може кілька разів перетинати зазначений фіксований рівень (з позитивною похідною).

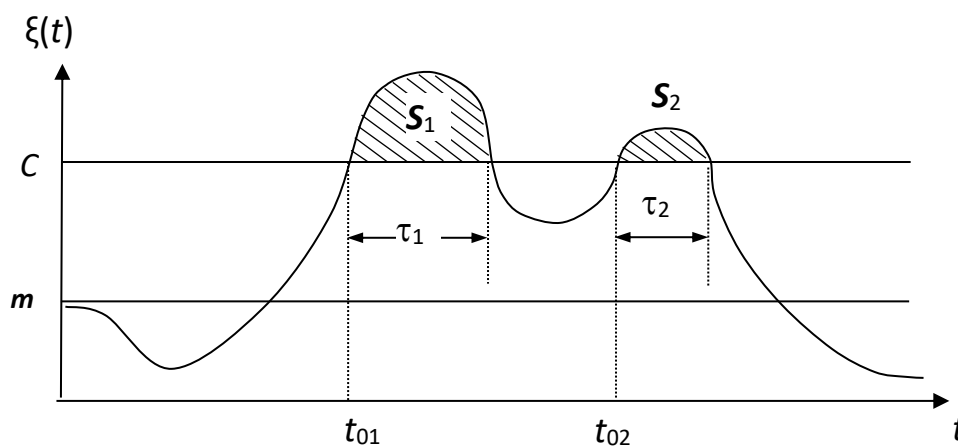


Рис. 5.5. Приклад реалізації випадкового процесу:

C – фіксований рівень; $\tau = \tau_1 + \tau_2$ – сумарна тривалість викидів;

$S = S_1 + S_2$ – сумарна площа викидів

Кількість таких перетинів відповідає кількості позитивних викидів випадкового процесу над рівнем C , для якого існує достатньо строгий математичний вираз [173]:

$$N^+(C, T) = \int_0^T dt \int_0^\infty \xi' \cdot f(C, \xi'; t) d\xi', \quad \xi' = \xi'(t),$$

де $f(\bullet)$ – функція щільності розподілу випадкового процесу

Для стаціонарних випадкових процесів наведена вище формула значно спрощується:

$$N^+(C, T) = f(C) \int_0^\infty \xi' \cdot f(\xi') d\xi'. \quad (5.32)$$

Вираз (5.32) дозволяє визначити середнє число викидів для довільного закону розподілу випадкового процесу. Якщо гаусів процес є стаціонарним, то середнє значення повного числа перетинів процесом рівня C в одиницю часу складе [173]:

$$N(C) = \frac{1}{\pi} \sqrt{-\rho_0''} \exp \left[-\frac{1}{2} \left(\frac{C - m}{\sigma} \right)^2 \right], \quad (5.34)$$

де ρ_0'' – друга похідна від коефіцієнта кореляції; σ – середньоквадратичне відхилення.

При достатньо високих рівнях $C \gg 0$ переважна частина викидів має малу тривалість і дорівнює кількості максимумів, які перевищують рівень C . випадковий процес $\xi(t)$, що гладко змінюється в невеликому околі максимуму (тобто є диференцуючим), як було показано вище, можна апроксимувати параболою.

Нехай t_0 – момент часу початку розглядаємого позитивного викиду, тобто:

$$\xi(t_0) = C, \quad \xi'(t_0) > 0.$$

Розкладемо функцію $\xi(t)$ в ряд Тейлора в околі точки t_0 і обмежимося квадратичним членом ряду:

$$\xi(t) \approx \xi(t_0) + \xi'(t_0)(t - t_0) + \frac{1}{2}\xi''(t_0)(t - t_0)^2. \quad (5.35)$$

Враховуючи, що при тривалості викиду τ $\xi(t_0) = \xi(t_0 + \tau) = C$, отримаємо:

$$\tau = -\frac{2\xi'(t_0)}{\xi''(t_0)}. \quad (5.36)$$

Застосувавши отримані співвідношення до нормального стаціонарного процесу з функцією кореляції $K(\tau) = \sigma^2 \cdot \rho(\tau)$ знайдемо щільність ймовірності тривалості викидів при достатньо великих позитивних рівнях C :

$$f(\tau, C) = \frac{1}{12\sqrt{\pi}}(-\rho_0'')\frac{C\tau}{\sigma} \exp\left[-\frac{1}{8}(-\rho_0'')\frac{C^2\tau^2}{\sigma^2}\right], \quad (5.37)$$

де $\rho_0'' = \rho''(t_0)$.

Параболічна апроксимація форми викидів дозволяє знайти розподіл викидів за площею:

$$S = \int_{t_0}^{t_0+\tau} [\xi(t) - C] dt. \quad (5.38)$$

З урахуванням виразу (5.36) і параболічного наближення викиду маємо:

$$S = \frac{2 \cdot (\xi'(t_0))^3}{3 \cdot (\xi''(t_0))^2}. \quad (5.39)$$

Скориставшись результатами [191] для нормального стаціонарного процесу, знайдемо щільність ймовірності розподілу викидів за площею, котрі перевищують рівень C :

$$f(S, C) = \frac{1}{3} \lambda^{2/3} S^{-1/3} \exp \left[-\frac{1}{2} (\lambda S)^{2/3} \right], \quad (5.40)$$

де
$$\lambda = \frac{2}{3} \frac{C^2}{\sigma^3} \sqrt{-\rho_0''}; C \gg \sigma. \quad (5.41)$$

Отримана формула (5.40) є надзвичайно важливою, оскільки площу викидів можна розглядати як об'єм буферної пам'яті у вузлах комутації, необхідний для того, щоб уникнути втрати пакетів за відсутності необхідного обчислювального ресурсу (рівень C в цьому випадку визначає максимально доступну швидкість передачі).

Затримані пакети можуть бути передані в моменти зниження інтенсивності трафіку нижче вказаного рівня, причому допустимий час затримки, очевидно, визначиться з вимог часової прозорості мережі, яка гарантує встановлену якість обслуговування абонента, що користується послугами відповідної служби.

Проведемо детальніший аналіз формули (5.40).

Нормована коефіцієнтом λ функція щільності ймовірності розподілу викидів за площею вище за рівень C нормального стаціонарного процесу представлена на рис. 5.6.

Визначимо середнє значення площі викидів:

$$S_{cp} = M[f(C, S)] = \frac{1}{3} \int_0^{\infty} S \lambda^{2/3} S^{-1/3} \exp\left[-\frac{1}{2}(\lambda S)^{2/3}\right] ds =$$

$$= \frac{1}{3} \lambda^{2/3} \frac{3}{2} \left(\frac{1}{2} \lambda^{2/3}\right)^{-5/2} \Gamma\left(\frac{5}{2}\right) = \sqrt{\frac{\pi}{2}} \cdot \frac{3}{\lambda},$$

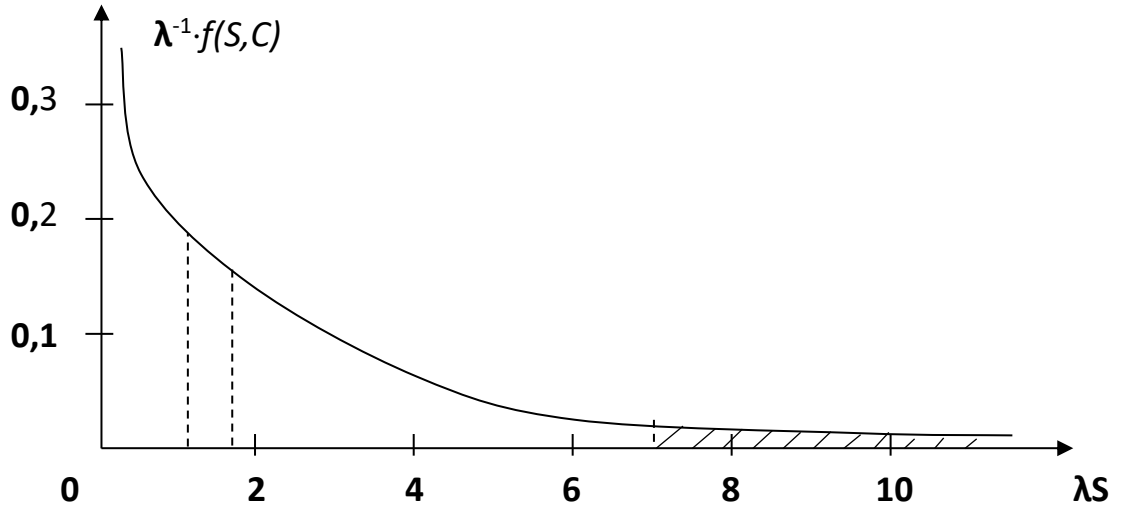


Рис. 5.6. Розподіл площі викидів

або із врахуванням (5.41):

$$S_{cp} = \sqrt{\frac{\pi}{2}} \frac{9\sigma^3}{2C^2 \sqrt{-\rho_0''}}. \quad (5.42)$$

Середнє значення тривалості викидів, які визначають додаткову затримку внаслідок зберігання надмірних комірок в буферній пам'яті, дорівнює:

$$\tau_{cp} = \frac{2\pi\sigma}{C \sqrt{-\rho_0''}}. \quad (5.43)$$

Коефіцієнти кореляції, типові для деяких процесів передачі даних, наведені в табл. 5.1 [173] (Δf_e – ефективна смуга частотного спектру розглядаємого трафіку).

Таблиця 5.1

Аналіз найбільш поширених коефіцієнтів кореляції

№	Коефіцієнт кореляції $\rho(t) =$		$-\rho_0''$	Частотний спектр коефіцієнта кореляції $S(f) =$	Δf_e	$\sqrt{-\rho_0''}$
1	$(1 + \alpha \tau) \times \exp(-\alpha \tau)$		α^2	$\frac{4\alpha^3}{(\alpha^2 + (2\pi f)^2)^2}$	$\alpha/8$	$8\Delta f_e$
2	$\exp(-\alpha\tau^2)$		2α	$\sqrt{\pi/\alpha} \exp\left(-\frac{\pi^2 f^2}{\alpha}\right)$	$0,5 \cdot \sqrt{\frac{\alpha}{\pi}}$	$\sqrt{8\pi/3} \cdot \Delta f_e$
3	$\left[1 + \alpha \tau \right] + \frac{1}{3} \times (\alpha\tau)^2 \exp(-\alpha \tau)$		$\frac{\alpha^2}{3}$	$\frac{16\alpha^5}{3} / (\alpha^2 + (2\pi f)^2)^3$	$(3/32)\alpha$	$\left(\frac{32}{3\sqrt{3}}\right) \cdot \Delta f_e$
4	$(1 + (\alpha\tau)^2)^{-1}$		$2\alpha^2$	$\frac{\pi}{\alpha} \cdot \exp\left(-\frac{2\pi f}{\alpha}\right)$	$\frac{1}{2\pi}\alpha$	$(2\pi\sqrt{2}) \cdot \Delta f_e$

Для прикладу розглянемо трафік мультимедійного потоку з коефіцієнтом кореляції $\rho(t) = \exp(-\alpha\tau^2)$ (рядок 2 табл. 5.1). Вирази (5.34), (5.37), (5.40) для нього набирають такого вигляду:

$$N(C) = A\Delta f_e \cdot \exp\left[-\frac{1}{2} \cdot \frac{(C-m)^2}{\sigma^2}\right]; \quad (5.44)$$

$$f(\tau, C) = \frac{1}{3\sqrt{\pi}} B \cdot \Delta f_e^2 \frac{C\tau}{\sigma} \cdot \exp\left[-\frac{1}{2} B \Delta f_e^2 \frac{C^2 \tau^2}{\sigma^2}\right]; \quad (5.45)$$

$$\lambda = D \frac{C^2}{\sigma^3} \Delta f_e, \quad (5.46)$$

де константи мають такі числові значення:

$$A = \sqrt{8/3}; \quad B = 2\pi/3; \quad D = 4\sqrt{2}\pi/(3\sqrt{3}).$$

Комбінацією виразів (5.43) і (5.44) можна знайти співвідношення між тривалістю і площею викидів:

$$S_{cp} = \frac{9}{4} \sqrt{\frac{1}{2\pi}} \frac{\sigma^2}{C} \tau_{cp} \quad (5.47)$$

Якщо площу S_{cp} зіставляти з необхідним об'ємом буферної пам'яті, то середній об'єм пам'яті $\bar{S}_\sigma$ через середній час пікового навантаження T_p розраховується таким чином:

$$\bar{S}_\sigma = k_p \cdot \frac{\sigma^2}{C} T_p, \quad (5.48)$$

де k_p – коефіцієнт перерахунку.

Проте на практиці навряд чи доцільно пов'язувати необхідний об'єм буферної пам'яті з середнім значенням площі викидів, оскільки це підсилює вимоги до системи зв'язку.

Рівень обмеження $C = C_n$ можна вибрати таким, щоб площа викидів з ймовірністю P_0 не перевищувала задану величину, сумісну з наявними ресурсами мережі.

На рис. 5.6 значень нижньої межі заштрихованої області визначимо як $(\lambda S)_n$ – ймовірність появи викидів з площею, яка перевищує задану величину.

Отже:

$$P_0(S) = P(S \leq S_n) = 1 - \int_{+S_n}^{\infty} f(S, C) ds = 1 - \exp\left(-\frac{1}{3} \lambda^{2/3} S_n^{2/3}\right), \quad (5.49)$$

де λ визначається формулою (5.43).

Криві залежності (5.49) при $\lambda = \text{Const}$ надані на рис. 2.7.

Вони дозволяють обчислити поріг, що визначає допустиму швидкість передачі, задаючись значеннями ρ_0 і S_n , по котрих параметр λ_n визначається однозначно згідно з таким виразом:

$$C_n = \sqrt{\frac{\lambda_n \sigma^3}{D \Delta f_e}} \quad (5.50)$$

При цьому поріг відлічується від середнього значення трафіку, тобто $C_n = C - m$ і відповідає геометричному місцю точок кривої (5.7), яка проходить через точку перетину прямих $P_0 = \text{Const}$ і $S_n = \text{Const}$.

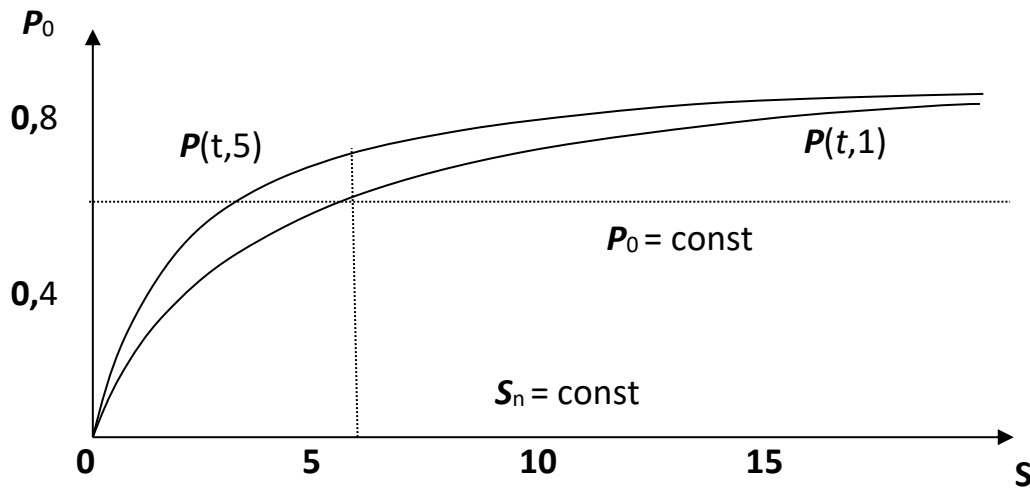


Рис.5.7. Залежність ймовірності P_0 від площі викидів

5.6. Фрактальна модель трафіку ІПД

Флуктуаційний характер трафіку інтегральних інформаційних потоків в інформаційно-телекомунікаційних мережах сприяє створенню локальних перевантажень навіть при обслуговуванні процесів, які сумарно не досягли номінальних значень. Хаотичний вплив трафіку на параметри мережі, що виникає в результаті його фрактального характеру, пред'являє додаткові вимоги до моделей трафіку [191]. У даному підрозділі проаналізовані процеси, які створюють трафік ІПД в ІТМ, виведені вирази для розрахунку фрактальної розмірності цих процесів, визначені їх спектральні особливості і розраховані основні характеристики.

5.6.1. Визначення фрактальної розмірності трафіку

Трафік, створюваний ІПД, описується випадковим процесом, який в загальному випадку має фрактальний характер з властивостями самоподібності і самоафінності (самоподібність при афінних перетвореннях) [191]. Дані властивості можна розглядати як в широкому, так і у вузькому сенсі, тобто самоподібними будуть нестационарні випадкові процеси, для яких одновимірна щільність ймовірності $w(x,t)$ зберігає свій вигляд при

узгоджений зміні масштабів змінних x та t , наприклад, для узагальненого вінерівського процесу:

$$w(b^{-H}x, bt) = b^{-H}w(x, t),$$

де $0 < H < 2$ (при $H = 1/2$ маємо стандартний вінерівський процес). Величину показника Херста H в [191] пропонується знаходити на основі моделі генератора фрактала. Зважаючи на складність побудови подібної конструкції часто простіше безпосередньо обчислити розмірність за визначенням фрактала. У [193] таким чином визначена розмірність корельованого гаусівського випадкового процесу за допомогою вирішення рівняння Ланжевена першого і другого порядку.

Розглянемо спосіб обчислення показника Херста H , що базується на метриці Хаусдорфа, обчислювальна складність якого менша, ніж в способах, запропонованих у [190].

Розмірність Хаусдорфа множини X визначимо наступним чином [189]. Введемо δ -покриття множини X як $K(\delta) = \{X_j, j = 1, 2, \dots\}$, де $X \subseteq \bigcup_j X_j$;

$0 < \text{diam}(X_j) \leq \delta \quad \forall j$; $\text{diam}(X_j)$ – діаметр множини.

Тоді міра Хаусдорфа s визначається величиною:

$$K_s(X) = \lim_{\delta \rightarrow 0} \left(\inf_{K(\delta)} \sum_j (\text{diam}(X_j))^s \right). \quad (5.51)$$

Згідно [166] для фракталів $K_s(x)$ існує та є хаусдорфова розмірність D_H множини X (одне з визначень фрактала – множина, хаусдорфова розмірність якої не співпадає з топологічною).

При визначенні розмірності самоподібності траєкторії випадкового процесу $X(t)$ допускається, що коефіцієнти при x та t у виразі щільності ймовірності $w(x, t)$ є однаковими, тобто траєкторія випадкового процесу покривається множинами, котрі мають однаковий характерний розмір по осях x і t , наприклад, квадратами. Тому:

$$\text{diam}(X_j) = |X(t_j) - X(t_{j-1})|,$$

тобто мірою Хаусдорфа (5.51) є s – довжина [189]:

$$K_s(X) \equiv L_s[X(t)] = \lim_{\delta \rightarrow 0} \alpha(s, \delta),$$

$$\alpha(s, \delta) = \inf \left[\sum_{j=1}^N |X(t_j) - X(t_{j-1})|^s \right] \text{ при } |t_j - t_{j-1}| < \delta, \quad (5.52)$$

де $N = T / \delta$ – кількість інтервалів дискретизації реалізації даного випадкового процесу за час спостереження T .

Для самоафінних процесів спроба визначення «штучної» розмірності самоподібності, тобто величини, яка не враховує властивостей процесу, призведе до деяких аномальних результатів [193]. В цьому випадку потрібно покривати траєкторію множинами, які враховують різні масштабні коефіцієнти по різних осях, наприклад, прямокутниками з розміром:

$$|X(t_j) - X(t_{j-1})| \times |t_j - t_{j-1}|^s.$$

тоді

$$K_s(X) = \lim_{\delta \rightarrow 0} b(s, \delta),$$

$$\text{де } b(s, \delta) = \inf \left(\left(\sum_{j=1}^k |X(t_j) - X(t_{j-1})| \cdot |t_j - t_{j-1}|^s \right)^{1/2} \right) \text{ при } |t_j - t_{j-1}|^{s/2} < \delta. \quad (5.53)$$

Розмірність D_H в обох випадках визначається як критичне значення s -переходу між нулем і нескінченністю величини $\langle K_s(X) \rangle$ – усередненої за ансамблем реалізацій міри Хаусдорфа [194]. Таким чином, розрахунок хаусдорфової розмірності D_H пов'язаний з обчисленням s -го абсолютного моменту приростів випадкового процесу.

Для випадкового гаусового процесу $X(t)$ з нульовим математичним сподіванням і кореляційною функцією $K(t_1, t_2)$ приросту:

$$\Delta X_j = X(t_j) - X(t_{j-1})$$

також мають нульове середнє і дисперсію, співпадаючу із структурною функцією процесу, тобто:

$$D[\Delta X_j] = K(t_j, t_j) + K(t_{j-1}, t_{j-1}) - 2 \cdot K(t_{j-1}, t_j) = \Psi(t_{j-1}, t_j) \equiv \Psi_{j-1, j}.$$

Далі розглядатимемо лише процеси, структурна функція яких має таку локальну поведінку:

$$\Psi(t, t + \delta) = A(t)\delta^\alpha + O(\delta^{\alpha+1}),$$

де $A(t)$ обмежена величиною M , а $0 < \alpha < 2$.

Оскільки:

$$\begin{aligned} \langle |\Delta X_j|^s \rangle &= \frac{2}{\sqrt{2\pi\Psi_{j-1, j}}} \cdot \int_0^\infty y^s \exp\left(-\frac{y^2}{2\Psi_{j-1, j}}\right) dy = \frac{2^{s/2+1}}{\sqrt{\pi}} \Gamma\left(\frac{s+1}{2}\right) \Psi_{j-1, j}^{s/2}; \\ \left\langle \sum_{j=1}^N |\Delta X_j|^s \right\rangle &= f(s) \sum_{j=1}^N \Psi_{j-1, j}^{s/2}, \end{aligned}$$

де $\Gamma(x)$ – гамма-функція, а функція $f(\cdot)$ залежить від s і не залежить від δ , то враховуючи (5.52) з точністю до співмножника, котрий залежить лише від s :

$$\alpha(s, \delta) \sim (\delta^\alpha)^{s/2} \cdot N \sim (\delta^\alpha)^{s/2} \cdot \delta^{-1} = \delta^{\frac{\alpha s}{2} - 1}.$$

Границя цього виразу при $\delta \rightarrow 0$ визначає $\langle K_s(X) \rangle$ у виразі (5.56) і є кінцевим лише при виконанні умови $\alpha s_0 / 2 - 1 = 0$, тобто $s_0 = 2 / \alpha$.

Отже, відповідно до раніше викладеного, для самоподібних процесів хаусдорфова розмірність дорівнює:

$$D_{Hc} = D_H = 2 / \alpha. \quad (5.54)$$

Аналогічні обчислення, що були проведені для хаусдорфової міри, котра задається співвідношенням (5.34), призвели до виразу:

$$\langle b(s, \delta) \rangle \sim \delta^{\alpha/2 \cdot 1/2} \cdot \delta^{s/2} \cdot N \sim \delta^{\alpha/4 + s/2 - 1},$$

тобто для самоафінних процесів хаусдорфова розмірність дорівнює:

$$D_{Ha} = D_H = 2 - \alpha / 2. \quad (5.55)$$

Далі розглянемо фрактальний броунівський рух (узагальнений вінерівський процес)

$$B_H(t) = \int_0^t (t - \tau)^{H-1/2} n(\tau) d\tau \quad (5.56)$$

де $n(\tau)$ – білий гаусів шум.

Відмітимо, що приріст величини $B_H(t)$ відбувається відповідно до виразу $|t_1 - t_2|^H$, $0 < H < 1$, а кореляційна функція має вигляд:

$$K_H(t_1, t_2) = \frac{t_1^{2H} + t_2^{2H} - |t_1 - t_2|^{2H}}{2}.$$

При $H = 1/2$ отримаємо вінерівський процес з приростом порядку $|t_1 - t_2|^{1/2}$ і кореляційною функцією:

$$K_{1/2}(t_1, t_2) = [t_1 + t_2 - |t_1 - t_2|] / 2 = \min(t_1, t_2).$$

Структурна функція $B_H(t)$ задається співвідношенням $\psi(t_1, t_2) = |t_1 - t_2|^{2H}$, тому $\psi(t, t + \delta) = \delta^{2H}$, $\delta > 0$, отже $\alpha = 2H$, тобто:

$$D_{Hc} = 1 / H; \quad D_{H\alpha} = 1 - H. \quad (5.57)$$

Зокрема для стандартного вінерівського процесу ($H = 1/2$) набуваємо загальновідомих значень, які інтерпретується як розмірність сліду багатовимірного броунівського руху [193]:

$$D_{Hc} = 2; \quad D_{H\alpha} = 3 / 2.$$

5.6.2. Фрактальні властивості трафіку ІПД з повторними запитами

Спираючись на результати, отримані в підрозділі 5.6.1, проведемо дослідження фрактальних властивостей трафіку ПІД з повторними запитами на прикладі об'єднаного трафіку служби передачі службової інформації і підсистеми обслуговування запитів (забезпечення розмови). Розглянемо модель, яка описує взаємодію цих підсистем.

Імовірнісні характеристики каналів передачі даних при певних припущеннях визначаються відношенням сигнал-шум і прийнятим способом кодування повідомлень (кодограмами). Помилки при передачі кодограм призводять до виникнення повторних запитів на обслуговування. Запити повинні реєструватися і обслуговуватися, тому повторні запити виникають при зайнятості пристрою реєстрації, який надалі вважатимемо одноканальним [200]. Структура даної підсистеми передачі службової інформації представлена на рис. 5.8.

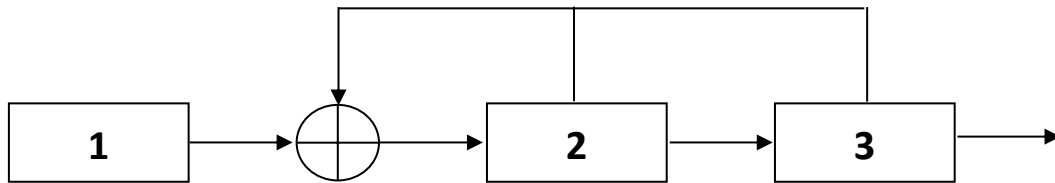


Рис. 5.8. Схема передачі службової інформації:

- 1 – джерело запитів на обслуговування (навантаження)
- 2 – приймач службової інформації
- 3 – одноканальний пристрій реєстрації запитів на обслуговування

Хай джерело 1 генерує пуассонівський потік первинних запитів з інтенсивністю λ , котрий обслуговується пристроєм реєстрації з часом реєстрації, розподіленим за експоненціальним законом з параметром $\mu = 1$. Якщо пристрій реєстрації зайнятий, то виникають повторні запити на обслуговування. Для опису поведінки абонента при відмові в обслуговуванні використовуємо модель, в котрій запит повторюється доти, поки не буде обслугований. Тоді кількість повторних запитів в одиницю часу задається співвідношенням:

$$Y = Y_1 \cdot Y_2,$$

де Y_1 – кількість джерел повторних запитів, а Y_2 – кількість запитів в одиницю часу, створюваних джерелом, що генерує пуассонівський потік з інтенсивністю ν . Кількість повторних запитів у момент часу t задається як:

$$Z(t) = \int_0^t Y(t-\tau) d\tau. \quad (5.58)$$

Для системи, представленої на рис. 5.8, можуть бути отримані динамічні рівняння для часової залежності середньої (за ансамблем) кількості обслугованих $x(t)$ і повторних $y(t)$ запитів в одиницю часу. На основі рівнянь для перехідної ймовірності [173] отримуємо закони збереження середніх значень кількості обслугованих і повторних запитів для системи з нульовими початковими умовами:

$$\begin{aligned} \dot{x} &= q\lambda - \nu y - x - (1+\nu) \left(\frac{x^2}{1-x} + \frac{p}{q} x \right); \\ \dot{y} &= -\nu y + (1+\nu) \left(\frac{x^2}{1-x} + \frac{p}{q} x \right); \\ x(0) &= 0, y(0) = 0, \end{aligned} \quad (5.59)$$

де p – ймовірність помилок при передачі службового повідомлення; $q = 1 - p$; λ і ν – інтенсивності потоків первинних і повторних запитів (враховуємо $\mu = 1$). Стаціонарне рішення системи рівнянь (5.59) виглядає таким чином:

$$x_c = q\lambda; \quad y_c = \frac{\nu+1}{\nu} \left(\frac{q^2 \lambda^2}{1-q\lambda} + p\lambda \right).$$

При $p \neq 0$ система (5.59) має єдину стаціонарну точку (аттрактор) у вузлі (x_c, y_c) при $0 < \nu < \infty$. Аналіз залежностей $x(t)$ і $y(t)$ в подвійному логарифмічному масштабі дозволяє використовувати такі наближені вирази:

$$x(t) \sim t^\beta (\beta \sim 1); \quad y(t) \sim t^\alpha (\alpha \sim 3).$$

Оцінимо фрактальну розмірність процесу $Z(t)$, задану виразом (5.58) при високій інтенсивності потоку запитів, що поступає. Оскільки кожне джерело повторних запитів генерує пуассонівський потік з інтенсивністю ν , то залежність кількості запитів від часу описується пуассонівським процесом.

При великих інтенсивностях він апроксимується дифузійним вінерівським процесом, а кількість запитів за малий інтервал часу (приріст вінерівського процесу) – гаусів білий шум і, отже $Y_2(t) \approx n(t)$, де $n(t)$ – імпульсна характеристика.

Якщо $Y_1(t)$ оцінимо математичним сподіванням кількості запитів $\overline{Y_1(t)}$, що надійшли в момент часу t , то враховуючи стаціонарність $n(t)$ в співвідношенні (5.58) можна використовувати інтеграл Дюамеля:

$$Z(t) = \int_0^t h(t-\tau) n(\tau) d\tau; \quad h(t) = \overline{Y_1(t)},$$

Рішення системи рівнянь (5.59) визначає перехідні процеси для системи з нульовими початковими умовами, проте по ним можна оцінити і характеристики перехідного процесу за будь-яких початкових умов.

Середня кількість повторних запитів у момент часу t зростає пропорційно $y(t)$ і убыває пропорційно $x(t)$ (за рахунок зростання кількості обслугованих запитів), тобто пропорційно $t^{\alpha-\beta}$. Тому середня кількість повторних запитів в одиницю часу (похідна) задає перехідну характеристику системи $g(t) \sim t^{\alpha-\beta-1}$.

Оскільки $h(t) = g'(t)$, то остаточно в умовах високої інтенсивності потоку запитів, що надходять, отримуємо:

$$Z(t) = \int_0^t (t-\tau)^{\alpha-\beta-2} n(\tau) d\tau. \quad (5.60)$$

де $Z(t)$ є процесом фрактального броунівського руху (5.37) з показником Херста (5.38) $H = \alpha - \beta - 3/2$ і хаусдорфовою самоафінною розмірністю $D_{Ha} = 2 - H$.

Система рівнянь (5.59) може бути вирішена чисельно. Наприклад, при $\nu = 10$, $\lambda = 0,75$, $\nu = 10$, $\mu = 1$ отримаємо: $\alpha \approx 2,86$, $\beta \approx 0,96$,

Запропоновані в даному підрозділі аналітичні вирази для визначення фрактальних характеристик трафіку інтегрального потоку використані при побудові моделі, що враховує властивість масштабної інваріантності відповідного процесу.

5.6.3. Фрактальна модель трафіку ІПД, що використовує властивість масштабної інваріантності

Для управління механізмами утворення віртуальних з'єднань необхідна розробка конструктивних математичних моделей мережевих процесів, що враховують фрактальний характер трафіку ІПД, що дозволяє надалі використовувати їх для розробки нових методів управління ІПД [186]. Використання властивості масштабної інваріантності фрактальних процесів дозволяє застосовувати різні імовірнісні методи для оперативного прогнозування процесів за допомогою моделей з мінімальною кількістю параметрів, що настраюються. Одним з параметрів фрактальних моделей таких процесів може бути кількість відліків при їхньої агрегації, коли починає виявлятися масштабна інваріантність. Для цілей дослідження важливою характеристикою таких процесів є їхня фрактальна розмірність, спосіб розрахунку котрої з використанням хаусдорфової міри наведений в підр. 5.6.1.

Пов'яжемо фрактальну розмірність з масштабом вимірювання його значень такою формулою [193]:

$$L(\delta) = a \cdot \delta^{1-D_H}, \quad (5.61)$$

де $L(\delta)$ – фрактальна міра процесу; δ – масштаб, що зіставляється вибраному вимірювальному елементу; a – коефіцієнт, що характеризує евклідову міру, котра може бути зіставлена даному процесу. Якщо величина D_H відмінна від одиниці, то значення $L(\delta)$ зростає зі зменшенням величини масштабу вимірювань δ .

Таким чином, $L(\delta)$ характеризує структуру процесу або об'єкту шляхом опису його властивостей за допомогою окремих складових, кожна з котрих в якомусь сенсі подібна до цілого. В результаті незалежно від масштабу спостереження процес виглядає однаково з погляду тих його характеристик, що володіють фрактальними властивостями. Так, інтенсивність трафіку в комп'ютерній мережі можна зміряти шляхом підрахунку кількості $N(\delta)$

пакетів, що надходять у період, заданий часовим інтервалом (базовим елементом) вибраної тривалості δ .

Введемо вимірювальний елемент вигляду $h(\delta) = \gamma(d)\delta^d$. В результаті міра множини вводиться як адитивна функція, котру можна записати як:

$$M_d = \sum_{h(\delta) \in H} h(\delta),$$

де H – множина вимірювальних елементів. У загальному випадку при $\delta \rightarrow 0$ міра M_d дорівнює нулю або нескінченності, що залежить від вибору параметра d – розмірності вибраної міри. Тому вираз для міри можна записати у вигляді:

$$M_d = \sum h(\delta) = \sum \gamma(d)\delta^d = \gamma(d)N(\delta)\delta^d \xrightarrow{\delta \rightarrow 0} \begin{cases} 0, d > D_H; \\ \infty, d < D_H. \end{cases} \quad (5.62)$$

Якщо $\Gamma(N)$ – коефіцієнт подібності, що дозволяє множину L накрити N множинами $L' = \Gamma(L)$, то розмірність подібності дорівнює:

$$D_S = -\ln N / \ln \Gamma(N). \quad (5.63)$$

Для фрактальних об'єктів, що володіють властивістю самоподібності, має місце рівність [200]:

$$D_H = D_S.$$

Простим фрактальним і самоподібним об'єктом, що почав використовуватися як модель складних процесів, є множина Кантора, для котрої після n -го етапу розбиття для відрізка завдовжки $\delta_i = (\xi)^n$ ($\xi = 1/3$):

$$M_d = N(\delta)\delta^d \xrightarrow{\delta \rightarrow 0} \lim_{n \rightarrow \infty} 2^n (1/\xi)^{n \cdot d}. \quad (5.64)$$

Така міра не розходиться, якщо $2^n (1/\xi)^{n \cdot d} = 1$, тому використовуючи (5.62) і (5.63), отримаємо, що $D_S = D_H = -\ln 2 / \ln(1/3) = \ln 2 / \ln 3$.

Для побудови моделі мережних процесів узагальнимо отримані результати на випадок, коли у якості об'єкту досліджень обраний часовий інтервал довільної тривалості t . Нехай відповідно до прийнятої умови нормування на цьому інтервалі задана деяка відносна щільність початкових станів ρ_0 . Тоді «відносна маса» всього інтервалу дорівнює добутку $\rho_0 \cdot t$.

Розділимо даний інтервал на три складові і видалимо середню частину. На кінцях інтервалу залишиться два відрізки довжиною ξt ($\xi < 1/2$). Координати точок після першого поділу дорівнюють $[0, \xi t]$ і $[t(1-\xi), t]$. Щільність станів, що залишилися, збільшимо таким чином, щоб "маса" всього інтервалу не змінилася. В цьому випадку щільність станів буде дорівнювати величині $1/(2\xi t)$. На другому етапі ділення кількість даних точок зростає до восьми, а їхні координати в порядку зростання визначають таку послідовність відрізків: $[0, \xi^2 t]$, $[(\xi(1-\xi)t, \xi t]$, $[t(1-\xi), t(1-\xi + \xi^2)]$, $[t(1-\xi^2), t]$.

Щільність станів на цих відрізках, виходячи з умови нормування, визначається виразом $1/(2\xi^2 t)$. Довжини отриманих відрізків рівні, а їхня «відносна маса» обчислюється як:

$$\mu_i = \ell_i^v = \left(t \cdot \xi^2\right)^{\ln 2 / \ln(1/\xi)} = t \cdot \left(\frac{1}{\xi}\right)^{-2 \cdot \ln(1/2) / \ln(1/\xi)} = t \cdot \left(\frac{1}{2}\right)^2, \quad (5.65)$$

де ℓ_i – довжина відрізання, $v = \ln 2 / \ln(1/\xi)$ – фрактальна розмірність даної множини станів, а щільність кожного з відрізків (станів), що залишилися, дорівнює:

$$\rho_i = \frac{\mu_i}{\ell_i} = \rho_0 \ell_i^{v-1}. \quad (5.66)$$

Показник μ_i може бути мірою будь-якого процесу, що має своїм носієм множину Кантора, з його допомогою можна отримати залежність «маси» деякого об'єкту при зміні його довжини в інтервалі $[0, x]$ у вигляді такого співвідношення:

$$M(x) = \int_0^x \rho(t) dt = \int_0^x d\mu(t).$$

Використовуючи описані вище властивості канторівської множини, представимо характер зміни станів деякого процесу, наприклад, зміни кількості пакетів, переданих по лінії зв'язку з постійною інтенсивністю $\lambda=1$, за допомогою функції $f(t)$. Для $r_L t$ частини огинає виконується рівність $f(r_L t) = \frac{1}{N} f(t)$. Проте, при розбитті інтервалу спостереження з використанням елементів канторівської множини ця рівність перетворюється на тотожність, якщо виконується умова:

$$1/3^2 = (1/2^2)^{1/\beta}, \quad \beta = \ln 2 / \ln 3.$$

Аналогічно для n -го етапу розбиття отримаємо $(1/3^n)^\beta = 1/2^n$, що призводить до значення $\beta = \ln 2 / \ln 3$, котре співпадає з розмірністю подібності для канторівської множини при $\xi = 1/3$. У загальному випадку задача побудови моделі процесу полягає у визначенні огинаючої функції $f(t)$, котра задовольняє рівнянню $f(r_L t) = \frac{1}{N} f(t)$, нетривіальне рішення якого має вид степеневі функції :

$$f(t) = A_\beta t^{-\beta}, \quad \beta = \ln N / \ln r_L,$$

що дозволяє визначити клас моделей, за допомогою котрих можна кількісно характеризувати прояви властивості масштабної інваріантності.

Розглянемо модель мережевих процесів, для котрих має місце втрата окремих пакетів. Ці процеси можна назвати процесами з неповною пам'яттю, в основі котрих лежать властивості розглянутої вище фрактальної канторівської множини. Зв'язок між вхідним і вихідним сигналами задається інтегралом згортки:

$$u(t) = \int_0^t h(t-\tau) f(\tau) d\tau, \quad (5.67)$$

де $h(t)$ – імпульсна перехідна функція, котра характеризує вплив на вихідну координату $u(t)$ об'єкту всіх значень вхідного сигналу $f(\tau)$ для $0 \leq \tau < t$. Проте, якщо в якості $h(t)$ використовувати дельта-функцію Діраку, то співвідношення (5.67) призводить до тривіальної рівності $u(t) = f(t)$, що характеризує властивості об'єкту, в якому відсутня пам'ять або який-небудь вплив на його стан сигналу $f(\tau)$ $0 \leq \tau < t$.

Визначимо імпульсну перехідну функцію вигляду:

$$h(\tau) = \begin{cases} 1/t, & 0 \leq \tau \leq t, \\ 0, & \tau < 0; \tau > t, \end{cases} \quad (5.68)$$

яка задовольняє умові нормування $\int_0^t h(\tau) d\tau = 1$. Тоді процесу $u(t)$ на виході системи з повною пам'яттю відповідає процедура усереднювання на інтервалі:

$$u(t) = \frac{1}{t} \int_0^t f(\tau) d\tau. \quad (5.69)$$

Таким чином, типовою операцією обробки результатів вимірювань є ковзаюче згладжування вигляду $X_T(t) = \frac{1}{T} \int_{t-T}^t \xi(\tau) d\tau$.

Обчислимо моменти і спектральну щільність процесу $X_T(t)$, за умови, що $\xi(t)$ – стаціонарний в широкому сенсі випадковий процес з математичним сподіванням m_ξ , кореляційною функцією $C_\xi(\tau)$ і спектральною щільністю $F_\xi(\omega)$. Тоді:

$$m_{X_T}(\tau) = M \{X_T(t)\} = \frac{1}{T} \int_{t-T}^t m_\xi d\tau = m_\xi,$$

а кореляційна функція має вигляд:

$$C_{X_T}(\tau) = M \left\{ \left(X_T(t) - m_{X_T} \right) \left(X_T(t+\tau) - m_{X_T} \right) \right\} = \frac{1}{T^2} \int_{t-T}^t \int_{t-T+\tau}^{t+\tau} C_{\xi}(u_1 - u_2) du_1 du_2.$$

Оскільки процес $\xi(\tau)$ має спектральну щільність $F_{\xi}(\omega)$, то:

$$C_{\xi}(u_1 - u_2) = \frac{1}{2\pi} \int_{-\infty}^{\infty} F_{\xi}(\omega) \exp\{j\omega(u_1 - u_2)\} d\omega.$$

Тому вираз для кореляційної функції процесу $X_T(t)$ представимо як:

$$\begin{aligned} C_{X_T} &= \frac{1}{2\pi T^2} \int_{-\infty}^{\infty} F_{\xi}(\omega) \int_{t-T}^t \exp\{-j\omega u_2\} du_2 \int_{t-T+\tau}^{t+\tau} \exp\{-j\omega u_1\} du_1 = \\ &= \frac{1}{2\pi T^2} \int_{-\infty}^{\infty} F_{\xi}(\omega) \left[\frac{1}{j\omega} e^{-j\omega u_2} \right]_{u_2=t-T}^{u_2=t} \cdot \left[\frac{1}{j\omega} e^{j\omega u_1} \right]_{u_1=t-T}^{u_1=t+\tau} d\omega = \\ &= \frac{1}{2\pi T^2} \int_{-\infty}^{\infty} F_{\xi}(\omega) \left[-\frac{1}{j\omega} e^{-j\omega T} (1 - e^{j\omega T}) \right] \cdot \left[\frac{1}{j\omega} e^{j\omega(t+\tau)} (1 - e^{j\omega T}) \right] d\omega = \\ &= \frac{1}{2\pi T^2} \int_{-\infty}^{\infty} F_{\xi}(\omega) \frac{1}{j\omega^2} e^{-j\omega\tau} (1 - e^{j\omega T}) d\omega. \end{aligned}$$

Зважаючи на формулу Ейлера, отримаємо:

$$C_{X_T}(\tau) = \frac{1}{2\pi} \int_{-\infty}^{\infty} F_{\xi}(\omega) \frac{2(1 - \cos \omega T)}{\omega^2 T^2} e^{j\omega\tau} d\omega = \frac{1}{2\pi} \int_{-\infty}^{\infty} F_{\xi}(\omega) \left(\frac{\sin \omega T / 2}{\omega T / 2} \right) e^{j\omega\tau} d\omega.$$

Отже, вираз для кореляційної функції процесу $X_T(t)$ є таким:

$$C_{X_T}(\tau) = \frac{1}{2\pi} \int_{-\infty}^{\infty} F_{\xi}(\omega) \left(\frac{\sin \omega T / 2}{\omega T / 2} \right) e^{j\omega\tau} d\omega,$$

тому спектральна щільність початкового $\xi(t)$ і агрегованого $X_T(t)$

процесів зв'язані співвідношенням $F_{X_T}(\omega) = F_{\xi}(\omega) \left(\frac{\sin \omega T / 2}{\omega T / 2} \right)^2$.

Відмітимо, що функція $\frac{\sin \omega T / 2}{\omega T / 2}$ має найбільше значення при малих значеннях $\omega T / 2$. Тому така операція агрегації пригнічує високочастотні складові початкового сигналу і сприяє прояву низькочастотних або протяжних статистичних залежностей.

Проведемо подальші перетворення, для чого підставимо в отримане співвідношення для C_{X_T} вираз для спектральної щільності:

$$F_{\xi}(\omega) = \int_{-\infty}^{\infty} C_{\xi}(u) \exp\{-j\omega u\} du.$$

В результаті після зміни порядку інтеграції отримаємо новий вираз:

$$\begin{aligned} C_{X_T} &= \frac{1}{2\pi} \int_{-\infty}^{\infty} F_{\xi}(u) du \int_{-\infty}^{\infty} \exp\{-j\omega u\} \left(\frac{\sin \omega T / 2}{\omega T / 2} \right)^2 \exp\{j\omega \tau\} d\omega = \\ &= \frac{1}{2\pi} \int_{-\infty}^{\infty} C_{\xi}(u) du \int_{-\infty}^{\infty} \exp\{j\omega(\tau - u)\} \left(\frac{\sin \omega T / 2}{\omega T / 2} \right)^2 \exp\{j\omega \tau\} d\omega. \end{aligned}$$

Для обчислення цього виразу зробимо заміну змінних $\tau - u = \lambda$. Внутрішній інтеграл в отриманому виразі для:

$$J = \frac{1}{2\pi} \int_{-\infty}^{\infty} \exp\{j\omega \lambda\} \left(\frac{\sin \omega T / 2}{\omega T / 2} \right)^2 d\omega = \frac{1}{T^2} \cdot c \int_{-\infty}^{\infty} \cos(\omega \lambda) \left(\frac{\sin \omega T / 2}{\omega T / 2} \right)^2 d\omega$$

є табличним. Для його обчислення використовуємо те, що інтеграл

$$J_1 = c \int_0^{\infty} f(\omega) \cos(\omega \lambda) d\omega \text{ при } f(\omega) = \sin^2(a\omega) / \omega^2 \text{ дорівнює:}$$

$$J_1 = \begin{cases} c^{-1} \left(a - \frac{1}{2} \lambda \right) & \lambda < 2a \\ 0 & \lambda > 2a. \end{cases}$$

Остаточний вираз для кореляційної функції набере вигляду:

$$C_{X_T} = \frac{1}{T^2} \int_{-T}^T (T - |u|) C_{\xi}(\tau - u) du.$$

Зіставимо інтервалу, на якому обчислюється імпульсна перехідна функція, процедуру побудови канторівської множини з параметром $\xi = 1/3$. Тоді після першого етапу ділення координати станів, що залишилися, будуть рівні $(0, \xi t)$ $(2\xi t, t)$ $2\xi t$. З урахуванням умови (5.65) щільність цих станів повинна змінитися і буде рівна $1/2\xi t$. На наступному етапі розбиття щільність станів, що залишилися, обчислюється за формулою $1/(2\xi)^2 t$.

На n -му етапі отримаємо 2^n підінтервалів завдовжки $\xi^n t$ з координатами $(t_m^{(n)}, t_m^{(n)} + \xi^n t)$, де $m = 1, \dots, 2^n$, $t_m^{(n)}$ – початкова координата інтервалів, що залишилися. Щільність станів, що залишилися, визначається виразом $1/(2\xi)^n t$, тому інтеграл (5.69) можна записати у вигляді:

$$u(t) = \frac{1}{(2\xi)^n t} \cdot \int_0^t f(\tau) \left[e\left(t_m^{(n)} \leq \tau < t_m^{(n)} + \xi^n t\right) \right] d\tau,$$

де одинична функція задається виразом:

$$e\left(t_m^{(n)} \leq \tau < t_m^{(n)} + \xi^n t\right) = \begin{cases} 1, & \tau \in \left(t_m^{(n)}, t_m^{(n)} + \xi^n t\right) \\ 0, & \tau < t_m^{(n)}, \tau \geq t_m^{(n)} + \xi^n t. \end{cases}$$

Після граничного переходу $n \rightarrow \infty$ отримаємо вираз інтеграла згортки на канторівській множині [199] у вигляді співвідношення:

$$u(t) = B_{\xi} \cdot \frac{1}{\Gamma(\beta)} \cdot \frac{1}{t^{\beta}} \int_0^t (t - \tau)^{\beta-1} f(\tau) d\tau, \quad (5.70)$$

де $\beta = \ln 2 / \ln 3$ – фрактальна розмірність канторівської множини, $\Gamma(\beta)$ – гамма-функція від аргументу β , B_{ξ} – константа, залежна від характеристики канторівської множини. Співвідношення (5.70) є однією із форм запису операції дробового інтегрування [188]. Запишемо (5.70) у формі інтеграла згортки:

$$u(t) = \int_0^t h(t - \tau) f(\tau) d\tau, \quad (5.71)$$

де $h(t) = kt^{\beta-1}$ – імпульсна перехідна функція, $k = B_{\xi} \Gamma^{-1}(\beta) t^{-\beta}$ – константа нормування.

Зміна форми запису інтеграла при збереженні значення обумовлена тим, що стан системи змінюється не на всьому безперервному інтервалі, а лише в точках не усюди щільної або фрактальної канторівської множини. В результаті при побудові моделі системи з неповною пам'яттю інтеграл (5.69) замінюється на інтеграл від функції, помноженої на нескінченну послідовність δ -функцій з координатами в точках канторівської множини, сумарна інтенсивність котрих дорівнює одиниці. У результаті значення (5.71) визначається сумою нескінченної кідькості нескінченно малих стрибків функції $f(\tau)$ в точках канторівської множини.

Повернемося до передграничного випадку. Розглянемо вираз:

$$\int_0^t f(\tau) \left[1 \left(t_m^{(n)} \leq \tau < t_m^{(n)} + \xi^n t \right) \right] d\tau, \quad (5.72)$$

котрому відповідає інтеграл вигляду:

$$\phi(t) = \int_0^t f(\tau) d\tau. \quad (5.73)$$

Порівнюючи (5.69) і (5.73), отримаємо $\phi(t) = t \cdot u(t)$. У свою чергу, помножаючи (5.70) на t^β , тобто обчислюючи $t^\beta \cdot u(t)$, отримаємо:

$$\phi_k(t) = \int_0^t k_1 \cdot (t - \tau)^{\beta-1} f(\tau) d\tau, \quad (5.74)$$

де $k_1 = B_\xi \Gamma^{-1}(\beta)$ – коефіцієнт нормування. Відмітимо, що отриманий вираз для коефіцієнта k_1 може бути використаний для побудови моделі процесів, якщо на інтервалі інтеграції $f(\tau)$ є постійною величиною. В цьому випадку значення дробового інтеграла (5.74) на інтервалі $[0, t]$ менше значення інтеграла (5.73) на цьому ж інтервалі, оскільки $\beta = \ln 2 / \ln 3 < 1$. Дана властивість отриманої моделі процесів є наслідком втрати частини станів на елементах фрактальної канторівської множини. Стосовно мережевого трафіку це означає, що для досягнення певного об'єму переданих даних, інтеграл (5.74) повинен обчислюватися в ширших часових межах. В цьому випадку права межа границі інтегрування буде дорівнювати $t^{1/\beta}$. Таким чином, процеси, відповідні операції дробового інтегрування, стають як би протяжнішими, а швидкість їх зміни описується інтегральними співвідношеннями дробового порядку.

В результаті, якщо для передачі файлу в каналі зв'язку з постійною інтенсивністю λ пакетів в секунду потрібно t секунд, то об'єм файлу дорівнює $x = \lambda t$, а $f(\tau) = \lambda$. Використання моделі з неповною пам'яттю дозволяє врахувати, що частина пакетів в процесі передачі може бути втрачена. Тому втратам пакетів зіставимо фрактальну канторівську множину з параметром ξ . Тоді на першому етапі побудови моделі каналу з втратами кількість переданих пакетів можна оцінити величиною $\lambda(2 \cdot \xi)^n t$, а втрачених пакетів – значенням $\lambda t [1 - (2\xi)^n]$. Після граничного переходу, коли $n \rightarrow \infty$, кількість пакетів, переданих через канал, буде дорівнювати:

$$x_k = \int_0^t k_1 \cdot (t - \tau)^{\beta-1} f(\tau) d\tau,$$

де $f(\tau) = \lambda$ – інтенсивність посилки пакетів, а $k_1 = B_\xi \Gamma^{-1}(\beta)$.

Ввівши нові змінні $t - \tau = y$ і $f(\tau) = \lambda$, отримаємо:

$$x_k = \lambda t^\beta \int_0^t k y^{\beta-1} dy. \quad (5.75)$$

Враховуючи умову нормування у виразі (5.75) отримаємо, що кількість переданих пакетів λt^β менше кількості посланих – λt , отже, на передачу втрачених пакетів, наприклад, за допомогою протоколу TCP, необхідно витратити додатковий час $t^{1/\beta} - t$.

Отже, використання властивостей масштабної інваріантності при моделюванні мережевого трафіку дозволяє побудувати адекватну модель мережевого процесу, ініційовану фрактальним трафіком, в котрому втрати пакетів компенсуються збільшенням часу передачі повідомлень, що призводить до формування протяжних статистичних часових залежностей. У отриманій моделі вплив втрат і причина появи протяжних залежностей формально враховані за допомогою введення операції дробового інтегрування. Проте, для практичного використання такої моделі необхідно ідентифікувати значення параметра, кількісно характеризуючих властивості масштабної інваріантності мережних процесів.

5.7. Модель процесу буферизації при управлінні трафіком інтегральних потоків даних

При управлінні трафіком інфокомунікаційних мереж необхідно враховувати, що у багатьох випадках управління віртуальним з'єднанням мережі зводиться до усунення перевантажень і подальшого відновлення його початкового стану [160]. Управління TCP-з'єднанням є важливою функцією контролю цілісності даних і захисту мережних застосунків від несанкціонованого доступу. Такий контроль можна здійснювати шляхом завдання правил фільтрації трафіку, який проходить крізь мережні інтерфейси комунікаційного устаткування інфокомунікаційних мереж. Оскільки в цьому випадку статистичне мультиплексування мережних потоків відбувається в буферах мережі, виділених для контролю з'єднання, то для усунення впливу алгоритмів фільтрації на продуктивність мережі потрібна

розробка спеціальних процедур буферизації і налагодження параметрів програми управління. Особливе це актуально у разі одночасного контролю за станом декількох ПД, наприклад, при їх інтерактивній взаємодії, коли мережна адреса джерела даних одного з них співпадає з мережною адресою вузла, який генерує пакети підтвердження для іншого потоку [162]. В цьому випадку сегменти першого ТСП-з'єднання передаються в одному напрямі разом з пакетами підтвердження про успішну доставку сегментів ТСП, утворених другим з'єднанням. В результаті пакети підтвердження потрапляють в загальний буфер з ТСП-сегментами і залежно від прийнятих правил фільтрації і буферизації можуть в різній послідовності перенаправлятися до даних віртуальних з'єднань [163]. Порухення встановленої черговості прибуття пакетів підтвердження і відправлення сегментів ТСП зменшує ефективну пропускну спроможність каналу, а процедура проміжної фільтрації може ще в більшій мірі підсилити ситуацію і навіть призвести до розриву віртуального з'єднання, тому необхідна розробка математичної моделі процесу заповнення буферів фільтрації при використанні відповідного комунікаційного устаткування [164].

Для визначення необхідного розміру буфера фільтрації розглянемо сегмент, що складається з двох вузлів з номерами i та j , які обмінюються між собою повідомленнями за допомогою ТСП-з'єднання. Стандартний алгоритм управління встановлює первинний розмір вікна передачі рівним одиниці і після прибуття кожного пакету підтвердження додає два ТСП-сегменти до початкової черги інтерфейсного буфера. У сучасних реалізаціях ТСП-протоколів два сегменти, отримані після прибуття підтвердження, будуть передані в канал раніше, ніж в початкову чергу потраплять пакети підтвердження про прибуття сегментів з протилежного напрямку [165]. Коли ці пакети підтвердження будуть отримані і між ними не буде ТСП-сегментів від іншого джерела, то в чергу будуть відправлені вже чотири ТСП-сегменти. У сформованій таким чином послідовності сегментів не буде місця пакетам підтвердження, які опиняться в черзі після сегментів даних. Таким чином, використання стандартних механізмів управління ТСП-з'єднанням призводить до втрати пакетів підтверджень за наявності зустрічних потоків даних. Цей ефект може ще більше посилитися у разі несиметричного каналу зв'язку.

Сегменти даних і пакети підтвердження, які передаються через ТСП-з'єднання в одному з напрямів, обробляються в загальній FIFO-очереди [166]. Нехай ρ_i – швидкість передачі з'єднання i , а ρ_j – з'єднання j , D_{ij} – складова затримки при передачі ТСП-сегмента від вузла i до вузла j . З метою спрощення

аналізу припустимо, що всі ТСП-сегменти мають однаковий розмір, а продуктивність транспортного протоколу така, що дані обробляються у вузлах мережі миттєво. Для опису процесу втрати пакету підтвердження позначимо розміри ТСП-окон відповідних з'єднань як W_i і W_j . Тоді умови виникнення втрати пакетів підтверджень можна записати у вигляді нерівності:

$$W_i / \rho_i + W_j / \rho_j > D_{ij} + D_{ji}. \quad (5.76)$$

Позначимо інтервал часу, в перебігу якого вузол i передає свої ТСП-сегменти, як $t[i]$ (оскільки час передачі пакету підтвердження істотно менше $t[i]$, то їм можна нехтувати). Позначимо черги ТСП-сегментів у вузлах i та j відповідно як $Q_i(t)$ і $Q_j(t)$. Розглянемо k -й інтервал передачі ТСП-сегментів вузлом i , позначивши його як $t[i, k]$. Цей час відповідає моменту, коли перший сегмент k -го інтервалу досягне вузла j [177].

Нехай $W_i - W_j > \rho_i \cdot D_{ij} + \rho_j \cdot D_{ji}$, тоді $t[i, r+1] = t[i, k] + W_i / \rho_i$. Дійсно, коли перший сегмент, відправлений з i -го вузла в k -й період передачі досягне вузла j , то він буде поміщений до черги $Q_j(t[i, k])$. Тому пакет підтвердження буде відправлений з вузла j у момент часу $t[i, k] + Q_j(t[i, k]) / \rho_j$ і досягне вузла i у момент часу $t_1 = t[i, k] + Q_j(t[i, k]) / \rho_j + D_{ji}$.

У вузлі i є власна початкова черга. Її розміри визначаються тим, що початок передачі першого сегменту в k -й період доводиться на момент часу $t[i, k] - D_{ij}$, тому коли перший пакет підтвердження повернеться до вузла i , з нього буде послано $\rho_i(t_1 - (t[i, k] - D_{ij})) = W_i - W_j > \rho_i \cdot D_{ij} + \rho_j \cdot D_{ji}$ сегментів. Оскільки кожен період передачі у вузлі i містить W_i сегментів, то його початкова черга має $Q_i(t_1) = W_i - Q_i(t[i, k]) + \rho_i \cdot D_{ij} + \rho_j \cdot D_{ji}$ сегментів на момент прибуття першого пакету підтвердження. Оскільки всі пакети підтвердження з'єднання j повернуться у вузол j як група пакетів і вузол i завжди має дані для передачі, тобто $Q_i(t_1) > 0$, то наступний період передачі почнеться у момент часу $t_1 + Q_i(t_1) / \rho_i$, а перший пакет досягне вузла j через час D_{ij} . Таким чином $t[i, k+1] = t_1 + Q_j(t_1) / \rho_j + D_{ij}$, звідкіля, можна отримати, що $t[i, k+1] = t[i, k] + W_i / \rho_i$, а для вузла j $t[j, k+1] = t[j, k] + W_j / \rho_j$.

Тепер можна визначити вираз для величини черги у вузлі j :

$$Q_j(t[i, k + 1]) = \min\{((W_i + W_j) - (\rho_i \cdot D_{ij} + \rho_j \cdot D_{ji}) - Q_j(t[i, k])), W_i\}, \quad (5.77)$$

з якого виходить оцінка максимального розміру черги, обмежена значенням:

$$\min\{((W_i + W_j) - (\rho_i \cdot D_{ij} + \rho_j \cdot D_{ji})), W_i\}. \quad (5.78)$$

Дійсно, коли перший сегмент $(k + 1)$ -го періоду передачі i -го вузла досягне вузла j , то в ньому існуватиме черга розміром $Q_j(t[i, k + 1])$. Ця черга утворилася в результаті прибуття до вузла j пачки пакетів підтверджень перед моментом початку $(k + 1)$ періоду передачі, тобто $t[i, k + 1]$. Припустимо, що ці пакети підтверджують прибуття сегментів, відправлених у m -й період передачі вузлом j . Позначимо як $t[j, m]$ час, коли перший сегмент в m -й період передачі j -го вузла досягнув вузла i . Величину $t[j, m]$ можна визначити через значення $t[i, k]$. У момент $t[i, k]$ вузол j передав $W_i - Q_j(t[i, k])$ сегментів, які відносяться до його m -го періоду передачі. Тому період передачі почався у момент часу $t[i, k] - (W_i - Q_j(t[i, k])) / \rho_j$, а оскільки перший сегмент досягне вузла i опісля D_{ji} , то $t[j, m] = t[i, k] - (W_i - Q_j(t[i, k])) / \rho_j + D_{ji}$. Вузол i завершує свій k -й період передачі в момент часу $t_2 = t[i, k] - D_{ji} + W_i / \rho_i$. Тому в період часу між $t[j, m]$ та t_2 вузол i отримує ТСП-сегменти від вузла j , які були згенеровані в m -й період передачі. При цьому початкова черга у вузлі j залишається непорожньою, формуючи угруповання пакетів підтвердження, які вузол i відправляє вузлу j . Кількість таких пакетів підтвердження на інтервалі $(t[j, m], t_2)$ визначається значенням $\min\{(t_2 - t[j, m]), W_i\}$, тому:

$$\rho(t_2 - t[j, m]) = (W_i + W_j - (\rho_i D_{ij} + \rho_j D_{ji}) - Q_j(t[i, k])). \quad (5.79)$$

При прибутті першого сегменту $(k + 1)$ періоду передачі i -го вузла розмір черги у вузлі j визначиться як:

$$Q_j(t[i, k + 1]) = \min\{W_i + W_j - (\rho_i D_{ij} + \rho_j D_{ji}) - Q_j(t[i, k]), W_i\}, \quad (5.80)$$

що співпадає з попередньою оцінкою. Використовуючи цей результат і

обчислюючи вираз для $Q_j(t[i, k + 2])$ на основі $Q_j(t[i, k + 1])$ отримаємо:

$$Q_j(t[i, k + 2]) = Q_j(t[i, k]). \quad (5.81)$$

Враховуючи періодичний характер зміни черги, можна обчислити інтервал часу між періодами передачі і на цій основі оцінити ефективність роботи віртуального каналу. Якщо виконується умова:

$$W_j - (\rho_i D_{ij} + \rho_j D_{ji}) < W_i < W_j + (\rho_i D_{ij} + \rho_j D_{ji}), \quad (5.82)$$

то
$$t[i, k + 2] - t[i, k] = (W_i / \rho_i + W_j / \rho_j) / + D_{ij} + D_{ji}.$$

Дійсно, нехай t_3 – момент часу, коли перший пакет підтвердження для k -го періоду передачі даних з вузла i повернувся назад в цей вузол, тобто $t_3 = t[i, k] + Q_j(t[i, k]) / \rho_j$. Якщо черга у вузлі i існує, тобто передача сегментів k -го періоду ще не закінчена, то $W_i / \rho_i > t_3 - t[i, k] - D_{ij}$. Зважаючи на вираз для t_3 , отримаємо, що $W_i > (\rho_i D_{ij} + \rho_j D_{ji}) + Q_j(t[i, k])$. Вузол i продовжуватиме передачу сегментів в стислих пакетах підтвердження. Передача першого сегменту, який відноситься до $(k+1)$ -го періоду їх генерації вузлом i почнеться у момент часу $t[i, k] + W_i / \rho_i - D_{ij}$ та завершиться при $t_4 = t[i, k] + 2W_i / \rho_i - D_{ij}$. Перший сегмент досягне вузла j в момент $t[i, k + 1] = t[i, k] + W_i / \rho_i$. Оскільки сегменти сліднують за стислими пакетами, підтверджуючими W_j сегментів, відправлених з вузла j , то перший пакет прибуде в буфер j -го вузла, в якому знаходиться $Q_j(t[i, k]) = W_i$ сегментів. Тому перший пакет підтвердження буде відправлений до моменту $t[i, k + 1] + W_i / \rho_i$ і досягне вузла i у момент часу $t_5 = t[i, k + 1] + W_i / \rho_i + D_{ij}$. Оскільки $t_5 > t_4$, то вузол i до цього часу завершить передачу, і тоді:

$$\begin{aligned} t[i, k + 2] &= t_5 + D_{ij} = t[i, k + 1] + W_i / \rho_i + D_{ij} + D_{ji} = \\ &= t[i, k] + W_i / \rho_i + W_j / \rho_j + D_{ij} + D_{ji}. \end{aligned} \quad (5.83)$$

Аналогічно можна показати справедливність отриманих співвідношень для випадку, коли $Q_i(t_2) = 0$. В результаті ефективність віртуальних каналів

можна оцінити за допомогою таких виразів:

$$\begin{aligned} E_i &= 2W_i / (W_j + W_i + (\rho_i D_{ij} + \rho_j D_{ji})); \\ E_j &= 2W_j / (W_j + W_i + (\rho_i D_{ij} + \rho_j D_{ji})). \end{aligned} \quad (5.84)$$

При цьому максимальне значення ефективності $E_i = 1$ досягається при $W_i > W_j + (\rho_i D_{ij} + \rho_j D_{ji})$, а при $W_i < W_j + (\rho_i D_{ij} + \rho_j D_{ji})$ досягається значення $E_i = W_i / W_j$. Отже, затримка, яка викликається підтвердженнями, що чекають в черзі, є однією із причин зменшення пропускної спроможності з'єднання. Тому розміри буферів фільтрів пакетів і продуктивність мережних інтерфейсів повинні бути вибрані відповідно до співвідношень, отриманих в запропонованій математичній моделі.

Маючи моделі трафіку, створюваного інтегральними потоками даних, та процесу буферизації при управлінні трафіком інтегральних потоків даних можна розробляти моделі інтелектуального управління трафіком інфокомунікаційних мереж об'єктів критичної інфраструктури.

5.8. Моделі інтелектуального управління трафіком інфокомунікаційних мереж об'єктів критичної інфраструктури

Розглянемо інтелектуальне управління розподілом навантаження віртуальних з'єднань на множині допустимих маршрутів інтегральних потоків даних (ІПД) $M = \left\{ \overline{M}_\xi = (\mu_{\xi 1}, \dots, \mu_{\xi \eta}, \dots, \mu_{\xi H_\xi}) \right\}$, де $\mu_{\xi \eta}$ – віртуальне з'єднання, що є η -ою координатою вектору, котрий визначає ξ -й маршрут; H_ξ – кількість віртуальних з'єднань на маршруті ξ . Множину віртуальних з'єднань, через які проходять маршрути ІПД, позначимо як $\Omega = \{z_s | s = \overline{1, S}\}$ і зіставимо їй множину функцій, що визначають динамічний профіль навантаження з'єднання $\Omega_{PN} = \{\beta_s(t) | s = \overline{1, S}\}$, де $\beta_s(t) = \sum_{\xi} \sum_{\eta=1}^{H_\xi} \ell(\mu_{\xi \eta}, t) \cdot \varsigma(\mu_{\xi \eta}, z_s) / L_s$; функція $\ell(\mu_{\xi \eta}, t)$ визначає навантаження з'єднання з координатою η пакетами ІПД, що проходять ξ -м маршрутом відповідно до заданого алгоритму розподілу

навантаження $\Psi(\Omega, M)$; булева функція $\zeta(\mu_{\xi\eta}, z_s)$ набуває значення «1» тоді і тільки тоді, коли її аргументи співпадають; L_s – допустиме навантаження на s -те з’єднання.

Математичне сподівання і дисперсія випадкової величини $v(z_s)$, що задає профілі навантаження з’єднань множини Ω у момент часу t_k , дорівнюють:

$$M[v] = \sum_{s=1}^S \beta_s(t_k); \quad D[v] = \sum_{s=1}^S \beta_s^2(t_k) - M^2[v]. \quad (5.85)$$

Згідно із теоремою про профіль навантаження [200] час проходження ПД зменшується при зменшенні розкиду випадкової величини $v(z_s)$, тому управління розподілом навантаження віртуальних з’єднань у момент часу t_k можна задати таким чином:

$$U = U\left(\Omega, M, \Omega_{PN}, t_k \left| D[v]_{\Psi(\Omega, M)} \rightarrow \min \right. \right). \quad (5.86)$$

Для вирішення даного завдання необхідно визначити множину Ω_{PN} . Для цього розглянемо процес проходження пакетів фіксованого маршруту $\overline{M}_{\xi}$ через віртуальний канал, котрий складається з певної кількості сполучних ліній і проміжних вузлів [190]. В цьому випадку переходи пакетів між проміжними вузлами можна представити як послідовність дискретних просторових моментів, інтервал між якими є випадковим і дорівнює часу перебування пакету в проміжному вузлі [191]. Така послідовність формує динаміку дискретних процесів пакетної комутації, безпосередньо впливає на характеристики спостережуваного трафіку і може бути проаналізована за допомогою математичного апарату функціонального недискретного аналізу, якщо всі розриви в моментах переходів описати δ -функціями [192]. Для опису таких процесів введемо функцію щільності розподілу $f(t)$ часу переходу пакету ПД по маршруту з віртуального вузла з координатою η у віртуальний вузол $\eta+1$ за час t . Враховуючи те, що з погляду внеску в оцінку значення величини затримки всі проміжні вузли ТСП-з’єднання незалежні, то справедливим буде припущення про незалежність функції щільності

розподілу $f(t)$ від координати η [193]. При розгляді індивідуальних маршрутів пакетів можливим втратам відповідає така умова: пакет не залишає проміжний вузол віртуального з'єднання з координатою η [194].

Таким чином, для розглянутого трафіку при заданій роздільній здатності спостереження в один пакет, існує ненульова ймовірність того, що середній час перебування окремого пакету задовольняє умові $\bar{t} = \int_0^{\infty} t \cdot f(t) dt = \infty$, котра в сукупності із загальними вимогами до функції щільності розподілу $f(t)$ дозволяє в класі статечних функцій отримати вираз $f(t) = \theta \cdot (1+t)^{-(\theta+1)}$, $0 < \theta < 1$, що відповідає характеру довготривалих статистичних залежностей, які спостерігаються при проходженні трафіку ПД.

Введемо функцію $F(\tau)$, котра характеризує ймовірність того, що пакет не зробить перехід в наступний вузол до настання моменту часу τ , тобто:

$$F(\tau) = 1 - \int_0^{\infty} f(t) dt = (1 + \tau)^{-\theta}, \quad (5.87)$$

де можна вважати, що τ – це час перебування пакету в проміжному вузлі віртуального з'єднання з координатою η [195]. Визначимо функцію, яка дозволяє розрахувати найбільш ймовірне число пакетів даного маршруту у

вузлі η на момент часу t як $\ell(\eta, t) = \int_0^t \ell(\eta-1; t-\tau) \cdot f(\tau) d\tau + \ell_0(\eta)F(t)$, де

$\ell_0(\eta)$ – кількість пакетів у вузлі η до приходу пакетів з вузла $\eta-1$. Позначимо

$\Delta L = \ell(\eta, t) - \int_0^t \ell(\eta; t-\tau) \cdot f(\tau) d\tau$. Тоді можна записати, що [196]:

$$\Delta L = \int_0^t (\ell(\eta-1; t-\tau) - \ell(\eta; t-\tau)) f(\tau) d\tau + \ell_0(\eta) \cdot F(t). \quad (5.88)$$

Розкладемо функцію $\ell(\eta-1; t-\tau)$ в ряд Тейлора:

$$\begin{aligned}
\ell(\eta-1; t-\tau) &= \ell(\eta; t-\tau) + \frac{\partial \ell(\eta; t-\tau)}{\partial \eta} \cdot ((\eta-1) - \eta) + R_2(\eta) = \\
&= \ell(\eta; t-\tau) - \frac{\partial \ell(\eta; t-\tau)}{\partial \eta} + O(\eta^2).
\end{aligned} \tag{5.89}$$

В (5.26) можна нехтувати доданками порядку $O(\eta^2)$ [202], тому:

$$\begin{aligned}
\Delta L &= \ell(\eta, t) - \int_0^t \ell(\eta; t-\tau) \cdot f(\tau) d\tau = \\
&= - \int_0^t \frac{\partial \ell(\eta; t-\tau)}{\partial \eta} \cdot f(\tau) d\tau + \ell_0(\eta) \cdot F(t).
\end{aligned} \tag{5.90}$$

Застосуємо до отриманого рівняння перетворення Лапласа L за часом:

$$\begin{aligned}
L \left(\int_0^t \frac{\partial \ell(\eta; t-\tau)}{\partial \eta} \cdot f(\tau) d\tau + \ell_0(\eta) \cdot F(t) \right) &= \frac{\partial \ell_p(\eta; p)}{\partial \eta} \cdot \int_0^\infty \exp(-p\tau) f(\tau) d\tau = \\
&= \frac{\partial \ell_p(\eta; p)}{\partial \eta} \int_0^\infty \exp(-p\tau) \theta \cdot (1+\tau)^{-(\theta+1)} d\tau,
\end{aligned} \tag{5.91}$$

де p і $\ell_p(\eta; p)$ – параметр і перетворення Лапласа функції $\ell(\eta; t)$ відповідно. Для обчислення інтеграла в правій частині (5.90) зробимо заміну змінних $y = \tau + 1$, після якої отримаємо такий вираз:

$$\theta \int_0^\infty \exp(-p(y-1)) y^{-(\theta+1)} dy = \theta \cdot \exp(p) \int_0^\infty \exp(-py) \cdot y^{-(\theta+1)} d\tau. \tag{5.92}$$

Якщо $py = t$, тобто $dy = \frac{dt}{p}$, то після низки перетворень отримуємо:

$$\theta \cdot \exp(p) \int_0^\infty \exp(-py) \theta \cdot y^{-(\theta+1)} d\tau = 1 - e^p \cdot p^\theta \int_p^\infty \exp(-t) \cdot t^{-\theta} dt.$$

Скориставшись виразом для гамма-функції $\Gamma(a; \eta) = \int_{\eta}^{\infty} \exp(-t) \cdot t^{a-1} dt$,

де $\Gamma(a)$ – гамма-функція Ейлера, а функція $g(a; \eta)$ виражається через $\Gamma(a)$ за допомогою таких співвідношень:

$$g(a; \eta) = h(a; \eta) \cdot \Gamma(a) = \int_0^{\eta} \exp(-t) \cdot t^{a-1} dt;$$

$$p(a; \eta) = \Gamma^{-1}(a) \int_0^{\eta} \exp(-t) \cdot t^{a-1} dt,$$

запишемо праву частину перетворення як:

$$\frac{\partial \ell_p(\eta; p)}{\partial \eta} \int_0^{\infty} \exp(-p\tau) \theta \cdot (1+\tau)^{-(\theta+1)} d\tau = \frac{\partial \ell_p(\eta; p)}{\partial \eta} (1 - p \cdot F_p(p)), \quad (5.93)$$

де $p \cdot F_p(p) = p^{\theta} e^{p\Gamma(1-\theta; p)}$, $\Gamma(1-\theta; p) = \int_{\eta}^{\infty} \exp(-t) \cdot t^{\theta} dt$.

Далі розглянемо перетворення Лапласа для лівої частини перетворення, інтегральний доданок якої матиме вигляд:

$$L \left(\int_0^t \ell(\eta; t-\tau) \cdot f(\tau) d\tau \right) = \ell_p(\eta; p) \cdot f_p(p), \quad (5.94)$$

де $f_p(p)$ – перетворення Лапласа функції щільності розподілу $f(t)$.

Виходячи з властивостей перетворення Лапласа для констант і визначених інтегралів, можна записати вираз для перетворення Лапласа функції $F(t)$ в області зображень: $F_p(p) = (1 - f_p(p)) / p$. Розглядаючи тільки часову складову і враховуючи, що в часовій області є дійсним такий вираз:

$$F(t) = 1 - \int_0^t \theta \cdot (1-\tau)^{\theta-1} d\tau = (1+t)^{-\theta}, \quad \text{можна обчислити в явному вигляді}$$

зображення Лапласа функції, зробивши заміну змінних $y = 1 + \tau$:

$$F_p(p) = \int_0^{\infty} \exp(-p\tau) \cdot (1+\tau)^{-\theta} d\tau = \exp(p) \int_1^{\infty} \exp(-py) \cdot y^{-\theta} dy. \quad (5.95)$$

Вважаючи, що $py = t$, обчислимо отриманий вираз:

$$e^p \int_1^{\infty} \frac{e^{-py}}{y^{\theta}} dy = e^p \int_p^{\infty} \frac{e^{-t}}{t^{\theta} p^{-\theta}} \frac{dt}{p} = e^p p^{\theta-1} \int_p^{\infty} t^{-\theta} e^{-t} dt = e^p p^{\theta-1} \Gamma(1-\theta, p). \quad (5.96)$$

Таким чином, перетворення Лапласа $F(t)$:

$$F_p(p) = e^p p^{\theta-1} \Gamma(1-\theta, p),$$

тому

$$\ell_p(\eta; p) - \ell_p(\eta; p) \cdot (1 - pF_p(p)) = \ell_p(\eta; p) \cdot pF_p(p)$$

і рівняння в області зображень перетворення Лапласа набере такого вигляду:

$$pF_p(p) \cdot \ell_p(\eta; p) = -\frac{\partial \ell_p(\eta; p)}{\partial \ell} \cdot (1 - pF_p(p)) + \ell_0(\eta) \cdot F_p(p). \quad (5.97)$$

Визначимо рішення рівняння 5.34 для випадку, коли $p \ll 1$ і $\theta < 1$ [174]:

$$\Gamma(1-\theta) \cdot p^{\theta} \ell_p(\eta; p) = -\frac{\partial \ell_p(\eta; p)}{\partial \eta} + \Gamma(1-\theta) \cdot p^{\theta-1} \ell_0(\eta). \quad (5.98)$$

Переходячи до оригіналів [177], отримаємо:

$$\frac{\partial}{\partial t} \int_0^t \frac{\ell(\eta, \tau)}{(t-\tau)^{\theta}} d\tau = -\frac{\partial \ell(\eta, t)}{\partial \eta} + \frac{\ell_0(\eta)}{t^{\theta}}.$$

Відзначимо, що з точністю до множника $\Gamma(1-\theta)$ є дробовою похідною від

функції $\ell(\eta; t)$ степеня θ :

$$D_t^\theta [\ell(\eta; t)] = \frac{1}{\Gamma(1-\theta)} \cdot \int_0^t \frac{\ell(\eta; \tau)}{(t-\tau)^\theta} d\tau,$$

тому рівняння розповсюдження пакетів можна записати як диференціальне рівняння дробової похідної порядку θ :

$$\Gamma(1-\theta) p^\theta \ell(k; p) = -\ell(k+1; p) + \ell(k; p) + \Gamma(1-\theta) p^{\theta-1} \ell_0(k).$$

Апроксимуючи часткову похідну кінцевою різницею, отримаємо, що:

$$\Gamma(1-\theta) \cdot D_t^\theta [\ell(\eta; t)] = -\frac{\partial \ell(\eta; t)}{\partial \eta} + \frac{\ell_0(\eta)}{t^\theta},$$

а після арифметичних перетворень:

$$\ell(k+1; p) = \left[1 - \Gamma(1-\theta) \cdot p^\theta \right] \cdot \ell(k; p) + \Gamma(1-\theta) \cdot p^{\theta-1} \ell_0(k). \quad (5.99)$$

Для отримання рішення рівняння (5.36) розглянемо випадок, коли в правій частині відсутній 2 доданок, тобто:

$$\ell(k+1; p) = \left[1 - \Gamma(1-\theta) \cdot p^\theta \right] \cdot \ell(k; p).$$

Рішення такого рівняння має вигляд:

$$\ell(k; p) = \left\{ \prod_{m=0}^{k-1} \left[1 - \Gamma(1-\theta) \cdot p^\theta \right] \right\} \cdot \ell(0; p),$$

або $\ell(k; p) = \left[1 - \Gamma(1-\theta) \cdot p^\theta \right] \cdot \ell(0; p)$, а неоднорідне рівняння можна записати як:

$$\ell(k+1; p) - \ell(k; p) + \Gamma(1-\theta) \cdot p^\theta \ell(k; p) = \Gamma(1-\theta) \cdot p^{\theta-1} \cdot \ell_0(k).$$

Представивши вираз для $\ell(k; p)$ у вигляді $\ell(k; p) = u(k) \cdot v(k)$ і позначивши $\Delta \ell(k; p) = \ell(k+1; p) - \ell(k; p)$, отримаємо:

$$\Delta \ell(k; p) + \Gamma(1-\theta) \cdot p^\theta \ell(k; p) = \Gamma(1-\theta) \cdot p^{\theta-1} \cdot \ell_0(k)$$

$$\text{або } u(k+1; p) \cdot \Delta v(k) + v(k) (\Delta u(k) + \Gamma(1-\theta) \cdot p^\theta u(k)) = \Gamma(1-\theta) \cdot p^{\theta-1} \cdot \ell_0(k).$$

З останнього співвідношення, застосовуючи метод Бернуллі, запишемо:

$$u(k) = \left[1 - \Gamma(1-\theta) \cdot p^\theta \right]^k u(0);$$

$$v(k) = \frac{\Gamma(1-\theta) \cdot p^{\theta-1}}{u(0)} \sum_{m=0}^{k-1} \frac{\ell_0(m)}{\left[1 - \Gamma(1-\theta) \cdot p^\theta \right]^m} + v(0).$$

В результаті рішення рівняння (5.36) прийме такий вигляд:

$$\ell(k; p) = \left(1 - \Gamma(1-\theta) \cdot p^\theta \right)^k \times$$

$$\times \left[\Gamma(1-\theta) \cdot p^{\theta-1} \sum_{m=0}^{k-1} \frac{\ell_0(m)}{\left(1 - \Gamma(1-\theta) \cdot p^\theta \right)^m} + u(0) \cdot v(0) \right].$$

Це рішення можна записати як:

$$\ell(k; p) = \left[1 - \Gamma(1-\theta) \cdot p^\theta \right]^k \times$$

$$\times \left\{ \Gamma(1-\theta) \cdot p^{\theta-1} \sum_{m=0}^{k-1} \frac{\ell_0(m)}{\left[1 - \Gamma(1-\theta) \cdot p^\theta \right]^m} + \ell(0; p) \right\}.$$

При $\ell_0(0) = \ell_0$ і $\ell_0(k) = 0$, $k = 1, 2, \dots$, отримаємо:

$$\ell(k; p) = \left[1 - \Gamma(1 - \theta) \cdot p^\theta\right]^k \left\{ \Gamma(1 - \theta) \cdot p^{\theta-1} \ell_0 + \ell(0; p) \right\}.$$

Запишемо отримане рішення за умов $\ell(0; t) = \ell_0 \cdot \delta(t)$, які моделюють генерацію серії пакетів об'ємом ℓ_0 у момент часу t у вигляді:

$$\ell(k; p) = \left[1 - \Gamma(1 - \theta) \cdot p^\theta\right]^k \left\{ \Gamma(1 - \theta) \cdot p^{\theta-1} + 1 \right\} \cdot \ell_0. \quad (5.100)$$

Розглядаючи праву частину отриманого виразу для сусідніх вузлів, можна записати наступну наближену рівність:

$$\begin{aligned} \ell(k; p) &\approx \ell_0 \left[1 - \Gamma(1 - \theta) \cdot p^\theta\right] \cdot \left\{ \Gamma(1 - \theta) \cdot p^{\theta-1} + 1 \right\} = \\ &= \ell_0 \left\{ \Gamma(1 - \theta) \cdot p^{\theta-1} + 1 - k \Gamma^2(1 - \theta) \cdot p^{2\theta-1} - k \Gamma(1 - \theta) \cdot p^\theta \right\}. \end{aligned}$$

Переходячи в цій рівності від зображень до оригіналів, отримаємо:

$$\ell(k; t) = \ell_0 \left\{ \frac{1}{t^\theta} - k \frac{\Gamma^2(1 - \theta)}{\Gamma(1 - 2\theta) \cdot t^{2\theta}} - k \Gamma(1 - \theta) \cdot \frac{1}{\Gamma(-\theta) \cdot t^{\theta+1}} \right\}$$

або

$$\ell(k; t) = \ell_0 \left\{ \frac{1}{t^\theta} - k \left[\frac{\Gamma^2(1 - \theta)}{\Gamma(1 - 2\theta)} \cdot \frac{1}{t^{2\theta}} + \frac{\Gamma(1 - \theta)}{\Gamma(-\theta)} \cdot \frac{1}{t^{\theta+1}} \right] \right\}.$$

Зокрема, при $k = 0$ $\ell(0; t) = \ell_0 \cdot t^{-\theta}$, оскільки отримане рішення носить асимптотичний характер.

Для обчислення функції кореляції розглянутого процесу повернемося до зображень [177]. Функція кореляції випадкового процесу $\ell(k; p)$ є такою:

$$c(m; p) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=1}^N \ell(i + m; p) \cdot \ell(i; p).$$

Тоді можна записати такий вираз [178]:

$$c(m; p) = \\ = \ell_0^2 \left(\Gamma(1-\theta) \cdot p^{\theta-1} + 1 \right)^2 \left(1 - \Gamma(1-\theta) \cdot p^\theta \right)^m \cdot \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{i=1}^N \left(1 - \Gamma(1-\theta) \cdot p^\theta \right)^{2i}.$$

При $p \ll 1$ для суміжних вузлів асимптотична частина функції кореляції в просторі зображень має вигляд [177]:

$$c(m; p) \approx \ell_0^2 \cdot \Gamma(1-\theta) \cdot p^{2(\theta-1)} \cdot \left[1 - m \Gamma(1-\theta) \cdot p^\theta \right] = \\ = \ell_0^2 \cdot \Gamma(1-\theta) \cdot \left[p^{2\theta-2} - m \Gamma(1-\theta) \cdot p^{3\theta-2} \right].$$

Переходячи до оригіналів, отримаємо:

$$c(m; p) \approx \ell_0^2 \cdot \Gamma(1-\theta) \cdot \left[\frac{1}{\Gamma(1-2\theta+1)} \cdot \frac{1}{t^{2\theta-1}} - m \frac{\Gamma(1-\theta)}{\Gamma(1-3\theta+1)} \cdot \frac{1}{t^{3\theta-1}} \right] = \\ = \ell_0^2 \cdot \Gamma(1-\theta) \cdot t^{1-2\theta} \cdot \left[\frac{1}{\Gamma(2-2\theta)} - m \frac{\Gamma(1-\theta)}{\Gamma(2-3\theta)} \cdot \frac{1}{t^\theta} \right].$$

Отриманий вираз показує, що функція кореляції має степеневу залежність щодо зміни часової координати t . Тому, при $\theta < 1$ процеси характеризуються довготривалими статистичними залежностями на рівні других моментів. При $m = 0$ отримаємо вираз для дисперсії:

$$D(t) = c(0; t) = \frac{\ell_0 \cdot \Gamma(1-\theta)}{\Gamma(2-2\theta)} \cdot t^{1-2\theta},$$

характерної для процесів з довготривалими статистичними залежностями і властивістю асимптотичної самоподібності.

Отже, при інтелектуальному управлінні інтегральними потоками даних в інфокомунікаційній системі необхідно для кожного маршруту ξ визначити значення $\ell_{0\xi}$ і оцінку параметра θ_ξ відповідного ІПД.

Висновки за главою 5

У главі синтезована двовимірна динамічна модель трафіку інтегрального потоку даних інтелектуальної системи управління об'єктом критичної інфраструктури, котра базується на оперативній статистичній інформації про проходження потоку та припускає наявність даних вимірювань по декількох сесіях.

Показано, що у агрегованого трафіку збільшується кількість викидів і з'являються фрактальні властивості. Результати порівняння трафіку, змодельованого стандартними і запропонованою моделями, показали, що сумарне відхилення від реального трафіку зменшилося в середньому на 15%.

Запропонований підхід до оцінки розмірів буферів фільтрації комунікаційного обладнання інфокомунікаційної мережі інтелектуальної системи управління об'єктом критичної інфраструктури, що дозволяє підвищити пропускну здатність віртуальних каналів за рахунок зменшення затримки, яка спричинена підтвердженнями про передачу пакетів, що очікують у чергах комунікаційного обладнання шляхом вибору оптимального розміру буферів фільтрації для інтегральних потоків даних, що обслуговуються.

Також синтезована математична модель інтелектуального управління трафіком інфокомунікаційних мереж об'єктів критичної інфраструктури на комутаційних вузлах інфокомунікаційної мережі. Зокрема, реалізоване динамічне управління розподілом навантаження віртуальних з'єднань, що забезпечує вимоги щодо проходження трафіку інтегральних потоків даних з використанням оцінки профілю навантаження віртуальних з'єднань з урахуванням фрактального характеру трафіку та дозволяє скоротити час обслуговування мережних транзакцій за рахунок вирівнювання рівнів профілю навантаження.

ГЛАВА 6

ПРИКЛАДНА РЕАЛІЗАЦІЯ РОЗРОБЛЕНОЇ МЕТОДОЛОГІЇ

6.1. Диференціально-ігровий шаблон нормальної поведінки Web-сервера Житомирського військового інституту імені С. П. Корольова

Одним із перспективних шляхів підвищення рівня захищеності інформаційних ресурсів на *Web-серверах* об'єктів критичної інфраструктури є вдосконалення активних засобів захисту інформації на базі систем виявлення атак (СВА) (вторгнень) – *IDS (Intrusion Detection Systems)*. На сьогодні таких систем відомо близько сотні. Аналіз концептуальних основ побудови найбільш поширених комерційних СВА на базі хосту *Intruder Alert* (компанія *Symantec*) і мережі *Cisco Secure Scanner* (компанія *Cisco Systems*), гібридної СВА *RealSecure* (компанія *Internet Security Systems*) та некомерційних СВА *ASAX (University of Namur, Belgium)*, *SHADOW (Naval Surface Warfare Center, Dahlgren Division)* та *NetSTAT (University of California at Santa Barbara)* відповідно, дозволяє зробити висновок, що робота кожної із систем ґрунтується на методах визначення аномалій та зловживань. Базисом зазначених методів є моделі шаблонів (профілів) поведінки. Виходячи з цього скориставшись розробленою методологією розробимо шаблон нормальної поведінки (ШНП) *Web-сервера* Житомирського військового інституту імені С. П. Корольова [238–240].

Вихідні дані для моделювання зібрано в період з 01.08.2009 року по 31.01.2010 року для *Web-сервера Apache 2.2.10 (Linux|SUSE)* з використанням опції *Webalizer Logfile Analysis* на основі аналізу *log-файлів*. Мінімальний період спостереження T обрано таким, що дорівнює 24 годинам (рис. 6.1), середній – календарному місяцю (рис. 6.2), максимальний – півроку, що адекватно відповідає циклічності звернень користувачів до ресурсу. З практичної точки зору збільшення інтервалу спостереження недоцільно.

Сервер, що досліджувався, забезпечував доступ клієнтів мережі *Internet* до державного ІР у вигляді згаданої вище динамічної *web-сторінки* за виділеним цифровим некомутованим каналом з пропускнуою здатністю 15 Мбіт/с. Середній об'єм *web-сторінки* складав 1 Мбайт. Доступ на сервері відкритий для усіх користувачів мережі.

Вимоги за доступністю до ІР на сервері – високі, тобто відмова в обслуговуванні – недопустима. Вимоги за конфіденційністю – низькі, оскільки інформація призначена для широкого кола користувачів. Вимоги за цілісністю – високі, оскільки деструктивний вплив на ІР призводить як до

дезорганізації діяльності підлеглих та взаємодіючих підрозділів, так і порушення нормальної роботи навчального закладу в цілому. Тобто стандартний функціональний профіль захищеності досліджуваної АС класу 3 згідно з визначається як: $3.ЦД.4 = \{КО-1, Д-4, ЦА-4, ЦО-2, ЦВ-3, ДР-3, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-3, НА-2, НП-2\}$.



Рис. 6.1. Флуктуація середньодобового трафіка: період спостереження з 01.08.2009 по 31.01.2010 року

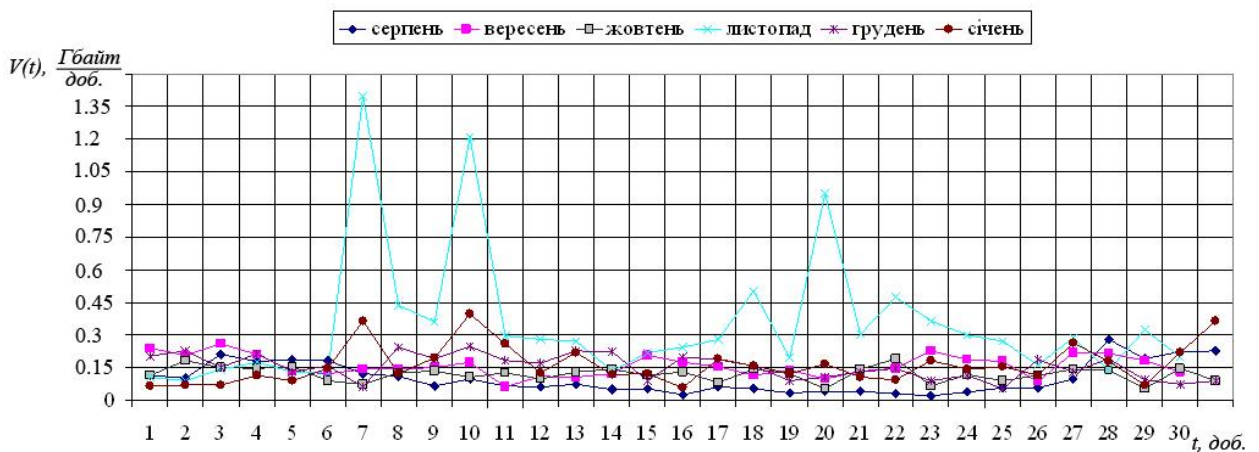


Рис. 6.2. Флуктуація місячного та піврічного трафіка: період спостереження з 01.08.2009 по 31.01.2010 року

Рівень гарантій оцінки коректності реалізації функції захисту – Г-5.

Як параметр оцінки захищеності *Web-сервера* від *DDoS-атаки* на визначених інтервалах спостереження обрано об'єм середнього вихідного мережевого трафіка за протоколом *http* – $V(t)$.

Спираючись на експлуатаційну статистику досліджуваного *Web-сервера Apache* (див. рис. 6.1 та рис. 6.2) його ШНП подамо графовою моделлю (рис. 6.3) [241].

У моделі (див. рис. 6.3) над кружками, що визначають множину станів

$\{P_z(t)\}$, де $z = 0 \dots 3$ – стани, в яких може перебувати *Web-сервер* з відповідними ймовірностями, стрілками визначено всі можливі його переходи зі стану в стан. Над стрілками переходів проставлено параметри потоків подій $\lambda(t)$ та $\mu(t)$, що переводять сервер зі стану в стан.

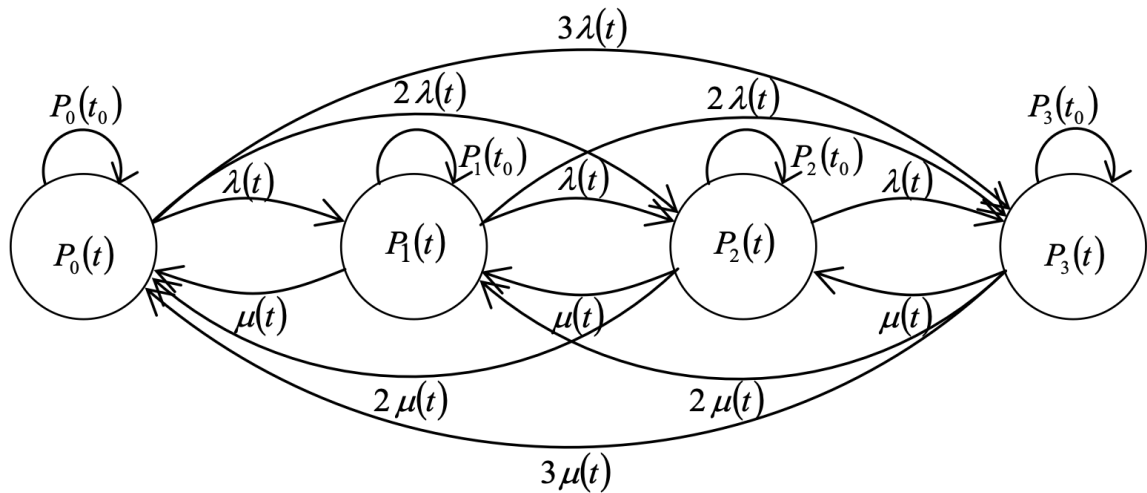


Рис. 6.3. Графова модель шаблону нормальної поведінки
Web-сервера Apache 2.2.10 (Linux|SUSE)

Під потоками подій $\lambda(t)$ та $\mu(t)$ слід розуміти стратегії гравців, що обираються ними для організації захисних дій, та організації *DDoS-атак* відповідно.

Передбачається, що $P_0(t)$ – ймовірність відмови *Web-сервера* від обслуговування під впливом *DDoS-атаки*, $P_1(t)$ – ймовірність перебування *Web-сервера* під впливом *DDoS-атаки* при дії МЗІ, $P_2(t)$ – ймовірність перебування *Web-сервера* під впливом МЗІ при дії *DDoS-атаки*, $P_3(t)$ – ймовірність перебування *Web-сервера* під впливом методів захисту інформації. $P_z(t_0)$ – початкові умови при перебуванні сервера в z -му стані, t_0 – час початку моделювання.

Особливістю запропонованої графової моделі ШНП (див. рис. 6.3) є те, що вона передбачає всі можливі переходи сервера зі стану в стан під впливом відповідних стратегій гравців. Ймовірність переходів, наприклад з нульового в четвертий стан, наближається до нуля, тому в моделі такі переходи не розглядаються.

Виходячи з графової моделі (див. рис. 6.3) та спираючись на дослідження приведені в роботі [241], інформаційний конфлікт який протікає під час *DDoS-атаки* на *Web-сервер Apache*, подамо у формалізованому вигляді

системою нелінійних диференціальних рівнянь Колмогорова-Чепмена [242]:

$$\begin{cases} \frac{dP_0(t)}{dt} = -6\lambda(t)P_0(t) + \mu(t)P_1(t) + 3\mu(t)P_3(t); \\ \frac{dP_1(t)}{dt} = -(\lambda(t) + \mu(t))P_1(t) + \lambda(t)P_0(t) + \mu(t)P_2(t) + 2\mu(t)P_3(t); \\ \frac{dP_2(t)}{dt} = -(\lambda(t) + \mu(t))P_2(t) + \lambda(t)P_1(t) + 2\lambda(t)P_0(t) + \mu(t)P_3(t); \\ \frac{dP_3(t)}{dt} = -6\mu(t)P_3(t) + \lambda(t)P_2(t) + 3\lambda(t)P_0(t). \end{cases} \quad (6.1)$$

Умова нормування для системи має вигляд:

$$\sum_{z=0}^3 P_z(t) = 1, \quad (6.2)$$

початкові умови – $P_0(t_0) = 1, P_1(t_0) = P_2(t_0) = P_3(t_0) = 0$.

Нехай стратегії гравців розподілені за законами загального вигляду:

$$\lambda(t) = \lambda t \quad (6.3)$$

та

$$\mu(t) = \mu t, \quad (6.4)$$

де λ та μ – параметри законів розподілу стратегій гравців, які невідомі;

t – часовий аргумент, $t \in [t_0, T]$.

Ресурси гравців (6.3) та (6.4) обмежені:

$$\lambda_{\min}(t) \leq \lambda(t) \leq \lambda_{\max}(t), \quad (6.5)$$

$$\mu_{\min}(t) \leq \mu(t) \leq \mu_{\max}(t), \quad (6.6)$$

де $\lambda_{\min}(t)$ і $\mu_{\min}(t)$ – мінімальні, а $\lambda_{\max}(t)$ і $\mu_{\max}(t)$ – максимальні інтенсивності потоків захисних дій та *DDos-атаки* відповідно. Стратегії

гравців $\lambda(t)$ та $\mu(t)$, що визначають їх ресурси, належать замкненим множинам $\Lambda \in E_\lambda$ та $M \in E_\mu$, які обмежені в евклідових просторах R_λ і R_μ .

Під час ІК (6.1) гравці намагаються досягти протилежних цілей. Ціль гравця захисту – забезпечити функціональну стійкість *Web-сервера* шляхом гарантування його захищеності, а гравця нападу – досягнути відмови сервера від обслуговування.

Для цього гравець КБз, що захищається від *DDoS-атаки*, намагається отримати найменший програш за рахунок вибору такої власної стратегії КБз $\lambda(t)$ (6.3), яка мінімізує плату $I_1(t, P_0(t), \lambda(t), \mu(t))$ за умови її максимізації іншим гравцем – гравцем КБн, тобто:

$$\min_{\lambda(t) \in E_\lambda} \max_{\mu(t) \in E_\mu} = I_1(t, P_0(t), \lambda(t), \mu(t)), \quad (6.7)$$

де $I_1(t, P_0(t), \lambda(t), \mu(t)) = I_1$ – плата, що є усередненою ймовірністю перебування *Web-сервера* під впливом *DDoS-атаки*.

Плата I_1 визначається як:

$$I_1 = \frac{1}{T} \int_{t_0}^T P_0(t) dt \quad (6.8)$$

при обмеженнях

$$0 \leq I_1 \leq I_{1\max}, \quad (6.9)$$

де $I_{1\max} = 1$.

Для досягнення цілі *DDoS-атаки* другий гравець – гравець КБн намагатиметься отримати найбільший виграш за рахунок вибору такої власної стратегії КБа $\mu(t)$ (6.4), яка максимізує плату $I_1(t, P_0(t), \lambda(t), \mu(t))$ за умови її мінімізації іншим гравцем, тобто:

$$\max_{\mu(t) \in E_\mu} \min_{\lambda(t) \in E_\lambda} = I_1(t, P_0(t), \lambda(t), \mu(t)). \quad (6.10)$$

Якщо виконується співвідношення рівності критеріїв (6.7) та (6.10):

$$\begin{aligned}
\min_{\lambda(t) \in E_\lambda} \max_{\mu(t) \in E_\mu} &= I_1(t, P_0(t), \lambda_{\min}^{opt}(t), \mu_{\max}^{opt}(t)) = \\
= \max_{\mu(t) \in E_\mu} \min_{\lambda(t) \in E_\lambda} &= I_1(t, P_0(t), \lambda_{\min}^{opt}(t), \mu_{\max}^{opt}(t)) = \\
= I_1^*(t, P_0^{HNP^{opt}}(t), \lambda_{\min}^{opt}(t), \mu_{\max}^{opt}(t)) &= I_1^{Gar},
\end{aligned} \tag{6.11}$$

то стратегії $\lambda_{\min}^{opt}(t)$ і $\mu_{\max}^{opt}(t)$ називаються оптимальними, а $P_0^{HNP^{opt}}(t)$ – оптимальною траєкторією, яка підлягає визначенню із системи (6.1) за критерієм (6.11) та є диференціально-ігровою моделлю ШНП поведінки *Web-сервера* з позиції гравця КБн.

I_1^{Gar} – ціна гри, що визначає прогнозований рівень захищеності *Web-сервера*, який досягається за рахунок вибору гравцями оптимальних стратегій $\lambda_{\min}^{opt}(t)$ і $\mu_{\max}^{opt}(t)$.

При відхиленні будь-ким з гравців від оптимальної стратегії неминуче виникають втрати в платі, тобто:

$$I_1(t, P_0(t), \lambda(t), \mu_{\max}^{opt}(t)) \geq \min_{\lambda(t) \in E_\lambda} I_1(t, P_0(t), \lambda(t), \mu_{\max}^{opt}(t)), \tag{6.12}$$

$$I_1(t, P_0(t), \lambda_{\min}^{opt}(t), \mu(t)) \leq \max_{\mu(t) \in E_\mu} I_1(t, P_0(t), \lambda_{\min}^{opt}(t), \mu(t)). \tag{6.13}$$

Знаходження вигляду диференціально-ігрової моделі ШНП *Web-сервера* $P_0^{HNP^{opt}}(t)$ здійснимо за розробленою методологією з використанням авторського методу диференціально-ігрового моделювання.

З використанням прямого диференціального перетворення ІК вигляду системи (6.1) в області зображень матиме вигляд :

$$\left\{ \begin{aligned} P_0(k+1) &= \frac{T}{k+1} (-6 \Lambda(k) * P_0(k) + M(k) * P_1(k) + 3M(k) * P_3(k)); \\ P_1(k+1) &= \frac{T}{k+1} (-(\Lambda(k) + M(k)) * P_1(k) + \Lambda(k) * P_0(k) + \\ &\quad + M(k) * P_2(k) + 2M(k) * P_3(k)); \\ P_2(k+1) &= \frac{T}{k+1} (-(\Lambda(k) + M(k)) * P_2(k) + \Lambda(k) * P_1(k) + \\ &\quad + 2 \Lambda(k) * P_0(k) + M(k) * P_3(k)); \\ P_3(k+1) &= \frac{T}{k+1} (-6M(k) * P_3(k) + \Lambda(k) * P_2(k) + 3 \Lambda(k) * P_0(k)), \end{aligned} \right. \quad (6.14)$$

де $\{P_z(k)\}$, $\Lambda(k)$, $M(k)$ – диференціальні зображення оригіналів $\{P_z(t)\}$, $\lambda(t)$ та $\mu(t)$ відповідно, що представляють собою дискретні (гратчасті) функції цілочислового аргументу $k = 0, 1, 2, \dots$.

Зауваження. Система спектральних рівнянь (6.14) справедлива при рівності масштабної сталої H періоду спостереження T ($H = T$).

З урахуванням властивості T -добутку диференціальних зображень $\Lambda(k) * P_z(k)$ та $M(k) * P_z(k)$, один з доданків в яких являє собою сталі λ та μ , множені на цілий степінь незалежного змінного T^m (при $m = 1$), в загальному вигляді маємо:

$$\Lambda(k) * P_z(k) = \lambda T P_z(k-1) = \begin{cases} \lambda T P_z(k-1), & k \geq 1, \\ 0, & k < 1, \end{cases} \quad (6.15)$$

$$M(k) * P_z(k) = \mu T P_z(k-1) = \begin{cases} \mu T P_z(k-1), & k \geq 1, \\ 0, & k < 1. \end{cases} \quad (6.16)$$

Система (6.14), з урахуванням виразів (6.15) та (6.16) матиме вигляд:

$$\left\{ \begin{array}{l} P_0(k+1) = \frac{T^2}{k+1} (-6\lambda P_0(k-1) + \mu P_1(k-1) + 3\mu P_3(k-1)); \\ P_1(k+1) = \frac{T^2}{k+1} (-(\lambda + \mu)P_1(k-1) + \lambda P_0(k-1) + \\ \quad + \mu P_2(k-1) + 2\mu P_3(k-1)); \\ P_2(k+1) = \frac{T^2}{k+1} (-(\lambda + \mu)P_2(k-1) + \lambda P_1(k-1) + \\ \quad + 2\lambda P_0(k-1) + \mu P_3(k-1)); \\ P_3(k+1) = \frac{T^2}{k+1} (-6\mu P_3(k-1) + \lambda P_2(k-1) + 3\lambda P_0(k-1)). \end{array} \right. \quad (6.17)$$

Присвоюючи послідовно цілочислові значення аргументу $k = 0, 1, 2, \dots$, від початкових умов:

$$P_0(0) = [P_0(t_0)] = 1, \quad P_1(0) = P_2(0) = P_3(0) = 0 \quad (6.18)$$

визначаємо дискрети диференціального спектра для диференціально-ігрової моделі ШНП *Web-сервера*. Дискрети мають вигляд:

$$P_0(1) = 0, \quad P_0(2) = -3\lambda T^2, \quad P_0(3) = 0, \quad P_0(4) = \frac{1}{4}\lambda(18\lambda + 7\mu)T^4, \quad (6.19)$$

$$P_0(5) = 0, \quad P_0(6) = -\frac{1}{12}\lambda\left(3\lambda(18\lambda + 7\mu) + \frac{1}{4}\mu(77\lambda + 53\mu)\right)T^6. \quad (6.20)$$

В області зображень плата (6.8), після підстановки дискрет (6.19)–(6.20), має вигляд:

$$\begin{aligned} I_1 = \sum_{k=0}^{k=\infty} \frac{P_0(k)}{k+1} \approx & 1 - \lambda T^2 + \frac{1}{20}\lambda(18\lambda + 7\mu)T^4 - \\ & - \frac{1}{84}\lambda\left(3\lambda(18\lambda + 7\mu) + \frac{1}{4}\mu(77\lambda + 53\mu)\right)T^6. \end{aligned} \quad (6.21)$$

Дослідження на екстремум функціонала (6.25) згідно з виразом:

$$\begin{cases} \frac{\partial I_1(\lambda, \mu)}{\partial \lambda} = 0; \\ \frac{\partial I_1(\lambda, \mu)}{\partial \mu} = 0 \end{cases} \quad (6.22)$$

після спрощень зводиться до розв'язання СЛАР вигляду:

$$\begin{cases} (36\lambda + 7\mu)T^2 - 20 = 0; \\ \frac{7}{5} - \frac{1}{42} \left(\frac{161}{2}\lambda + 53\mu \right) T^2 = 0. \end{cases} \quad (6.23)$$

Розв'язання даної СЛАР дозволяє визначити невідомі параметри λ^{opt} та μ^{opt} у стратегіях гравців (6.15) та (6.16), які дорівнюють:

$$\lambda^{opt} = \frac{6484}{13445T^2} \approx 0.4823 \frac{1}{T^2}, \quad (6.24)$$

$$\mu^{opt} = \frac{5068}{13445T^2} \approx 0.3769 \frac{1}{T^2}. \quad (6.25)$$

Виконання достатніх умов:

$$\begin{cases} \frac{\partial^2 I_1(\lambda, \mu)}{\partial \lambda^2} > 0; \\ \frac{\partial^2 I_1(\lambda, \mu)}{\partial \mu^2} < 0, \end{cases} \Rightarrow \begin{cases} 36T^2 > 0; \\ -\frac{53}{42}T^2 < 0, \end{cases} \quad (6.30)$$

дозволяє стверджувати, що знайдені параметри (6.24) та (6.25) є мінімумом та максимумом відповідно.

Перевірка умов існування сідлової точки в даній диференціальній грі передбачає знаходження параметра Δ , що визначається аналітичною залежністю як:

$$\Delta = \left(\frac{\partial^2 I_1(\lambda, \mu)}{\partial \lambda \partial \mu} \right)^2 - \left(\frac{\partial^2 I_1(\lambda, \mu)}{\partial \lambda^2} \right) \left(\frac{\partial^2 I_1(\lambda, \mu)}{\partial \mu^2} \right). \quad (6.26)$$

Виконання умови $\Delta > 0$ свідчить про існування в грі сідлової точки. Оскільки згідно з (6.26) для умов (6.30) $\Delta > 0$, де $\Delta = 0.33T^8$ при $T > 0$, то в даній диференціальній грі існує сідлова точка.

Отже, знайдені коефіцієнти (6.24) та (6.25), що визначають вигляд стратегій гравців при переході до області оригіналів з використанням зворотних перетворень, є оптимальними і є відповідно мінімумом та максимумом:

$$\lambda_{\min}^{opt}(t) = \sum_{k=0}^{k=\infty} \left(\frac{t}{T} \right)^k \Lambda(k) \approx 0.4823 \frac{t}{T^2}, \quad (6.27)$$

$$\mu_{\max}^{opt}(t) = \sum_{k=0}^{k=\infty} \left(\frac{t}{T} \right)^k M(k) \approx 0.3769 \frac{t}{T^2}. \quad (6.28)$$

Прогнозований рівень захищеності IP I_1^{Gar} , що забезпечуватиме досліджуваний *Web-сервер Apache* від *DDoS-атаки* на добовому, місячному та піврічному інтервалах спостереження за визначених початкових умов та після підстановки (6.24) і (6.25) у вираз (6.21) дорівнює:

$$I_1^{Gar} = 0.6658. \quad (6.29)$$

Диференціально-ігрова модель ШНП *Web-сервера* з урахуванням (6.24) та (6.25) при переході в область оригіналів має вигляд:

$$\begin{aligned} P_0^{HNP^{opt}}(t) &= \sum_{k=0}^{k=\infty} \left(\frac{t}{T} \right)^k [P_0(k)]_{\substack{\lambda=\lambda_{\min}^{opt} \\ \mu=\mu_{\max}^{opt}}} \approx \sum_{k=0}^{k=6} \left(\frac{t}{T} \right)^k [P_0(k)]_{\substack{\lambda=\lambda_{\min}^{opt} \\ \mu=\mu_{\max}^{opt}}} = \\ &= 1 - 1.4469 \left(\frac{t}{T} \right)^2 + 1.3649 \left(\frac{t}{T} \right)^4 - 0.8747 \left(\frac{t}{T} \right)^6. \end{aligned} \quad (6.30)$$

При відхиленні гравців від оптимальних стратегій (6.24) та (6.25) модель ШНП (6.30) визначатиметься точною аналітичною моделлю:

$$P_0(t) = 1 - 3\lambda t^2 + \frac{1}{4}\lambda(18\lambda + 7\mu)t^4 - \frac{1}{12}\lambda\left(3\lambda(18\lambda + 7\mu) + \frac{1}{4}\mu(77\lambda + 53\mu)\right)t^6. \quad (6.31)$$

Змістовний аналіз диференціально-ігрової моделі ШНП. Як видно з моделі (6.31) та отриманої оцінки прогнозованого рівня захищеності I_1^{Gar} (6.29) зрозуміло, що досліджуваний *Web-сервер Apache* при виборі гравцями оптимальних стратегій (6.24) та (6.25) з ймовірністю 0,6658 відмовить від обслуговування. Звісно, чим менше величина даної оцінки, тим рівень захищеності I_1 – кращий.

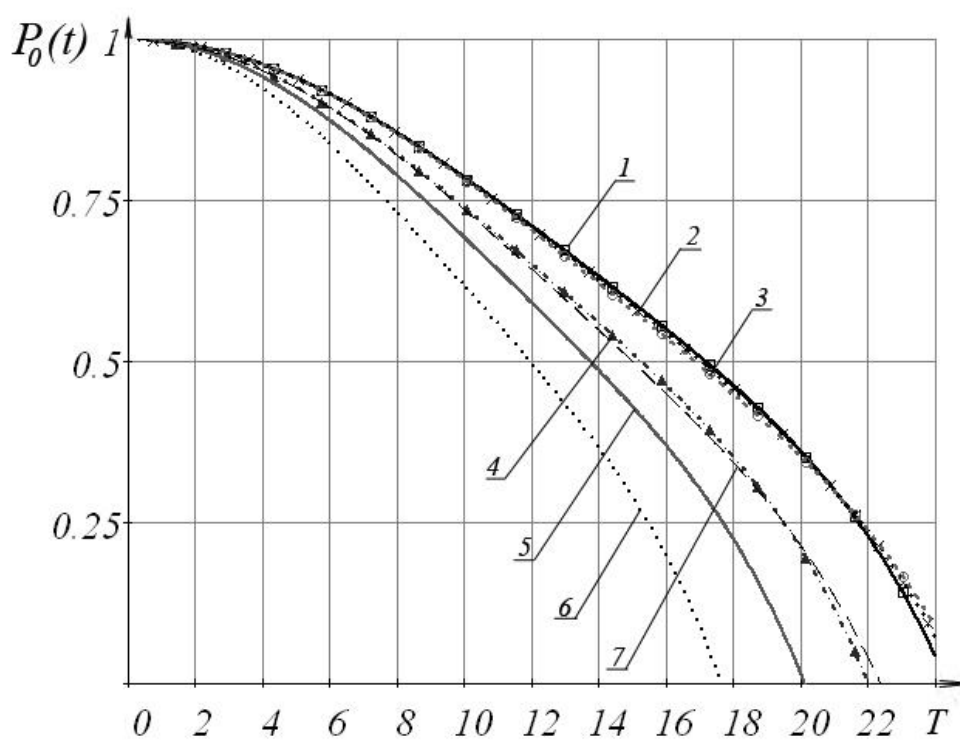
У табл. 6.1 приведено аналітичні моделі ШНП для різних умов експлуатації *Web-сервера*, що досліджується та результати моделювання з оцінювання РЗ ІР, який він забезпечуватиме за розробленим шаблоном при виборі гравцями оптимальних стратегій (6.24), (6.25) та при їх відхиленні від них.

Таблиця 6.1

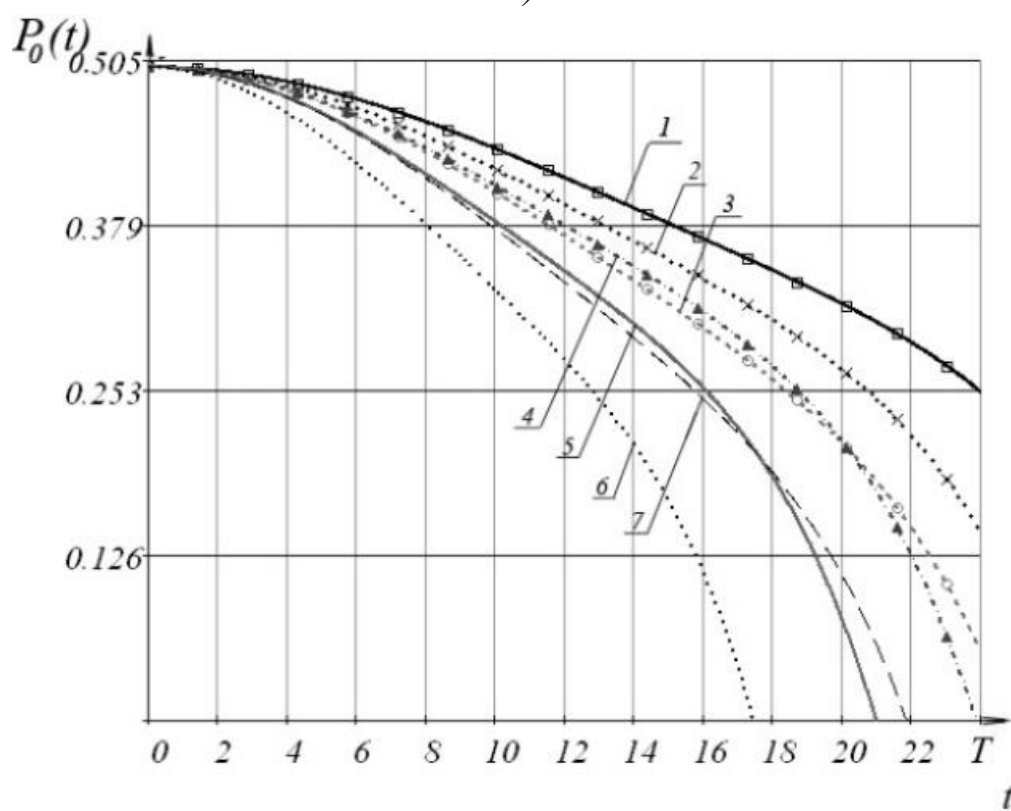
Вихідні дані для моделювання

Модель ШНП $P_0^{HNP opt}(t) = 1 - 1.4469\left(\frac{t}{T}\right)^2 + 1.3649\left(\frac{t}{T}\right)^4 - 0.8747\left(\frac{t}{T}\right)^6$ для умов $P_0(t_0)=1, P_1(t_0)=P_2(t_0)=P_3(t_0)=0$								
Стратегії	$\lambda(t)$	$\lambda^{opt}(t) = 0.4823 \frac{t}{T^2}$	$0.4823 \frac{t}{T^2}$	$0.4823 \frac{t}{T^2}$	$0.6029 \frac{t}{T^2}$	$0.7235 \frac{t}{T^2}$	$0.9646 \frac{t}{T^2}$	$0.6029 \frac{t}{T^2}$
	$\mu(t)$	$\mu^{opt}(t) = 0.3769 \frac{t}{T^2}$	$0.2827 \frac{t}{T^2}$	$0.1885 \frac{t}{T^2}$	$0.3769 \frac{t}{T^2}$	$0.3769 \frac{t}{T^2}$	$0.3769 \frac{t}{T^2}$	$0.1885 \frac{t}{T^2}$
Рівень захищеності	I_1	$I_1^{Gar} = 0.6658$	0.665	0.6631	0.5837	0.4887	0.2331	0.5869
Модель ШНП $P_0^{HNP opt}(t) = 0.5 - 0.4134\left(\frac{t}{T}\right)^2 + 0.3445\left(\frac{t}{T}\right)^4 - 0.1792\left(\frac{t}{T}\right)^6$ для умов $P_0(t_0)=0.5, P_1(t_0)=P_2(t_0)=0, P_3(t_0)=0.5$								
Стратегії	$\lambda(t)$	$\lambda^{opt}(t) = 0.5906 \frac{t}{T^2}$	$0.5906 \frac{t}{T^2}$	$0.5906 \frac{t}{T^2}$	$0.7382 \frac{t}{T^2}$	$0.8858 \frac{t}{T^2}$	$1.181 \frac{t}{T^2}$	$0.7382 \frac{t}{T^2}$
	$\mu(t)$	$\mu^{opt}(t) = 0.6299 \frac{t}{T^2}$	$0.4724 \frac{t}{T^2}$	$0.315 \frac{t}{T^2}$	$0.6299 \frac{t}{T^2}$	$0.6299 \frac{t}{T^2}$	$0.6299 \frac{t}{T^2}$	$0.315 \frac{t}{T^2}$
Рівень захищеності	I_1	$I_1^{Gar} = 0.4055$	0.3761	0.3498	0.3495	0.2806	0.0764	0.2957
Модель ШНП $P_0^{HNP opt}(t) = 0.6693\left(\frac{t}{T}\right)^2 + 0.7671\left(\frac{t}{T}\right)^4 - 0.5541\left(\frac{t}{T}\right)^6$ для умов $P_0(t_0)=P_1(t_0)=P_2(t_0)=0, P_3(t_0)=1$								
Стратегії	$\lambda(t)$	$\lambda^{opt}(t) = 0.417 \frac{t}{T^2}$	$0.417 \frac{t}{T^2}$	$0.417 \frac{t}{T^2}$	$0.5213 \frac{t}{T^2}$	$0.6255 \frac{t}{T^2}$	$0.834 \frac{t}{T^2}$	$0.6255 \frac{t}{T^2}$
	$\mu(t)$	$\mu^{opt}(t) = 0.4462 \frac{t}{T^2}$	$0.3347 \frac{t}{T^2}$	$0.2231 \frac{t}{T^2}$	$0.4462 \frac{t}{T^2}$	$0.4462 \frac{t}{T^2}$	$0.4462 \frac{t}{T^2}$	$0.2231 \frac{t}{T^2}$
Рівень захищеності	I_1	$I_1^{Gar} = 0.1488$	0.1117	0.0758	0.1503	0.155	0.1738	0.0747

На рис. 6.4 зображено графіки ШНП для умов, вихідні дані на які наведено у табл. 6.1.



a)



b)

1 – $\lambda_{\min}^{opt}(t)$, $\mu_{\max}^{opt}(t)$; 2 – $\lambda_{\min}^{opt}(t)$, $\mu(t) = 0.75 \mu_{\max}^{opt}(t)$;

3 – $\lambda_{\min}^{opt}(t)$, $\mu(t) = 0.5 \mu_{\max}^{opt}(t)$; 4 – $\lambda(t) = 1.25 \lambda_{\min}^{opt}(t)$, $\mu_{\max}^{opt}(t)$;

5 – $\lambda(t) = 1.5 \lambda_{\min}^{opt}(t)$, $\mu_{\max}^{opt}(t)$; 6 – $\lambda(t) = 2 \lambda_{\min}^{opt}(t)$, $\mu_{\max}^{opt}(t)$; 7 –

$\lambda(t) = 1.25 \lambda_{\min}^{opt}(t)$, $\mu(t) = 0.5 \mu_{\max}^{opt}(t)$

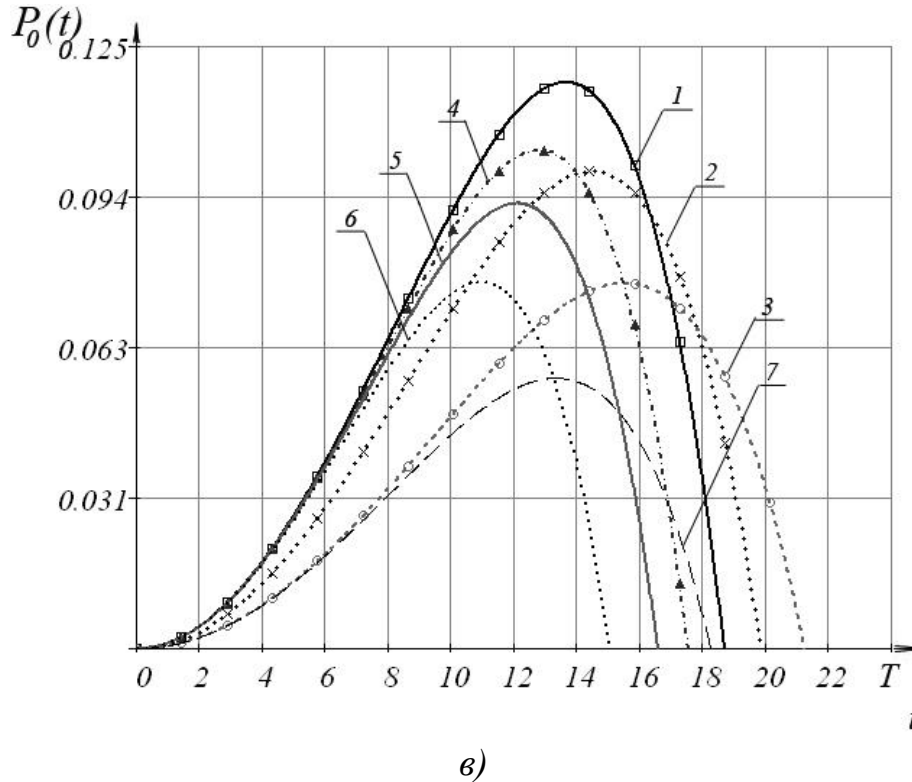


Рис. 6.4. Моделі шаблонів нормальної поведінки

Web-серверу Apache 2.2.10 (Linux|SUSE): а – $P_0(t_0) = 1$,
 $P_1(t_0) = P_2(t_0) = P_3(t_0) = 0$; б – $P_0(t_0) = 0.5$, $P_1(t_0) = P_2(t_0) = 0$, $P_3(t_0) = 0.5$; в –
 $P_0(t_0) = P_1(t_0) = P_2(t_0) = 0$, $P_3(t_0) = 1$

Аналіз даних (див. табл. 6.1) показав, що шаблон нормальної поведінки для *Web-сервера Apache 2.2.10 (Linux|SUSE)* $P_0^{HNP^{opt}}(t)$ залежить від початкових умов $P_i(t_0)$. На зміну динаміки процесу кібернападу за шаблоном нормальної поведінки також впливають стратегії, що обираються гравцями (див. рис. 6.4 а–в, 1–7). Цифрою 1 на рис. 6.4 позначено найкращу, з позиції гравця нападу ситуацію, яку він може реалізувати в процесі диференціальної гри.

З аналізу траєкторій диференціальної гри, що описують шаблон нормальної поведінки (6.30) рис. 6.4 випливає важливий висновок: гарантований рівень захищеності інформації в системі залежить від

початкового стану, в якому перебуває СІБ ОКІ на початок інформаційного конфлікту t_0 . При цьому початкові умови $P_i(t_0)$, що визначають стан СІБ ОКІ на початок інформаційного конфлікту також впливають на динаміку розвитку диференціальної гри. Так, для гравця захисту найбільш прийнятними умовами є рівність $P_0(t_0)$ нулю, тобто $P_0(t_0) = 0$, оскільки траєкторія диференціальної гри у даному випадку найшвидше досягне термінального стану (див. рис. 6.4 в).

Отже, застосування розробленого шаблону нормальної поведінки [242] для *Web-сервера Apache 2.2.10 (Linux|SUSE)* дозволяє в процесі інформаційного конфлікту відслідковувати динаміку поведінки системи, відхилення якої від нормальної сигналізує про кібернапад на ІР в системі [243]. Як результат, для гравця захисту відкривається можливість гарантованого управління рівнем захищеності *Web-сервера*.

6.2. Експериментальна верифікація диференціально-ігрових моделей критичної кіберінфраструктури на прикладі сайту Центральної виборчої комісії

Метою даного пункту є перевірка адекватності диференціально-ігрових моделей та методів моделювання процесів КБн на діючих зразках СІБ, що задіяні для захисту державних ІР шляхом їх аудиту. *Об'єктом дослідження* визначено РЗ державних ІР, що забезпечує СІБ при різних стратегіях КБа та КБз [244]].

Керуючись створеною методологією синтезу диференціально-ігрових моделей [45, 245] у якості множини контрольованих параметрів для КБа II-го класу обрано обсяг вхідного та вихідного трафіку, що може бути інтерпретований як стратегії гравців КБн та КБз відповідно. При цьому при оцінюванні РЗ державних ІР вважаються відомими такі параметри, як β – інтенсивність відмов СІБ; γ – інтенсивність знаходження вразливостей у СІБ; φ – інтенсивність усунення вразливостей; ρ – інтенсивність створення нової інформації.

На рівні держави доступ користувачів (клієнтів) до державних ІР здійснюється через Єдину точку доступу, одним із засобів захисту в якій є СІБ – програмно-апаратний комплекс (ПАК) *Arbor Peakflow SP*, що пройшов відповідну процедуру сертифікації.

Функції адміністрування ПАК *Arbor Peakflow SP* здійснюється безпосередньо Командою *CERT-UA*. Таким чином, як засіб збору експериментальних даних обрано діючий зразок засобів КБз – ПАК *Arbor Peakflow SP*, який призначений для захисту ОКІ шляхом виявлення та відбиття розподілених КБа I-го та II-го класу. Місцем збору експериментальних даних обрано Ситуаційний центр Команди *CERT-UA*.

Час для збору експериментальних даних обрано в період з 28 жовтня по 30 жовтня 2012 р., що найбільш адекватно відповідав мережевій активності щодо доступу до державних IP –web-сайтів Президента України (www.president.gov.ua) та Центральної виборчої комісії (ЦВК) України (www.cvk.gov.ua) й підтверджується офіційними даними з web-сайту Державної служби спеціального зв'язку та захисту інформації України (рис. 6.5).

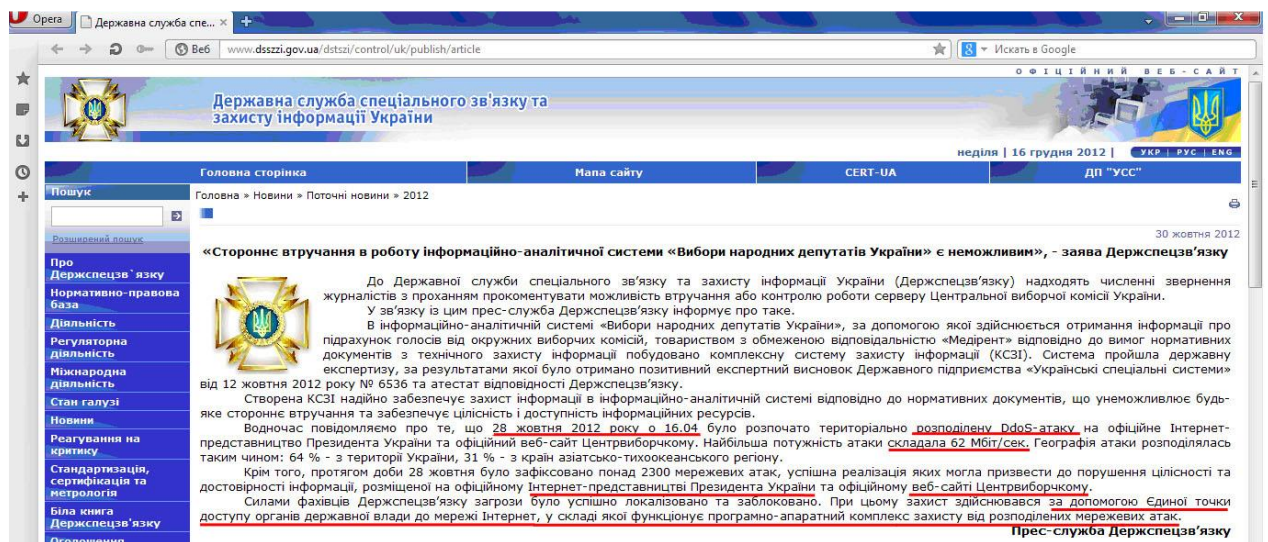


Рис. 6.5. Офіційні дані з сайту Державної служби спеціального зв'язку та захисту інформації щодо мережевої активності

Згідно офіційних даних (див. рис. 6.5) 28 жовтня 2012 року о 16 год. 04 хв. за київським часом було реалізовано процес КБн у вигляді DDos-атаки (КБа II-го класу) (рис. 6.6). Так, гравцем КБн через центр командування і управління ботами *C&C Web-server (Command & Control System)* ініціалізовано потужну КБа (див. рис. 6.6) на державні IP. Гравцем КБз для захисту державних IP застосовано ПАК *Arbor Peakflow SP*.

Для моніторингу та виявлення КБа в *Arbor Peakflow SP* використано аналізатор трафіка (*Collector Platform*) (див. рис. 6.6), який здійснював аналіз та класифікацію вхідного трафіка на предмет його відхилення від ШНП.

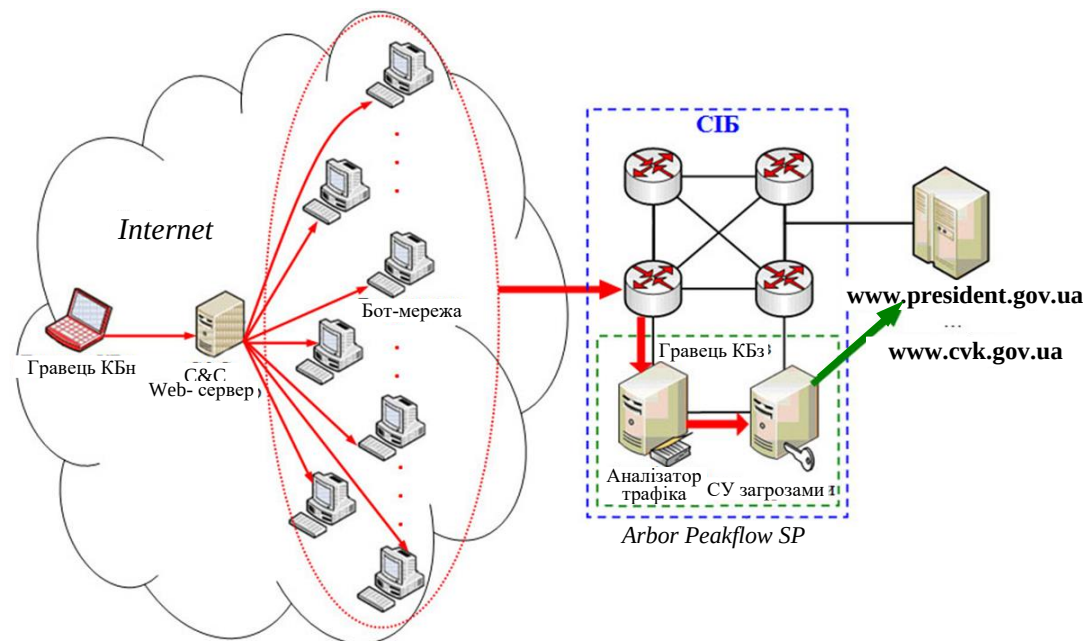


Рис. 6.6. Технологія реалізації процесу кібернападу на державні інформаційні ресурси 28 жовтня 2012 року

У випадку відхилення від заданих норм система визначає джерело КБа, а потім після реєстрації відповідної події в автоматичному або автоматизованому режимі реалізує стратегію КБз. Функції фільтрації шкідливого трафіку здійснювалися на прикладному рівні із застосуванням системи управління (*Threat Management System*). Інтерфейс адміністратора ПАК *Arbor Peakflow SP*, за допомогою якого збиралися експериментальні дані за визначеними вище параметрами у вказаний період наведено на рис. 6.7.

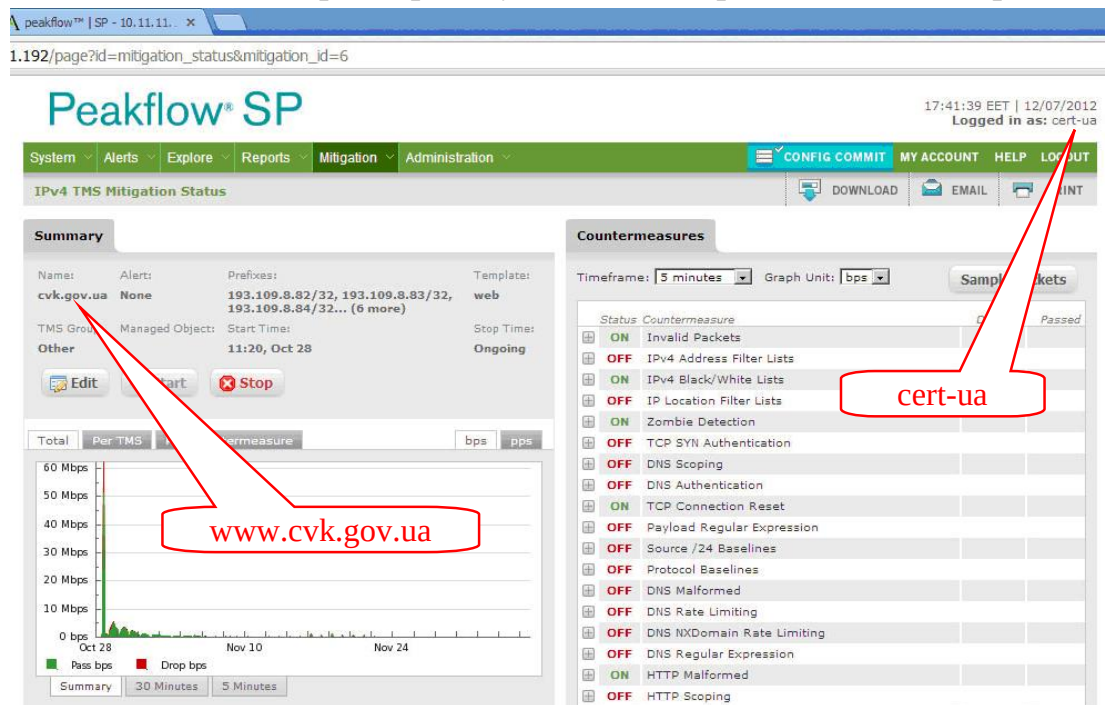


Рис. 6.7. Інтерфейс адміністратора *Arbor Peakflow SP*

Графік DDoS- атаки, спрямованої на сайт ЦВК подано на рис. 6.8.

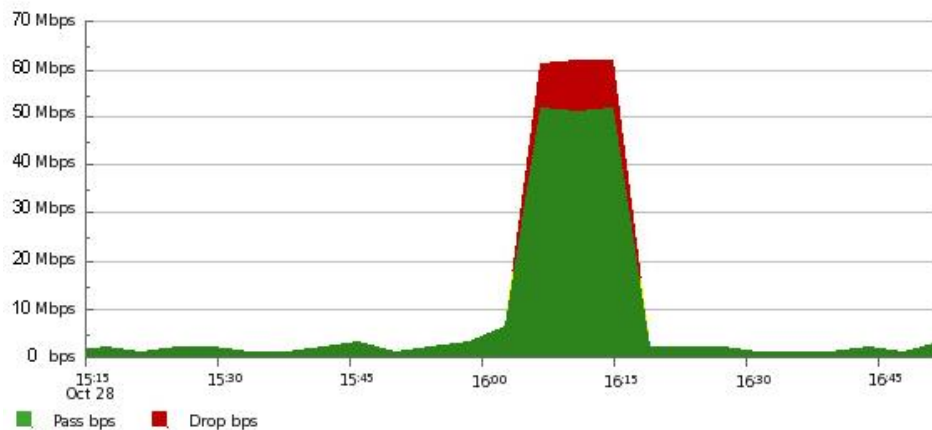


Рис. 6.8. Трафік DDos-атаки на web-сайт www.cvk.gov.ua

Урахувавши те, що web-сайт Президента України www.president.gov.ua 28 жовтня 2012 року обслуговувався одним і тим самим Web- сервером, що й сайт ЦВК за виділеним каналом пропускнуою здатністю 100 Мбіт/с, то одержані у результаті експерименту дані з оцінювання РЗ державного IP www.cvk.gov.ua є справедливими й для web-сайту Президента.

Аналіз результатів. Скориставшись методологією синтезу й аналізу диференціально-ігрових моделей та методів моделювання процесів КБн на основі зібраних експериментальних даних розробимо ШНП Web- серверу www.cvk.gov.ua та з його використанням оцінимо РЗ державного IP [3, 246, 247].

1. Для побудови ШНП Web- серверу www.cvk.gov.ua визначимо множину станів СІБ *Arbor Peakflow SP* у яких вона перебувала під час КБа II- го класу. Відповідна множина станів обрана виходячи з потреби забезпечення доступності державного IP. Так при заданих показниках, що визначають профіль захищеності АС класу 3 (табл. 6.2), множина станів дорівнює трьом (рис. 69), тобто $\{P_z(t)\}$ ($z = \overline{0,2}$), де $P_0(t)$ – ймовірність відмови Web- серверу від обслуговування (модель процесу КБн при досягненні мети DDoS-атаки); $P_1(t)$ – ймовірність перебування Web- серверу в роботоспроможному, але у вразливому стані без спроби реалізації DDoS-атаки; $P_2(t)$ – ймовірність перебування Web- серверу у роботоспроможному невразливому стані без спроб реалізації гравцем КБн DDoS-атаки.

Згідно графової моделі (див. рис. 6.9) для створюваного ШНП інформаційний конфлікт, що породжений процесом КБн, який протікає в СІБ під час DDoS-атаки, подамо у формалізованому вигляді системою нелінійних

диференціальних рівнянь Колмогорова-Чепмена:

$$\begin{cases} \frac{dP_0(t)}{dt} = -\lambda_0(t)P_0(t) + \mu_0(t)P_2(t); \\ \frac{dP_1(t)}{dt} = -\lambda_1(t)P_1(t) + \mu_1(t)P_2(t); \\ \frac{dP_2(t)}{dt} = -(\mu_0(t) + \mu_1(t))P_2(t) + \lambda_1(t)P_1(t) + \lambda_0(t)P_0(t), \end{cases} \quad (6.32)$$

яка справедлива за початкових умов $P_0(0)=0$, $P_1(0)=\frac{1}{2}$, $P_2(0)=\frac{1}{2}$ та умов нормування $P_0(0)+P_1(0)+P_2(0)=1$. Стратегії КБа для гравця КБн, виходячи з вигляду трафіку *DDos-атаки* на web-сайт *www.cvk.gov.ua* (див. рис. 6.9), визначаються аналітичними моделями загального вигляду:

$$\mu_0(t) = t e^{-\mu t}, \quad (6.33)$$

$$\mu_1(t) = \mu, \quad (6.34)$$

де μ – інтенсивність потоку КБа, яка є невідомою;

t – часовий аргумент, $t \in [t_0, T]$ ($T = 1$ доба).

Ресурс гравця КБн (6.33) щодо реалізації відповідного процесу у вигляді *DDos-атаки* web-сайт *www.cvk.gov.ua* обмежений смугою пропускання кінцевого комутаційного обладнання – каналу зв’язку $C = 100$ Мбіт/с, тобто

$$\mu_{0\max} = \frac{\mu_0}{\tilde{N}}. \text{ У випадку } \mu_0 \rightarrow C \text{ } \mu_{0\max} = 1.$$

Отже, обмеження на ресурс гравця КБн у загальному вигляді можуть бути подані моделлю вигляду:

$$\mu_{0\min} \leq \mu_0 \leq \mu_{0\max}, \quad (6.35)$$

$$\mu_{1\min} \leq \mu_1 \leq \mu_{1\max} \quad (6.36)$$

де $\mu_{0\min} = \mu_{1\min} = 0$ – для випадку відсутності КБа.

Таблиця 6.2

Система показників безпеки

№ з/п	Критерії	Показники		
		СІБ-1 <i>Arbor Peakflow SP</i>	СІБ-2	СІБ-3
1.	Прогнозований рівень захищеності державного інформаційного ресурсу	I_1^*	0.32	I_3^*
2.	Середня інтенсивність перевірок якості функціонування СІБ (КБз)	0.52	0.73	0.25
3.	Середня інтенсивність нападу (КБа) на СІБ	0.62	0.9	0.25
4.	Середня інтенсивність відмов СІБ	0.0027	0.0027	0.0027
5.	Середня інтенсивність знаходження вразливостей СІБ	0.0328	0.328	0.028
6.	Середня інтенсивність усунення вразливостей СІБ	0.0328	0.328	0.0328
7.	Середня інтенсивність оновлення сигнатур вірусів в СІБ	1	1	1
8.	Рівень захищеності інформації, що забезпечує СІБ	max	max	max
9.	Середні витрати ресурсів СІБ та системою атаки	min	min	min
10.	Надійність функціонування СІБ	max	max	max
11.	Ефективність СІБ	max	max	max

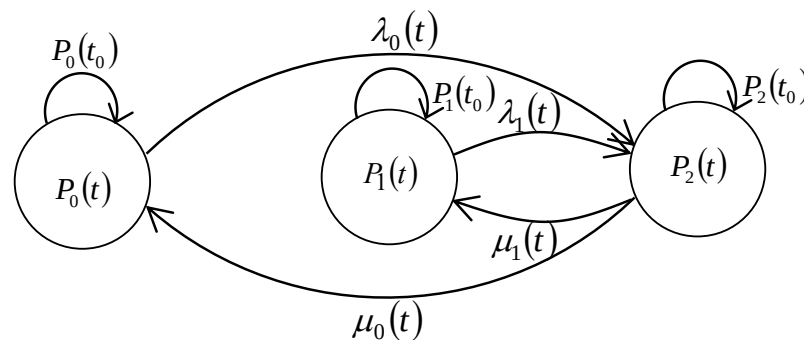


Рис. 6.9. Графова модель шаблону нормальної поведінки сайту ЦВК

2. На другому етапі, згідно з розробленою методологією виходячи з експериментальних даних (див. рис. 6.9) та принципу, який покладено в основу побудови ШНП ПАК *Arbor Peakflow SP*, враховуючи антагонізм інтересів та цілей гравців, а також спираючись на моделі, що описують стратегії КБа гравця КБн (6.33), (6.34), оберемо моделі для стратегій гравця КБз. Враховуючи вищесказане вони можуть бути подані виразами вигляду:

$$\lambda_0(t) = t e^{-\lambda t}, \quad (6.37)$$

$$\lambda_1(t) = \lambda, \quad (6.38)$$

де обмеження на стратегії, аналогічно до (6.35), (6.36) визначаються як:

$$\lambda_{0\min} \leq \lambda_0 \leq \lambda_{0\max}, \quad (6.39)$$

$$\lambda_{1\min} \leq \lambda_1 \leq \lambda_{1\max}. \quad (6.40)$$

У випадку невжиття гравцем КБз контрзаходів, спрямованих на забезпечення захищеності державного ІР в обмеженнях (6.39), (6.40) значення показників $\lambda_{0\min}$ та $\lambda_{1\min}$ приймається рівними нулю, тобто $\lambda_{0\min} = \lambda_{1\min} = 0$.

3. На третьому етапі, скориставшись авторським методом диференціально-ігрового моделювання здійснюються процедури оптимізації обраних на етапі 2 (див. рис. 6.9) стратегій КБз $\lambda_{z\min}^{opt}(t)$ та оцінювання прогнозованого РЗ $I^*(\lambda_{z\min}^{opt}, \mu_{z\max}^{opt})$. Так в області зображень, з урахуванням стратегій (6.37)–(6.40), модель ІК набуватиме вигляду:

$$\begin{cases} P_0(k+1) = \frac{T}{k+1} \left[- \sum_{l=0}^k P_0(k-l) \frac{(-\lambda)^l}{l!} T^l + \sum_{l=0}^k P_2(k-l) \frac{(-\mu)^l}{l!} T^l \right]; \\ P_1(k+1) = \frac{T}{k+1} [-\lambda P_1(k) + \mu P_2(k)]; \\ P_2(k+1) = \frac{T}{k+1} \left[-\mu P_2(k) - \sum_{l=0}^k P_2(k-l) \frac{(-\mu)^l}{l!} T^l + \lambda P_1(k) + \right. \\ \left. + \sum_{l=0}^k P_0(k-l) \frac{(-\lambda)^l}{l!} T^l \right], \end{cases} \quad (6.41)$$

Присвоївши цілочисловому аргументу k відповідні значення $k = 0, 1, 2$ дискрети спектральної моделі $P_0(k)$ дорівнюватимуть:

$$P_0(0) = [P_0(t_0)] = 0, \quad P_0(1) = \frac{1}{2}T, \quad P_0(2) = \frac{1}{4}(\lambda - 2 - 2\mu)T^2, \quad (6.42)$$

$$P_0(2) = -\frac{1}{12}(\lambda^2 - 4\mu^2 + 2\lambda\mu - 7\mu - 4)T^3. \quad (6.43)$$

Таким чином, плата для гравця КБз з урахуванням (6.42)–(6.43) описуватиметься моделлю:

$$I = \frac{1}{4}T + \frac{1}{12}(\lambda - 2 - 2\mu)T^2 - \frac{1}{48}(\lambda^2 - 4\mu^2 + 2\lambda\mu - 7\mu - 4)T^3. \quad (6.44)$$

Оптимальні стратегії гравців (6.33), (6.34) та (6.37), (6.38) відповідно до необхідних умов зводяться до розв'язання СЛАР вигляду:

$$\begin{cases} \frac{1}{12}T^2 - \frac{1}{48}(2\lambda + 2\mu)T^3 = 0; \\ -\frac{1}{6}T^2 - \frac{1}{48}(2\lambda - 8\mu - 7)T^3 = 0, \end{cases}$$

звідки:

$$\lambda^{opt} = \frac{1}{10} \frac{8 + 7T}{T}, \quad (6.45)$$

$$\mu^{opt} = \frac{1}{10} \frac{12 - 7T}{T}. \quad (6.46)$$

Виконання достатніх умов:

$$\begin{cases} -\frac{1}{24}T^3 < 0; \\ \frac{1}{6}T^3 > 0, \end{cases} \quad (6.47)$$

дозволяє стверджувати, що (6.45) та (6.46) є відповідно $\lambda_{\max}^{opt}$ та $\mu_{\min}^{opt}$.

Для одержання оцінки прогнозованого РЗ державного ІР, що забезпечувала за розробленим ШНП СІБ потрібно визначити ціну гри, в яку переходить плата (6.44) після підстановки в неї оптимальних стратегій (6.45) та (6.46). Але достовірність одержуваної оцінки РЗ ІР, виходячи з фізичних міркувань, забезпечуватиметься відповідністю одержаних оптимальних стратегій встановленим обмеженням, які накладаються виходячи з параметрів виділеного каналу зв'язку. Отже, урахувавши стратегії гравців (6.33), (6.34) та (6.37), (6.38) зі значенням коефіцієнтів, що визначають їх оптимальні значення (6.45) та (6.46), а також врахувавши відповідні обмеження одержимо наступне. Протягом доби 28 жовтня 2012 року прогнозований РЗ державного ІР – веб-сайту ЦВК згідно розробленого ШНП дорівнював [247, 248]:

$$I^* = 0.2188.$$

Співставлення одержаної кількісної оцінки з інтервальною оберненою нормованою фундаментальною шкалою оцінок ефективності СІБ дозволило зробити висновок: що за даними показниками система забезпечує достатньо ефективний захист від КБа II-го класу.

Оцінимо поточний РЗ, що забезпечила СІБ *Arbor Peakflow SP* під час *DDoS-атаки* згідно з описаними вище вихідними даними. Результати подамо у вигляді табл. 6.3 та графіку (рис. 6.10).

Таблиця 6.3

Результати

Оперативний час (28 жовтня 2012 року)	Стратегії гравців		Поточний рівень захищеності
15:15	0.02	0.02	0.1679
15:20	0.02	0.02	0.1679
15:25	0.01	0.01	0.1672
15:30	0.01	0.01	0.1672
15:35	0.02	0.02	0.1679
15:40	0.03	0.03	0.1685
15:45	0.01	0.01	0.1672

Оперативний час (28 жовтня 2012 року)	Стратегії гравців		Поточний рівень захищеності
15:50	0.02	0.02	0.1679
15:55	0.03	0.03	0.1685
16:00	0.06	0.06	0.1705
16:05	0.61	0.52	0.2095
16:10	0.62	0.51	0.2091
16:15	0.62	0.52	0.2101
16:20	0.02	0.02	0.1679
16:25	0.02	0.02	0.1679
16:30	0.02	0.02	0.1679
16:35	0.01	0.01	0.1672
16:40	0.01	0.01	0.1672
16:45	0.01	0.01	0.1672
16:50	0.02	0.02	0.1679
16:55	0.01	0.01	0.1672
17:00	0.03	0.03	0.1685
28.10.12 00:00 – 29.10.12 00:00	0.05	1	0.2188

4. Після третього етапу застосування методології перейдемо до її заключного етапу та цінимо ефективність СІБ *Arbor Peakflow SP* в цілому за системою показників, що визначають профіль захищеності відповідної АС класу 3 (див. табл. 6.3) та синтезуємо найефективнішу СІБ із заданих (див. табл. 6.3).

Оцінювання ефективності проведемо на основі авторського методу оцінювання ефективності СІБ. У результаті маємо:

– для СІБ-1 (*Arbor Peakflow SP*):

$$I_{01}^{(2)} = 1 - 0.2188 = 0.7812,$$

$$I_{02}^{(2)} = 1 - \frac{2}{\frac{1}{1-0.52} + \frac{1}{0.62}} \approx 0.458,$$

$$I_{03}^{(2)} = 1 - \frac{4}{\frac{1}{1-0.0027} + \frac{1}{0.0328} + \frac{1}{0.0328} + 1} \approx 0.94,$$

$$I_0^* = 1 - \frac{3}{\frac{1}{0.7812} + \frac{1}{1-0.458} + \frac{1}{0.94}} \approx 0.28;$$

– для СІБ-2:

$$I_{01}^{(2)} = 1 - 0.68 = 0.32,$$

$$I_{02}^{(2)} = 1 - \frac{2}{\frac{1}{1-0.73} + \frac{1}{0.9}} \approx 0.58,$$

$$I_{03}^{(2)} = 1 - \frac{4}{\frac{1}{1-0.0027} + \frac{1}{0.328} + \frac{1}{0.328} + 1} \approx 0.51,$$

$$I_0^* = 1 - \frac{3}{\frac{1}{0.58} + \frac{1}{1-0.58} + \frac{1}{0.51}} \approx 0.49;$$

– для СІБ-3:

$$I_{01}^{(2)} = 1 - 0.1 = 0.9,$$

$$I_{02}^{(2)} = 1 - \frac{2}{\frac{1}{1-0.25} + \frac{1}{0.25}} \approx 0.62,$$

$$I_{03}^{(2)} = 1 - \frac{4}{\frac{1}{1-0.0027} + \frac{1}{0.028} + \frac{1}{0.0328} + 1} \approx 0.99,$$

$$I_0^* = 1 - \frac{3}{\frac{1}{0.1} + \frac{1}{1-0.62} + \frac{1}{0.99}} \approx 0.37.$$

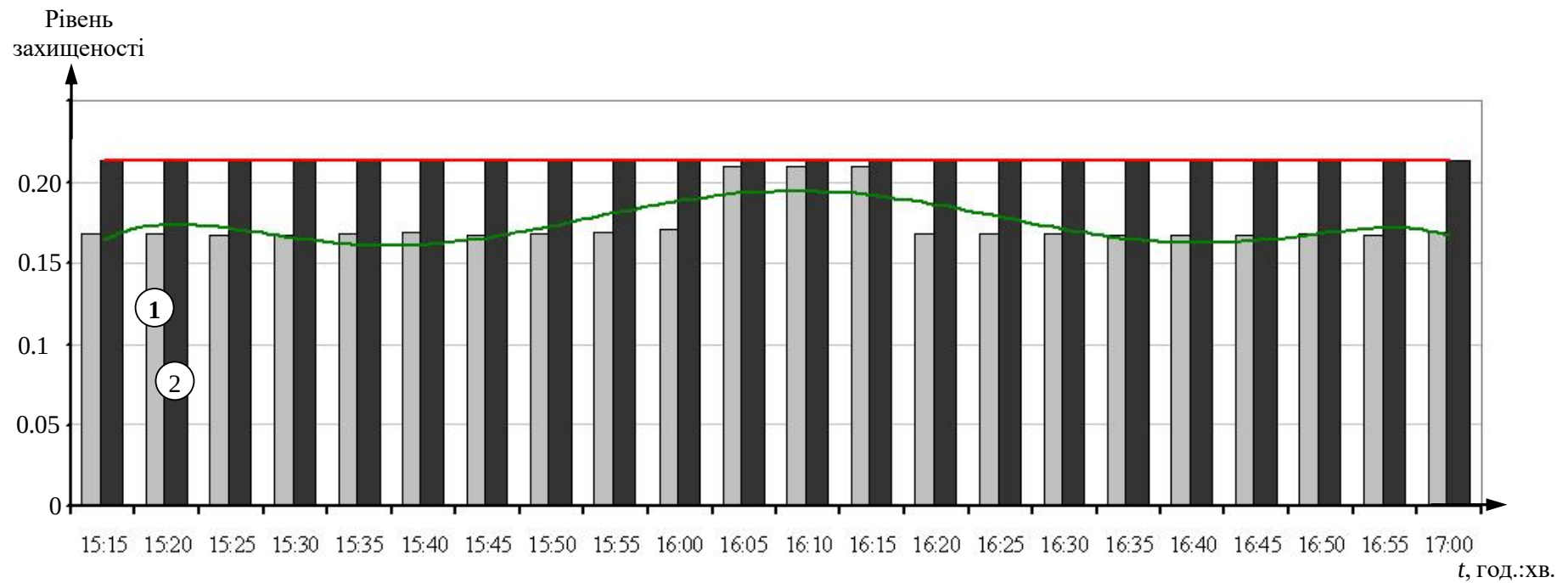


Рис. 6.10. Результати оцінювання прогнозованого та поточного рівнів захищеності
державного інформаційного ресурсу www.cvk.gov.ua:

- 1 – поточний рівень захищеності;
- 2 – прогнозований рівень захищеності

Звівши отримані дані подамо у вигляді рис. 6.11. та табл. 6.4.

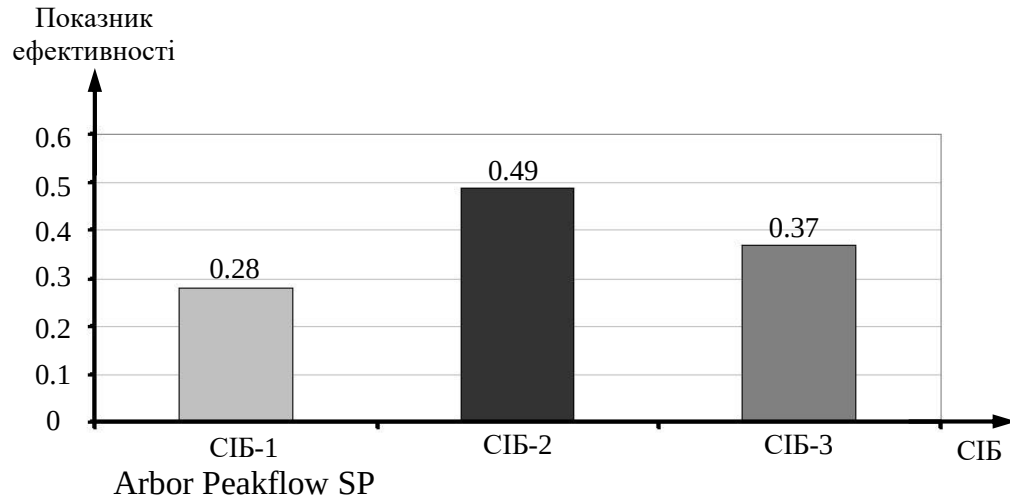


Рис. 6.11. Значення показника ефективності, що забезпечує система інформаційної безпеки

Таблиця 6.4

Результати оцінювання

СІБ-1 <i>Arbor Peakflow SP</i>	Критерії 1-го рівня ієрархії						
	$I_{01}^{(1)}$	$I_{02}^{(1)}$	$I_{03}^{(1)}$	$I_{04}^{(1)}$	$I_{05}^{(1)}$	$I_{06}^{(1)}$	$I_{07}^{(1)}$
	0.66	0.52	0.96	0.0027	0.0328	0.0328	1
	Критерії 2-го рівня ієрархії						
	$I_{01}^{(1)}$		$I_{02}^{(1)}$		$I_{03}^{(1)}$		
	0.34		0.34		0.93		
	Критерії 3-го рівня ієрархії						
	$I_0^{(3)}$						
	0.28						
	Ефективність						
Достатньо ефективна							
СІБ-2	Критерії 1-го рівня ієрархії						
	$I_{01}^{(1)}$	$I_{02}^{(1)}$	$I_{03}^{(1)}$	$I_{04}^{(1)}$	$I_{05}^{(1)}$	$I_{06}^{(1)}$	$I_{07}^{(1)}$
	0.68	0.73	0.9	0.0027	0.328	0.328	1
	Критерії 2-го рівня ієрархії						

	$I_{01}^{(1)}$		$I_{02}^{(1)}$		$I_{03}^{(1)}$		
	0.32		0.58		0.51		
	Критерії 3-го рівня ієрархії						
	$I_0^{(3)}$						
	0.49						
	Ефективність						
	Ефективна						
СІБ-3	Критерії 1-го рівня ієрархії						
	$I_{01}^{(1)}$	$I_{02}^{(1)}$	$I_{03}^{(1)}$	$I_{04}^{(1)}$	$I_{05}^{(1)}$	$I_{06}^{(1)}$	$I_{07}^{(1)}$
	0.9	0.25	0.25	0.0027	0.028	0.0328	1
	Критерії 2-го рівня ієрархії						
	$I_{01}^{(1)}$		$I_{02}^{(1)}$		$I_{03}^{(1)}$		
	0.1		0.62		0.99		
	Критерії 3-го рівня ієрархії						
	$I_0^{(3)}$						
	0.37						
	Ефективність						
	Достатньо ефективна						

Таким чином, з результатів експерименту впливають такі основні науково-прикладні висновки:

обраний для збору експериментальних даних засіб захисту – СІБ *Arbor Peakflow SP* є діючим зразком засобів захисту, який використовується CERT-UA для захисту державних інформаційних ресурсів, а тому усі вихідні дані для оцінювання зібрано коректно;

як ОКІ, державний ІР на якому підлягав захисту, обрано web-сайт ЦВК – www.cvk.gov.ua, актуальність підвищення РЗ якого обумовлена виборами до Верховної Ради України, які відбулися 28 жовтня 2012 року. Показано, що згідно з одержаною за розробленим шаблоном нормальної поведінки Web-сервера моделлю оцінка РЗ державного інформаційного ресурсу оцінюється як така, що є достатньо захищеною від КБа II-го класу (*DDoS*); динаміка зміни оцінок

поточного РЗ державного ІР (див. рис. 6.11) показує, що його величина не перевищує прогнозованого рівня. Такий практичний результат добре узгоджується з одержаними в роботі теоретичними результатами; проведений синтез СІБ показує, що з обраних систем захисту державних інформаційних ресурсів СІБ *Arbor Peakflow SP* є такою, що найбільш ефективно забезпечує доступність ІР до користувачів.

Отже, одержані науково-прикладні результати за реальними експериментальними даними в результаті аудиту діючої СІБ державних інформаційних ресурсів *Arbor Peakflow SP* підтверджують адекватність диференціально-ігрових моделей та достовірність методів моделювання. Одержані в результаті оцінювання за диференціально-ігровими моделями оцінки РЗ державного ІР *www.cvk.gov.ua* є збіжними за результатами обчислювальних експериментів.

6.3. Методологія синтезу диференціально-ігрових моделей та методів моделювання процесів кібернападу

Розроблена методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів КБн містить шість етапів (рис. 6.12):

- 1) визначення множини станів СІБ;
- 2) вибір стратегій КБз;
- 3) оптимізація стратегій КБз та оцінювання РЗ;
- 4) прогнозування розвитку динаміки процесу КБн;
- 5) оптимізація ресурсів КБз та оцінювання РЗ;
- 6) оцінювання ефективності СІБ.

1. Визначення множини станів СІБ. На першому етапі, виходячи з того які характеристики безпеки ІР повинні бути забезпечені (конфіденційність, цілісність, доступність) та множини параметрів, що визначають інтенсивності реалізації КБа $\mu_i(t)$ ($i = \overline{1, n}$, де n – кількість КБа), відмов СІБ $\beta_i(t)$, знаходження вразливостей $\gamma_i(t)$ тощо, експертом з ІБ вирішується концептуальне завдання щодо визначення множини можливих станів $\{P_z(t)\}$, у яких може перебувати новостворювана СІБ ($P_z(t)$ – ймовірності перебування СІБ під впливом відповідних методів, $z = \overline{0, c}$, c – кількість станів СІБ).

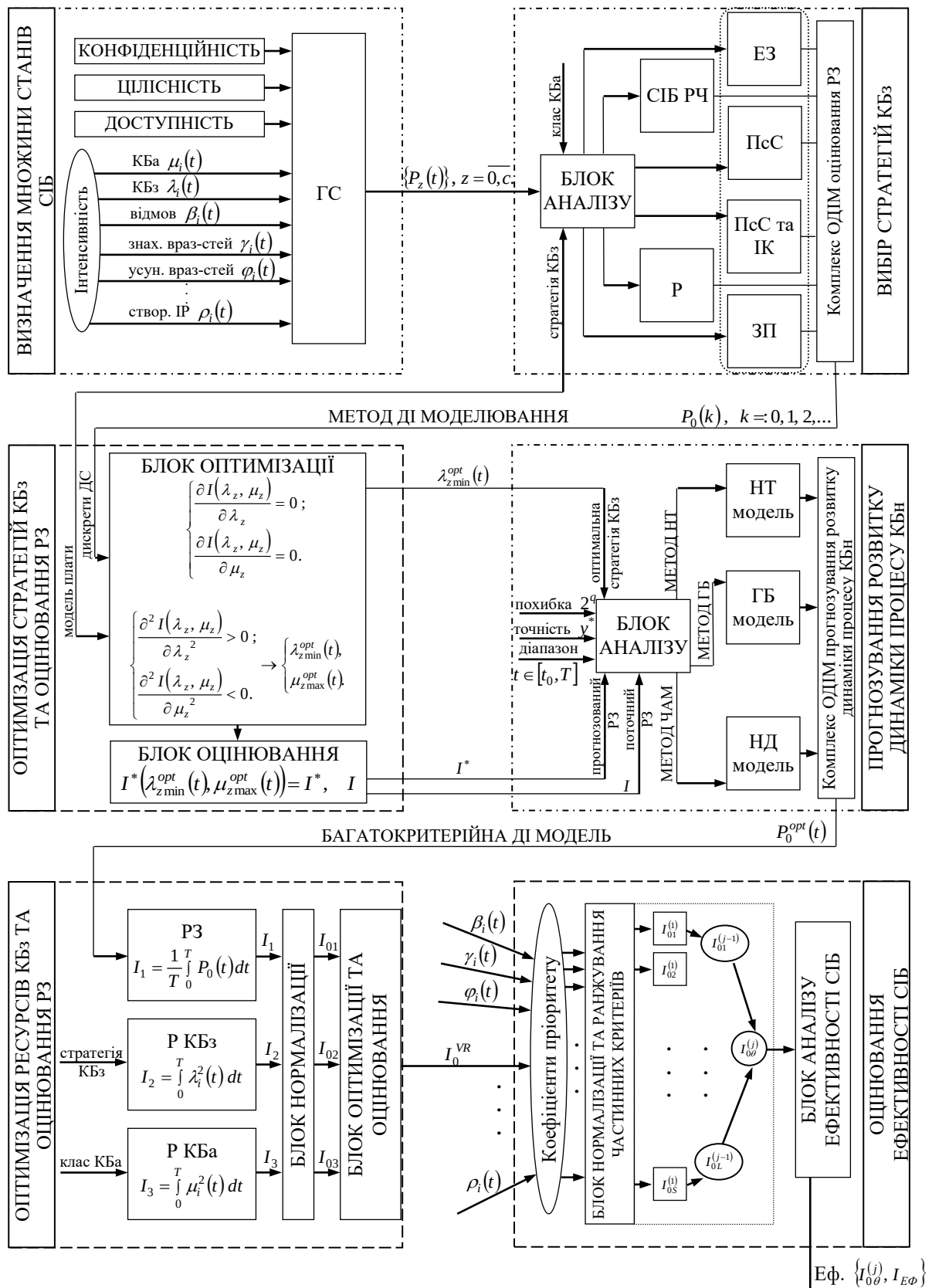


Рис. 6.12. Схема методології синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси об'єктів критичної інфраструктури

Наприклад, якщо $z = 0$, то СІБ у момент часу t перебуває під впливом методів НСД, якщо $z = 1$ – під впливом МЗІ тощо.

2. Вибір стратегій КБз. На основі сформованої множини можливих станів СІБ $\{P_z(t)\}$, класу КБа і параметрів, які її характеризують, обирається стратегія КБз: стратегія побудови СІБ реального часу (РЧ); стратегія ешелонованого захисту (СЕЗ); стратегія хибного відведення гравця КБн на псевдосервіс (ПсС); стратегія хибного відведення гравця КБн на псевдосервіс з подальшим втягуванням його в ІК (ПсС та ІК); стратегія КБз, що характеризується змінними потоками захисних дій (ЗП); стратегія розподіленого (Р) захисту. Як результат, за обраною стратегією будується граф станів СІБ під час КБа при реалізації процесу КБн та формалізується модель ІК, яка у подальшому використовується як вихідна для моделювання процесу КБн.

3. Оптимізація стратегій КБз та оцінювання РЗ. На третьому етапі, на основі методу диференціально-ігрового моделювання здійснюються процедури оптимізації обраних на етапі 2 стратегій КБз $\lambda_{z\min}^{opt}(t)$ та оцінювання прогнозованого $I^*(\lambda_{z\min}^{opt}, \mu_{z\max}^{opt})$ й поточного I РЗ. Кількісні оцінки поточного I та прогнозованого I^* РЗ знаходяться в інтервалі $I, I^* \in [0, 1]$. Чим ближче оцінка наближається до 0, тим РЗ вищий. Процедура оптимізації на третьому етапі реалізується у відповідному блоці, а в блоці оцінювання реалізується процедура оцінювання прогнозованого РЗ. Одержані дані з вказаних блоків є вихідними даними для наступного, четвертого етапу.

4. Прогнозування розвитку динаміки процесу КБн. На четвертому етапі вирішується завдання прогнозування розвитку динаміки процесу КБн $P_0^{opt}(t)$ на основі комплексу однокритерійних диференціально-ігрових моделей (ОДІМ) $P_0^{NTopt}(t)$, $P_0^{GLopt}(t)$ або $P_0^{opt}_i(t)$.

З цієї метою на блок аналізу, окрім оцінок $\lambda_{z\min}^{opt}(t)$, I^* та I , надходять вимоги, що висуваються до похибки моделі 2^q (q – кількість дискрет, які враховуються для диференціальних спектрів (ДС) $P_0(k)$ при побудові відповідної моделі (k – цілочисловий аргумент, $k = 0, 1, 2, \dots$)), її точності y^* , а також діапазону прогнозування $t \in [t_0, T]$ на якому вона працює із заданими характеристиками. Виходячи з висунутих вимог обирається один з трьох

диференціально-ігрових методів моделювання: метод моделювання на основі нетейлорівських перетворень (НТ) – метод НТ; метод ГБ моделювання – метод ГБ; метод числово-аналітичного моделювання (ЧАМ) – метод ЧАМ. Далі будується відповідна диференціально-ігрова модель прогнозування розвитку динаміки процесу КБн – НТ диференціально-ігрова модель $P_0^{NT\ opt}(t)$, ГБ модель $P_0^{G\ L\ opt}(t)$ або неперервна-дискретна (НД) диференціально-ігрова модель $P_0^{opt}_i(t)$.

5. Оптимізація ресурсів КБз та оцінювання РЗ. На цьому етапі вирішуються ряд задач. Основна задача – це задача оптимізації обмеженого ресурсу КБз $\lambda_{z\ min}^{opt}(t)$ за умови відповідності поточного РЗ прогнозованому, який не гірше за ціну гри I_0^{VR} . Другорядна задача – задача підвищення достовірності одержуваних оцінок прогнозованого РЗ та адекватності відповідних багатокритерійних диференціально-ігрових моделей $P_0^{opt\ VR}(t)$. Вказані задачі вирішуються шляхом введення експертом з ІБ додаткових частинних критеріїв $I_j = \Phi_j[\lambda_i(t), \mu_i(t), T, P_0(t)]$, що характеризують той чи інший аспект функціонування СІБ (Φ_j – функції, що мають неперервні частинні похідні за $\lambda_i(t)$ та $\mu_i(t)$). Частинні критерії I_j є компонентами r -мірного векторного критерію $I_0 = \overline{I_1, I_r}$, який обмежений допустимою областю $I_0 \in M$. Наприклад, додатковими частинним критеріями є ресурс (Р) гравця КБз I_2 , Р гравця КБн I_3 . Процедура багатокритерійного оцінювання реалізується із застосуванням відповідної багатокритерійної диференціально-ігрової моделі (див. роз. 4), яка ґрунтується на методі диференціально-ігрового моделювання (етап 2) та нелінійній схемі компромісів. Так, усі частинні критерії I_j надходять на блок нормалізації, де реалізується процедура їх нормалізації шляхом зведення до безрозмірної величини I_{0j} . У блоці оптимізації та оцінювання здійснюється процедура регуляризації вихідної некоректної задачі моделювання процесів КБн за багатокритерійною диференціально-ігровою моделлю, забезпечується суттєве спрощення проблеми динамічної векторної оптимізації.

6. Оцінювання ефективності СІБ. Шостий етап є заключним. Він передбачає реалізацію диференціально-ігрової процедури оцінювання ефективності СІБ, яка проектується. Так, при проектуванні СІБ експерт вирішує

завдання забезпечення вибору найефективнішої альтернативи $I_{0\theta}^{(j)*}$ з можливих, тобто $I_{0\theta}^{(j)*} \in \{I_{0\theta}^{(j)}\}$ (j – рівень ієрархії частинних критеріїв, θ – її властивості, що оцінюються). Для множини властивостей, що оцінюються, розраховуються коефіцієнти пріоритету $\alpha_{S\theta}^{(j-1)} = f_{S\theta} \left[\sum_{s=1}^{L_{\theta}^{(j-1)}} f_{s\theta} \right]^{-1}$, $\theta \in [1, L^{(j)}]$, $j \in [2, m]$, де $\alpha_{S\theta}^{(j-1)}$ – S -а компонента вектора пріоритету критерію на $(j-1)$ -у рівні ієрархії при розрахунках ефективності θ -ї властивості j -го рівня ($S \in [1, L^{(j-1)}]$, $L^{(j-1)}$ – кількість частинних критеріїв, за якими оцінюється ефективність СІБ на $(j-1)$ -у рівні ієрархії); $f_{s\theta}$ – оцінка важливості s -ї властивості $(j-1)$ -го рівня ієрархії для θ -ї властивості j -го рівня, визначена експертом з ІБ за шкалою балів. У блоці нормалізації та ранжування частинних критеріїв здійснюється процедура приведення усіх частинних критеріїв до однієї безрозмірної форми та ранжування їх у вигляді структурної схеми (див. рис. 4.1). У блоці аналізу, на основі диференціально-ігрового методу оцінювання ефективності СІБ, знаходяться кількісні та якісні оцінки ефективності системи $\{I_{0\theta}^{(j)*}, I_{E\Phi}\}$ ($I_{E\Phi}$ – базова терм-множина лінгвістичної змінної, яка визначається п'ятьма термами: $I_{E\Phi} = \bigcup_{i=1}^5 I_{E\Phi} = \{\text{«абсолютно неефективна»}, \text{«недостатньо ефективна»}, \text{«ефективна»}, \text{«достатньо ефективна»}, \text{«абсолютно ефективна»}\}$). Застосування методу (див. п. 4.4) забезпечує оцінювання ефективності СІБ на різних рівнях ієрархії, що сприяє розширенню діапазону його практичного застосування на процедури оцінювання ефективності комплексних СІБ, як діючих, так і перспективних.

На рис. 15.6 штриховою лінією виділено порядок розв'язання оберненої задачі – задачі синтезу, яка полягає у знаходженні прогнозованого I^* та поточного РЗ, а також оптимальних стратегій КБз $\lambda_{i\min}^{opt}(t)$ при найгірших, з точки зору захищеності ІР проявах КБа гравцем КБн $\mu_{i\max}^{opt}(t)$; лінією в крапку виділено порядок розв'язання прямої задачі – задачі аналізу, яка полягає у знаходженні в аналітичному вигляді диференціально-ігрових моделей процесів КБн $P_0^{opt}(t)$.

У результаті застосування методології формується звіт, у якому відображаються результати 1–6 етапів. Отримані результати можуть бути використані для формування додаткових наборів вхідних даних, які слід враховувати при проектуванні та створенні прогресивних СІБ [44, 240–245]. Особливістю методології є те, що кожен з визначених етапів може бути реалізований як окремо, так і в сукупності з іншими.

6.4. Верифікація моделей постквантових алгоритмів у модифікації протоколу SSL/TLS

В основу формування компенсованого алгоритму для забезпечення послуг безпеки в протоколі SSL/TLS пропонується використати синтез алгоритмів постквантової криптографії з удосконаленням алгоритмом UMAC [252], що забезпечить необхідний рівень стійкості, оперативності та достовірності в постквантовий криптоперіод [34, 18]. При цьому відмінною особливістю запропонованого підходу є зміна принципу формування автентифікованого повідомлення.

Спочатку дані надходять на каскадний алгоритм гешування, і паралельно формуються параметри для ССС (див. розділ 3), векторів ініціалізації модифікованих еліптичних кодів [250]. Такий підхід забезпечує максимальну швидкість перетворення і дає змогу розпаралелити задачі шифрування та формування MAC-коду. На приймальній стороні перетворення виконуються також у паралельному режимі, що дає змогу забезпечити необхідний рівень оперативності. На рис. 6.13 представлено структурну схему формування автентифікованого повідомлення, а також у вигляді алгоритму:

Крок 1. Формування приватного ключа сеансу: вибір параметрів еліптичної кривої:

$$K = \{a_1, a_2, \dots, a_6\}, a_i \forall GF(q) \quad (6.48)$$

$$\text{Private key } G^{EC_i}, X^i, P^i, D^i, e.$$

Крім цього, за необхідності формуються вектори ініціалізації – $|IV_1|$, $|IV_2|$ (для параметризації та формування укорочених та/або подовжених модифікованих еліптичних кодах).

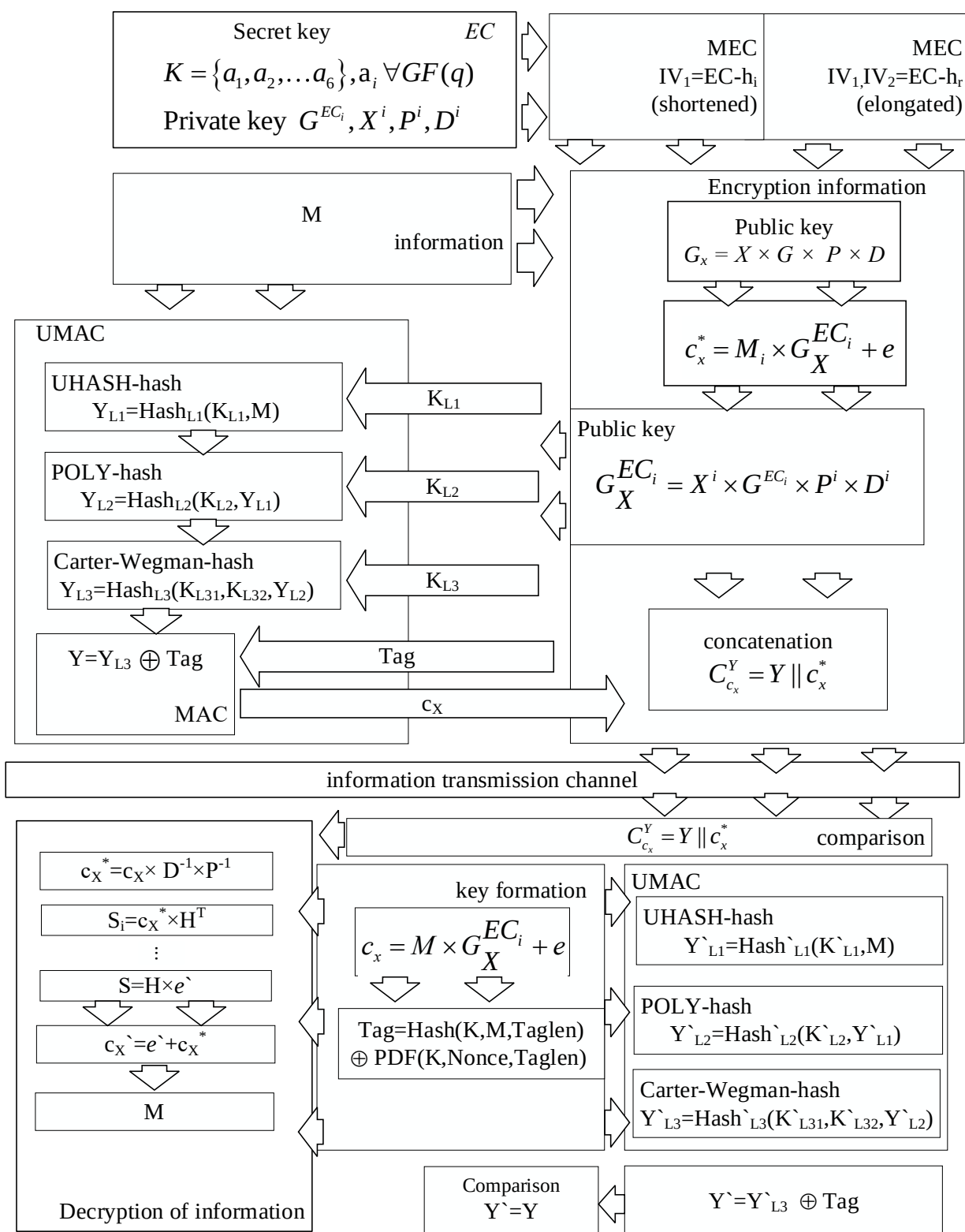


Рис. 6.13. Структурна схема формування автентифікованого повідомлення
Введення інформації на перший шар каскадного алгоритму UMAC:

$$\begin{aligned}
Hash_{L1_i} &= Hash_{L1_i} +_{64} ((M_{i_{j+0}} +_{32} K_{L1_{j+0}}) \times_{64} (M_{i_{j+4}} +_{32} K_{L1_{j+4}})), \\
Hash_{L1_i} &= Hash_{L1_i} +_{64} ((M_{i_{j+1}} +_{32} K_{L1_{j+1}}) \times_{64} (M_{i_{j+5}} +_{32} K_{L1_{j+5}})), \\
Hash_{L1_i} &= Hash_{L1_i} +_{64} ((M_{i_{j+2}} +_{32} K_{L1_{j+2}}) \times_{64} (M_{i_{j+6}} +_{32} K_{L1_{j+6}})), \\
Hash_{L1_i} &= Hash_{L1_i} +_{64} ((M_{i_{j+3}} +_{32} K_{L1_{j+3}}) \times_{64} (M_{i_{j+7}} +_{32} K_{L1_{j+7}})).
\end{aligned} \tag{6.49}$$

Крок 2. Формування геш-коду на другому шарі каскадного алгоритму гешування $Y_{L2} = (M_{P_n} + kM_{P_{n-1}} + \dots + k^{n-1}M_{P_1} + k^n) \bmod(p)$, яке обчислюється ітеративною процедурою (для всіх $i = 1, 2, \dots, n$): $Poly_i = (kPoly_{i-1} + M_{P_i}) \bmod(p)$, $Poly_0 = 1$, $p = \text{prime}(\text{Wordbits})$, за допомогою схеми Горнера:

$$\begin{aligned}
&M_{P_n} + kM_{P_{n-1}} + \dots + k^{n-1}M_{P_1} + k^n = \\
&(((k + M_{P_1})k + M_{P_2})k + \dots + M_{P_{n-1}})k + M_{P_n}
\end{aligned} \tag{6.50}$$

Крок 3. Шифрування відкритого тексту M на основі MEC у крипто-кодівій конструкції Мак-Еліса:

$$c_x^* = M_i \times G_X^{EC_i} + e, \tag{6.51}$$

де $G_X^{EC_i} = X^i \times G^{EC_i} \times P^i \times D^i$ – публічний ключ.

Формування MAC-коду з використанням Pad на основі CCC на MEC :

$$\begin{aligned}
Y_{L3} &= \left(\left(\left(\sum_{i=1}^m Y_{L2_i} K_{L3_{i_i}} \right) \bmod(\text{prime}(36)) \right) \bmod(2^{32}) \right) \text{xor}(K_{L3_2}), \\
Y &= Y_{L3} \oplus Pad.
\end{aligned} \tag{6.52}$$

Крок 4. Формування автентифікованого повідомлення на основі алгоритму конкатенації: $C_{c_x}^Y = Y \parallel c_x^*$. (6.53)

Структурна схема формування автентифікованого повідомлення на основі НССС на збиткових кодах представлена на рис. 6.14.

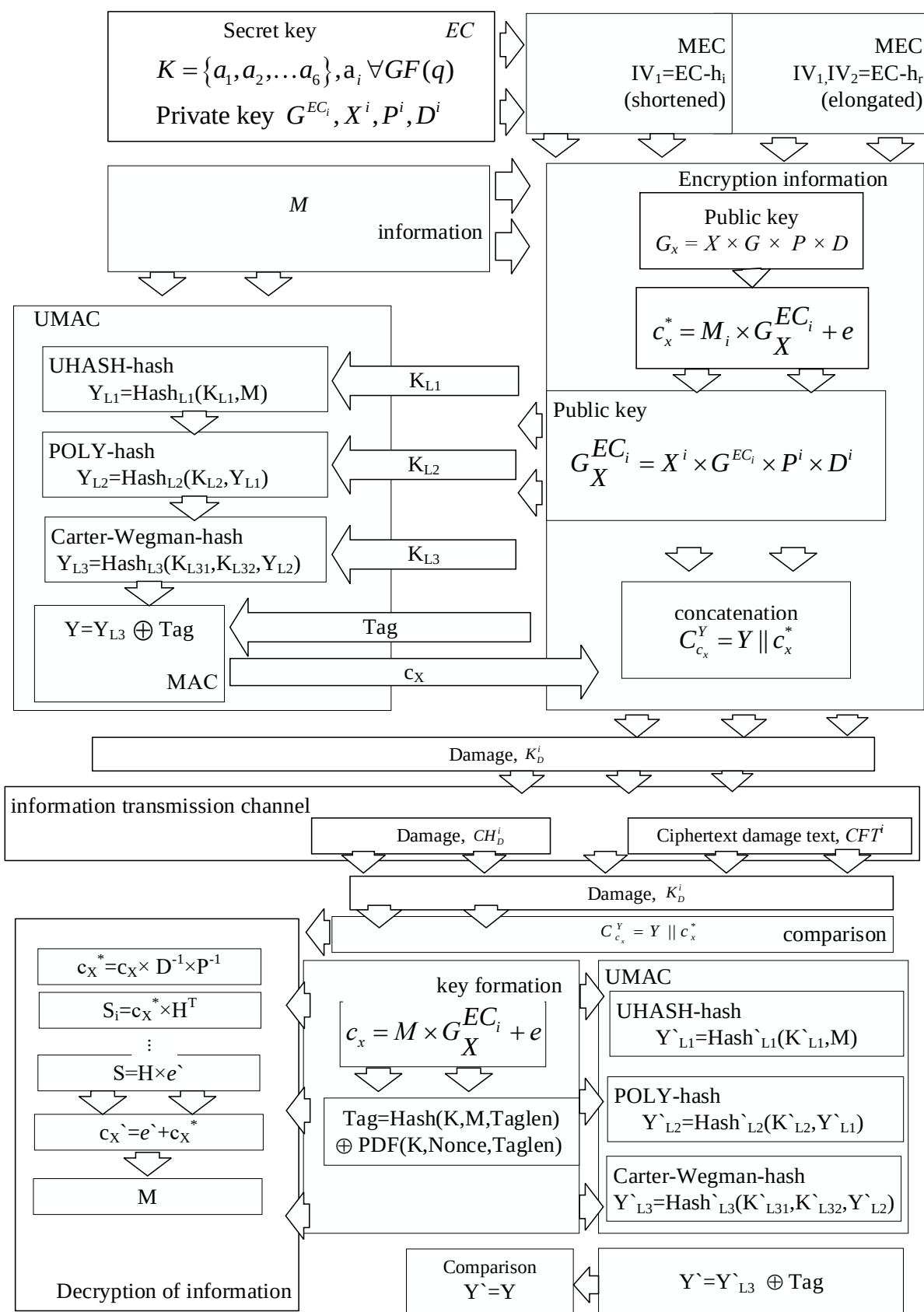


Рис. 6.14. Структурна схема формування автентифікованого повідомлення на

основі HCCC на збиткових кодах (DC)

При використанні в смарт-технологіях запропонованого підходу використовується HCCC Мак-Еліса на збиткових кодах, що дає змогу знизити енергетичні та обчислювальні витрати за збереження стійкості. Для збереження необхідного рівня стійкості використовується технологія нанесення збитку і поділ на два канали: передавання збитку і передавання збиткового тексту.

Основною перевагою в запропонованих способах і протоколах забезпечення послуг безпеки на основі використання збиткових кодів є використання не блочних симетричних шифрів (БШ), а CCC Мак-Еліса для забезпечення криптостійкості збитку та/або збиткового тексту [251].

Таким чином, для формування ключових даних як на стороні Сервера, так і на стороні Клієнта достатньо передати тільки коефіцієнти $a_1, a_2, a_3, a_4, a_5, a_6$, тобто бінарну послідовність із п'яти символів. При цьому обидві сторони зможуть сформувати необхідні матриці і бути готовими до обміну інформацією. Крім цього, немає необхідності використовувати додаткові несиметричні алгоритми (Діфі-Гелмана, RSA) для передавання ключових даних для симетричного алгоритму (у запропонованому випадку використовуються несиметричні криптосистеми зі швидкістю криптоперетворень, які можна порівняти із симетричними криптоалгоритмами). На рис. 6.15 представлено вдосконалену схему протоколу SSL/TLS.

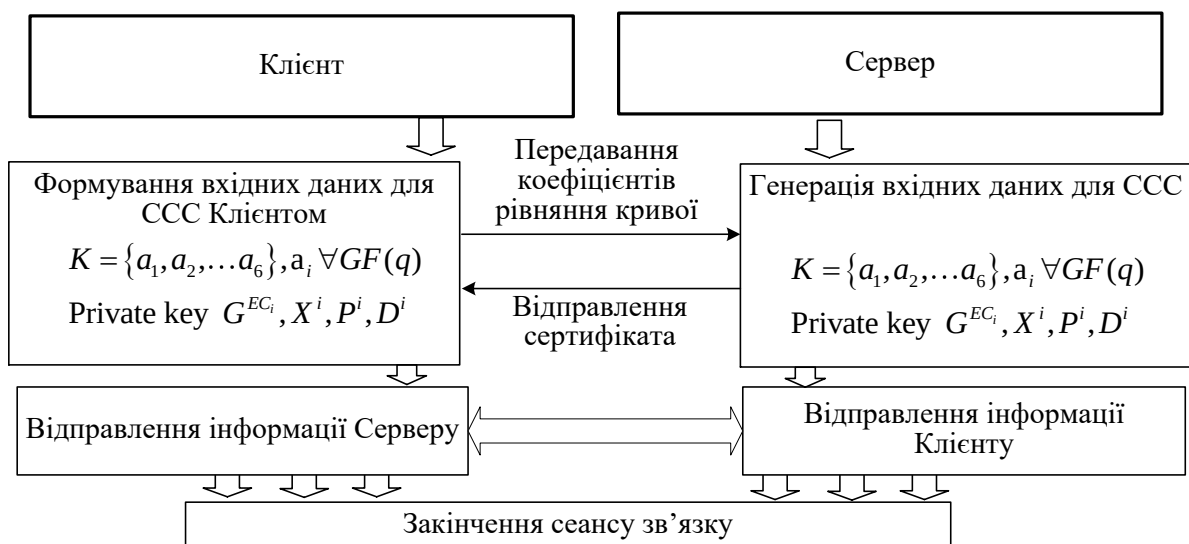


Рис. 6.15. Вдосконалена схема протоколу SSL/TLS

За необхідності «відновлення» сеансу в режимі 0-RTT також немає

необхідності забезпечувати обмін ключовими даними та частиною зашифрованого коду для перевірки правильності визначення ключа, що розділяється. Клієнту достатньо відправити тільки коефіцієнти кривої для того, щоб сервер визначив ключові дані для CCC. Використання вектора помилки e під час передавання інформації дає змогу його розглядати як сеансовий ключ для кожного окремого пакета, що істотно підвищує рівень стійкості.

На рис. 6.16 представлено структурну схему вдосконаленого протоколу SSL/TLS у режимі 0-RTT.

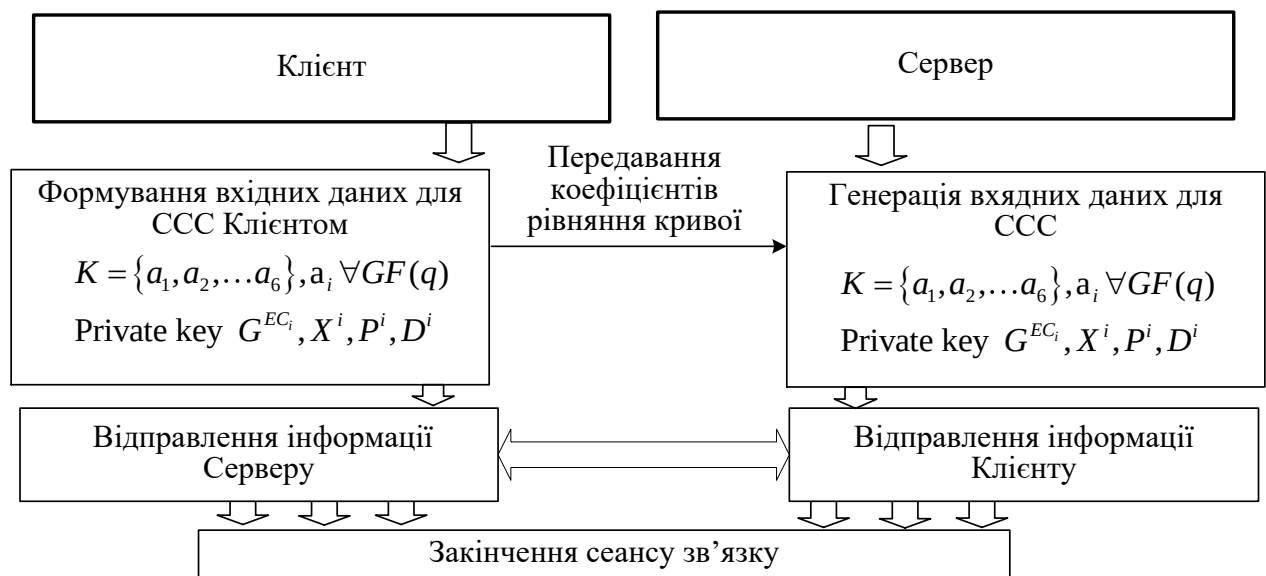


Рис. 6.16. Структурна схема вдосконаленого протоколу SSL/TLS у режимі 0-RTT

Такий підхід усуває можливі вразливості replay attack і дає змогу забезпечити необхідний рівень безпеки (досконала пряма секретність). Використання несиметричних криптоалгоритмів (постквантових алгоритмів – CCC Мак-Еліса на МЕС та збиткових кодах, «спрощує» обмін ключами і не вимагає додаткових енергетичних (обчислювальних) витрат на використання несиметричних криптоалгоритмів.

6.5. Методологія побудови багатоконтурних систем захисту об'єктів критичної інфраструктури

Для побудови методології багатоконтурної системи захисту системи інформації об'єктів критичної інфраструктури пропонується наступна послідовність дій (структурна схема наведена на рис. 6.17):

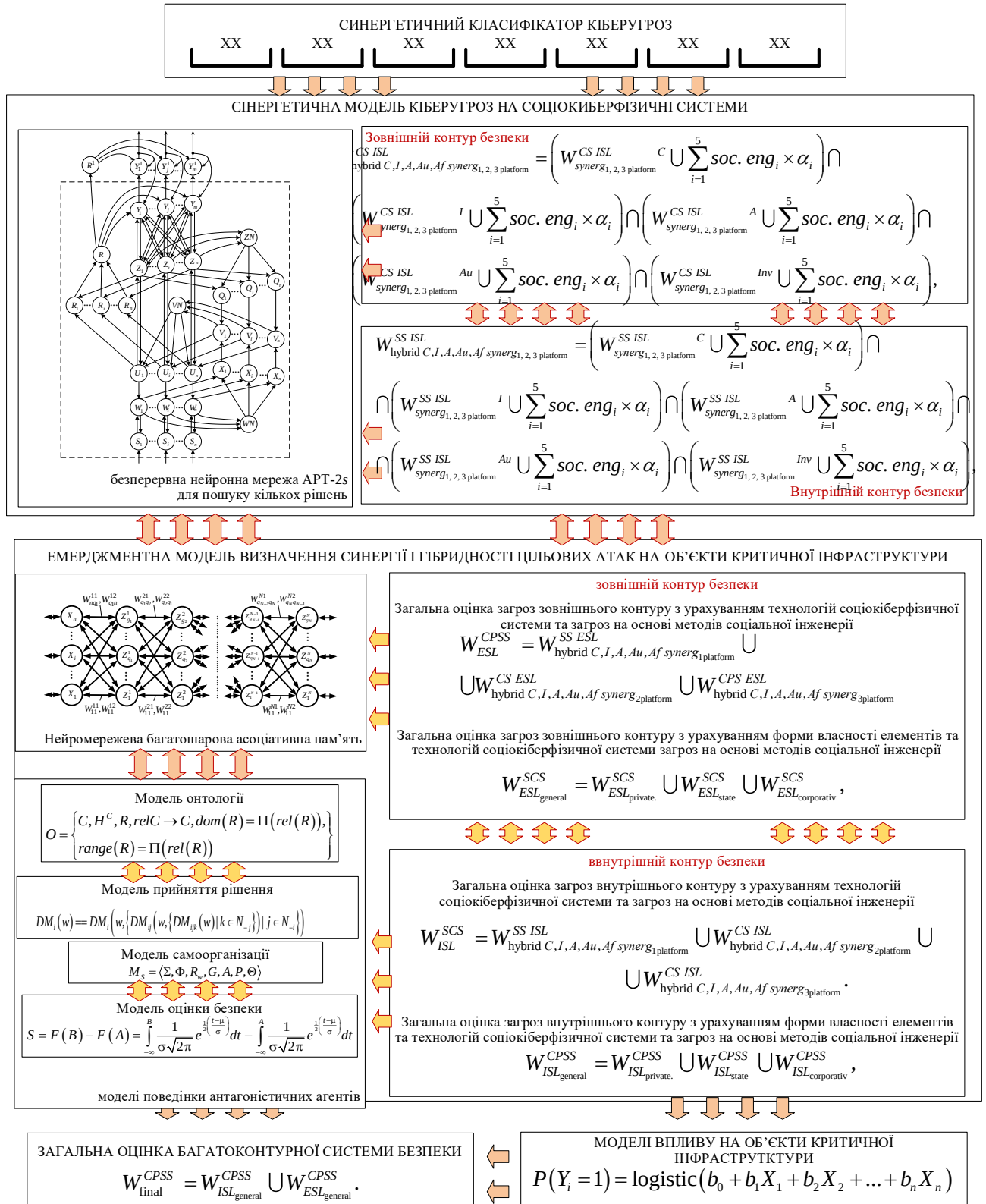


Рис. 6.17. Структурна схема методологія побудови багатоконтурних систем захисту об'єктів критичної інфраструктури

Етап 1. Формується класифікація загроз на основі множини загроз на основних службах безпеки. При цьому враховуються властивості гібридності та загрози синергізму, можливість кожного їх комплексування з методами соціальної інженерії, а також їх вплив на контури об'єктів критичної інфраструктури, при цьому враховується платформеність побудови інфраструктури об'єкта (поєднання кібернетичної з фізичною та платформою соціальних мереж, а також елементами інтернет-речей(смарт-технологій)).

Етап 2. Формування моделей моделювання поведінки агентів систем безпеки, яка реалізується на трьох рівнях (рівень системи безпеки, рівень індивідуальних агентів, рівень групи агентів, що гарантоване забезпечує безпеку бізнес-процесів об'єктів критичної інфраструктури, та дозволяє створити контур бізнес-процесів системи безпеки. Запропонований комплекс моделей дозволяє зробити економічно обґрунтований розподіл обмежених коштів на захист інформаційних ресурсів контуру бізнес-процесів об'єктів критичної інфраструктури.

Етап 3. Оцінка співвідношення загроз до кількості зловмисників та елементів систем об'єктів критичної інфраструктури на основі динамічних моделей Лотки-Вольтери. Пропоновані моделі дозволяють враховувати сучасні фінансові обчислювальні можливості зловмисників.

Етап 4. Оцінка інтегрованого показника поточного рівня безпеки багатоконтурної системи захисту об'єкту критичної інфраструктури.

Етап 5. Модифікація механізмів послуг безпеки у багатоконтурній системі захисту інформації (інтеграція постквантових алгоритмів – CCC). Використання постквантових алгоритмів для забезпечення основних послуг безпеки.

Для оцінки інтегрованого показника безпеки об'єктів критичної інфраструктури пропонується використовувати програмний комплекс оцінки (<https://skl.sspu.sumy.ua/login>), а також запропоновану методику та обмеження:

1 крок. Формування експертних оцінок загроз, їх вплив на послуги безпеки, можливість ознак синергізму та гібридності, а також комплексування методів соціальної інженерії.

Визначення впливу загрози на рівень інфраструктури (моделі ISO/OSI). При цьому формується матриця вагових коефіцієнтів:

$$S_{\text{sthreats}}^* = \left\| S_{\text{sthreats}_{ij}} \right\|,$$

де i – послуги безпеки, j – загроза, $j \in \overline{\forall 1 \dots N}$.

2 крок. Формування матриці відповідності між інформаційними ресурсами та послугами безпеки:

$$S_{\text{inf}}^* = \left\| S_{\text{inf}_{il}} \right\|,$$

де l – інформаційний ресурс, $l \in \overline{\forall 1 \dots L}$. Під час заповнення матриці враховується необхідність надання відповідної послуги безпеки (1 – послуга, 0 – послуга не потрібна).

3 крок. Формування залежності між інформаційними ресурсами та рівнями інфраструктури (моделі ISO/OSI), де циркулює та/або зберігається інформація:

$$S_{\text{ISO}}^* = \left\| S_{\text{ISO}_{kl}} \right\|,$$

де k – наявність та тип зв'язку, елемент інфраструктури (рівень) де зберігається інформація, l – інформаційний ресурс, $l \in \overline{\forall 1 \dots L}$.

4 крок. Формування залежності загроз та інформаційних ресурсів (оцінка критичності інфраструктури):

$$S_{\text{inf/sthreats}}^* = \left\| S_{\text{inf}_{lj}} \right\|,$$

що дозволяє визначити критичність несанкціонованого доступу до того чи іншого інформаційного ресурсу.

5 крок. Формування залежності загроз та елементів інфраструктури (рівень моделі ISO/OSI):

$$S_{\text{sthreats/ISO}}^* = \left\| S_{\text{sthreats/ISO}_{kj}} \right\|,$$

що дозволяє визначити критичні точки в інфраструктурі та заздалегідь визначити превентивні заходи безпеки.

6 крок. Формування оцінки захищеності соціокіберфізичної системи на основі аналізу 2 та 3 кроків (знаходження зв'язку між інформаційними ресурсами, елементами інфраструктури (критичними точками несанкціонованого доступу/витоку інформації) та послугами безпеки).

7 крок. Формування оцінки можливостей чинної системи захисту інформації протистояти загрозам:

$$S_{\text{streats/protection system}}^* = \|S_{\text{streats/protection system}_{qj}}\|,$$

де q – наявність механізму протидії загрозі.

8 крок. Формування оцінки регуляторів та законодавчих актів.

9 крок. Формування оцінки поточного стану системи безпеки. При цьому враховуються результати кроків 7–9.

Подана методика використовує такі вимоги:

Після розрахунку ключових матриць відповідності необхідно визначити синергетичний ефект взаємодії компонентів кібербезпеки (послуг безпеки, інформаційних ресурсів та елементів інфраструктури).

Для матриці відповідності між послугами безпеки та інформаційними ресурсами:

$$S_{\text{inf}}^* = \|S_{\text{inf}_{il}}\|.$$

Після розрахунку матриці визначається рівень важливості кожної послуги безпеки та кожного інформаційного ресурсу:

$$S_{\text{inf}_i} = \sum_{l=1}^8 S_{\text{inf}_{il}}, \quad S_{\text{inf}_l} = \sum_{i=1}^5 S_{\text{inf}_{il}}.$$

Сумарні рівні важливості послуг безпеки та інформаційних ресурсів визначається:

$$S_{inf_i s} = \sum_{i=1}^5 S_{inf_i}, \quad S_{inf_l s} = \sum_{l=1}^8 S_{inf_l}.$$

Визначаються вагові коефіцієнти послуг безпеки інформаційних ресурсів αS_{inf_i} :

$$\alpha S_{inf_i} = \frac{S_{inf_i}}{S_{inf_i s}}, \text{ де } i=1, \dots, 5; \quad \alpha S_{inf_l} = \frac{S_{inf_l}}{S_{inf_l s}}, \text{ де } l=1, \dots, 8.$$

Після цього послуги та ресурси ранжуються за певними ваговими коефіцієнтами від найбільшого до найменшого для визначення найбільш значущих послуг/ресурсів відповідно до матриці їхньої взаємодії.

Далі формується інтегральний показник поточного рівня безпеки для відповідності матриці між послугами безпеки та інформаційними ресурсами.

Для цього визначається абсолютне та відносне значення інтегрального показника:

$$IS_{inf\_abs} = \frac{\sum S_{inf_{il}}}{i \times l}, \quad IS_{inf\_rel} = \frac{IS_{inf\_abs} - S_{inf_{il} \min}}{S_{inf_{il} \max} - S_{inf_{il} \min}},$$

де IS_{inf_abs} – абсолютний інтегральний показник поточного рівня захищеності інформації для матриці відповідності послуг безпеки та інформаційних ресурсів; IS_{inf_rel} – відносний інтегральний показник поточного рівня захищеності інформації для матриці відповідності послуг безпеки та інформаційних ресурсів; $S_{inf_{il}}$ – елементи загальної матриці відповідності послуг безпеки та інформаційних ресурсів; i – кількість послуг безпеки; l – кількість інформаційних ресурсів; $S_{inf_{il} \min}$ – мінімальний елемент матриці відповідності послуг безпеки та інформаційних ресурсів; $S_{inf_{il} \max}$ – мінімальний елемент матриці відповідності послуг безпеки та інформаційним ресурсам.

Ресурси та рівні інфраструктури ранжуються за певними ваговими коефіцієнтами від найбільшого до найменшого для визначення найбільш значущих ресурсів/рівнів відповідно до матриці їхньої взаємодії.

Формується інтегральний показник поточного рівня безпеки для відповідності матриці між інформаційними ресурсами і рівнями інфраструктури. Для цього визначається абсолютне та відносне значення інтегрального показника:

$$IS_{ISO\_abs} = \frac{\sum S_{ISO_{kl}}}{k \times l}, \quad IS_{ISO\_rel} = \frac{IS_{ISO\_abs} - S_{ISO_{kl} \min}}{S_{ISO_{kl} \max} - S_{ISO_{kl} \min}},$$

Загальний інтегральний показник поточного рівня захищеності інформації в аналізованій системі безпеки формується за допомогою аддитивної згортки окремих абсолютних інтегральних показників та мультиплікативної згортки окремих відносних інтегральних показників.

Адитивний інтегральний показник поточного рівня захищеності інформації у системі безпеки об'єкта критичної інфраструктури розраховується за формулою:

$$IS_{add} = IS_{inf\_abs} + IS_{ISO\_abs} + IS_{serv\_abs}.$$

Мультиплікативний інтегральний показник поточного рівня захисту в системі безпеки розраховується за формулою:

$$IS_{mult} = IS_{inf\_rel} + IS_{ISO\_rel} + IS_{serv\_rel}.$$

Таким чином, можна визначити загальну інтегральну оцінку захищеності системи: чим ближче значення відносного показника до 1, тим вищий вплив відповідних факторів на захищеність інформації в системі безпеки об'єкта критичної інфраструктури.

Висновки за главою 6

1. Розроблено модифікації архітектур та алгоритмів функціонування двох безперервних нейронних мереж АРТ-2s та АРТ-2ms, які можуть вибирати та відновлювати зі своєї пам'яті кілька рівноцінних рішень.

2. Розроблено підхід, пов'язаний із введенням в архітектуру нейронної мережі шару додаткових реєструючих нейронів, що дозволяє додати можливість

визначення кількох рівноцінних рішень для класу нейронних мереж, у яких у шарі, що розпізнає кожен з елементів дозволяє визначати тільки одне рішення.

3. На основі аналізу особливостей стабільно-пластичних нейронних мереж АРТ і мереж Хеммінга розглядається розробка архітектури та алгоритмів функціонування нових стабільно-пластичних нейронних мереж Хеммінга, які, на відміну від їх класичних аналогів не здатних донавчатися в процесі свого функціонування та визначати більше одного рішення та дискретних мереж АРТ, що здійснюють ідентифікацію між вхідним і еталонними зображеннями тільки по одиничним компонентам бінарних векторів в яких вони збігаються, здатні розпізнавати нову інформацію, донавчатися в процесі свого функціонування, і мають можливість визначати кілька рішень, використовуючи при цьому параметр подібності між вхідним і еталонними зображеннями, що враховує всі компоненти бінарних векторів, у яких вони збігаються, що дозволяє використовувати їх як альтернативу дискретним нейронним мережам АРТ.

4. *Вперше* на модельному прикладі системи інформаційної безпеки А. А. Пономарьова показано можливість прикладного застосування створеного єдиного математичного підходу для реалізації процедури диференціально-ігрового аналізу надійності системи захисту. Одержані в аналітичному вигляді математичні співвідношення для показників надійності СІБ, що досліджувалася, дозволяють здійснювати процедуру диференціально-ігрового аналізу їх надійності як на етапі проєктування прогресивних систем, так і на етапі штатної експлуатації у рамках визначених замовником або адміністратором з інформаційної безпеки вимог. Як результат замовник СІБ, ще на етапі її розробки має можливість кількісно оцінити надійність системи, що розробляється.

5. *Вдосконалено* математичне забезпечення сучасних систем виявлення атак. Як результат на прикладі *Web-сервера Apache 2.2.10 (Linux|SUSE)*, що **експлуатується** Житомирським військовим інститутом імені С. П. Корольова розроблено диференціально-ігрові шаблони поведінки – диференціально-ігрову модель шаблону нормальної поведінки та відповідний шаблон атаки. Вихідні дані для моделювання відповідних шаблонів одержано за результатами аналізу *log-файлів* й зібрано в період з 01.08.2009 року по 31.01.2010 року. Результати моделювання шаблону нормальної поведінки *Web-сервера* показали збіжність одержаних результатів з відомими результатами експлуатації сервера, чим підтверджено адекватність відповідної диференціально-ігрової моделі.

Розроблена вперше диференціально-ігрова модель шаблону атаки дозволяє з високою достовірністю виявляти *атаки сканування портів, DoS-атаки та DDoS-атаки*.

6. З метою перевірки адекватності диференціально-ігрових моделей було проведено експеримент з аудиту безпеки державних ІР на діючих зразках СІБ, що залучені для їх захисту. Під час проведення експерименту вирішено такі основні задачі: розроблено схему експерименту; зібрано експериментальні дані шляхом пасивного спостереження за динамікою поведінки СІБ під час реалізації КБа II-го класу на державні ІР; на основі методології синтезу та аналізу диференціально-ігрових моделей та методів моделювання оброблено експериментальні дані, розроблено шаблон нормальної поведінки Web- сервера, який забезпечував доступ користувачів до державного ІР та оцінено РЗ ІР та ефективність СІБ в цілому. Одержані в результаті експерименту науково-прикладні результати за реальними експериментальними даними підтверджують адекватність диференціально-ігрових моделей та достовірність методів моделювання. Одержані оцінки РЗ є збіжними з реальними даними.

У результаті проведеного дослідження створено методологію синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів КБн. Створена методологія дозволяє науково обґрунтовано підійти до побудови як програмних, так і програмно-апаратних СІБ, інтегрованих до новостворюваних інформаційних технологій, що призначені для забезпечення в реальному масштабі часу прогнозованого РЗ ІР від кібератак прогнозованого класу. Застосування методології також забезпечує вибір найкращого варіанту побудови прогресивної СІБ, що ґрунтується на інтегральному показнику ефективності системи на базі розроблених моделей та методів моделювання. Створена методологія дозволяє оцінювати поточний та прогнозований РЗ, а також забезпечує прогнозування розвитку динаміки процесу КБн, протягом якого поточний рівень відповідатиме заданому, що сприятиме вибору превентивних стратегій КБз, адекватних умовам протікання ІК в СІБ. Таким чином, одержані теоретичні й практичні результати верифікації та дослідження адекватності диференціально-ігрових моделей та достовірності диференціально-ігрових методів моделювання процесів кібернападу повністю підтверджено.

У практичному плані одержані в роботі результати знайшли впровадження у складові систем управління та безпеки об'єктів критичної інфраструктури, які

є важливі для: національної безпеки та оборони (система забезпечення інформаційної безпеки оперативно-тактичного ракетного комплексу «Гром-2» (ОТРК «Сапсан») /замовник ДП «КБ «Південне» ім. М. К. Янгеля/); економіки України (системи навігації та управління рухом мобільних об'єктів – для оцінювання варіантів побудови перспективних компонент згаданих комплексів /ДП «ЦНДІ навігації і управління» Мінпромполітики України/. Також результати впроваджені на об'єктах критичної інфраструктури, які використовують системи спеціального радіозв'язку. Моделі впроваджені в системах керування кібербезпекою електропостачанням залізниць, в системах виявлення та аналізу вторгнень шляхом впровадження технології побудови шаблонів потенційно небезпечних кібератак – кібератак нульового дня. Розроблені та досліджені спектральні однокритерійні та багатокритерійні моделі та методи виступили підґрунтям для створення нового класу систем кіберзахисту, спроможних в умовах агресивного атакуючого середовища забезпечувати достатній рівень захищеності державних інформаційних ресурсів від кібератак на заданому часовому інтервалі з наперед визначеними показниками стійкості.

7. *Набула подальшого розвитку* модель забезпечення автентичності інформаційних ресурсів, яка ґрунтується на удосконаленому протоколі SSL/TLS на крипто-кодових конструкціях Мак-Еліса та Нідеррайтера, що дозволяє реалізувати послуги безпеки на об'єктах критичної інфраструктури в постквантовий період.

8. Запропонована методологія побудови багатоконтурних систем захисту об'єктів критичної інфраструктури забезпечує можливість отримання об'єктивної оцінки поточного стану захищеності об'єктів критичної інфраструктури. Запропонований програмний комплекс оцінки дозволяє отримати інтегрований показник безпеки, виявити критичні точки вразливості та «можливість» зловмисника отримати доступ до конфіденційної інформації. А запропоновані механізми та протоколи на основі постквантових алгоритмів забезпечать необхідний рівень стійкості та оперативності у період появи повномасштабного квантового комп'ютера.

ВИСНОВКИ

В монографії представлені результати вирішення актуальної науково-прикладної проблеми створення принципово нової методології синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури, що дозволяє підвищити рівень захищеності інформаційних ресурсів цих об'єктів, будувати та/або модернізувати існуючі системи захисту інформації на основі постквантових криптоалгоритмів в умовах комплексування цільових (змішаних) атак з ознаками гібридності та синергізму з методами соціальної інженерії.

Розроблено концепцію побудови синергетичної моделі загроз безпеки інформаційним ресурсам інтелектуальних систем управління та безпеки, базис якої становить трирівнева модель стратегічного управління безпекою об'єктів критичної інфраструктури. Розроблена на основі концепції модель шляхом комплексування складових інформаційної безпеки, кібербезпеки та безпеки інформації відкриває новий напрям у забезпеченні безпеки інформаційних ресурсів об'єктів критичної інфраструктури та враховує величину ризику на кожному рівні для дієвого контролю за виконанням інтелектуальними системами управління інформаційною безпекою критичної інфраструктури своїх функцій.

Вдосконалено модель самоорганізації інтелектуальних системи безпеки, яка відрізняється від чинних поєднанням в єдиній моделі складових прийняття рішень, рефлексивності, адаптації та навчання, а її практична реалізація призводить до появи синергетичного ефекту під час захисту контуру бізнес-процесів об'єктів критичної інфраструктури.

Вперше з системних позицій обґрунтовано належність системи управління об'єктів критичної інфраструктури до систем з критичною кіберінфраструктурою, що обумовлено їх функціонуванням під управлінням інформаційно-комунікаційних систем. Це дозволило розробити графову модель взаємодії систем управління об'єктів критичної інфраструктури, які є важливими для національної безпеки та оборони, а також економіки України. На основі розробленої моделі забезпечується завчасне виявлення таких об'єктів з поміж інших систем управління з обов'язковим оцінюванням їх рівня та категорії важливості для подальшого удосконалення необхідної інституційної бази, вироблення науково обґрунтованих пропозицій для виділення фінансових ресурсів на їх захист, запобігання виникненню ефектів ланцюгових реакцій, створення для цього необхідних організаційних безпекових

структур з чіткою вертикаллю управління, оснащення їх необхідними апаратними та програмними засобами захисту державних інформаційних ресурсів.

Набула подальшого розвитку концепція побудови моделей розподілених систем інформаційної безпеки об'єктів критичної інфраструктури, яка на відміну від відомих ґрунтується на моделях напівмарковських процесів, що дозволяють в реальному масштабі часу відстежувати динаміку протікання процесів кібернападу у ході кіберконфлікту в системі інформаційної безпеки об'єкта під час кібератаки та, на основі накопичених знань, прогнозувати такі безпекові інциденти для визначеного класу систем управління та безпеки у майбутньому. Розроблені на основі концепції диференціально-ігрові моделі дозволяють виробляти відповідні політики безпеки для нового класу систем захисту – інтелектуальних систем безпеки об'єктів критичної інфраструктури.

Набули подальшого розвитку моделі інтелектуального управління трафіком інфокомунікаційних мереж об'єктів критичної інфраструктури, які, на відміну від відомих, враховують різномірний і пульсаційний характер трафіку і дозволяють прийняти рішення щодо його структурної та (або) параметричної оптимізації. Це дало можливість підвищити оперативність передачі інформації в інфокомунікаційних мережах об'єктів критичної інфраструктури.

Удосконалено N-направлену та багатопланову асоціативну пам'ять, котрі, на відміну від чинних нейронних мереж двонаправленої асоціативної пам'яті, здатної зберігати лише пари асоціативних зображень (векторів), дозволяють відновлювати за вхідною інформацією множину з N асоціативних зображень та ланцюжки асоціацій, що дозволило використати їх в базах знань інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури.

Запропоновано механізми кібербезпеки, які базуються на постквантових алгоритмах, котрі формують несиметричні криптосистеми – крипто-кодові конструкції Мак-Еліса та Нідеррайтера на основі алгеброгеометричних (еліптичних, модифікованих еліптичних кодах, збиткових кодах та LDPC-кодах), що дозволяє будувати криптосистеми з різним показником стійкості та забезпечити їх використання у будь-якої системи безпеки об'єктів критичної інфраструктури. Набула подальшого розвитку модель забезпечення автентичності інформаційних ресурсів, яка ґрунтується на удосконаленому протоколі SSL/TLS на крипто-кодових конструкціях Мак-Еліса та Нідеррайтера, що дозволяє реалізувати послуги безпеки на об'єктах критичної інфраструктури в постквантовий період.

Вперше розроблено методологію синтезу моделей інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури в основі якої лежить концепція побудови синергетичної моделі загроз та удосконалений класифікатор загроз, методи забезпечення конфіденційності, цілісності та автентичності державних інформаційних ресурсів на гібридних крипто-кодових конструкціях зі збитковими кодами та удосконалений метод оцінювання рівня безпеки інформаційних ресурсів на основі комплексного показника ефективності інвестицій, що дозволило відкрити новий з позицій управління та безпеки, ефективний з позицій витрачених коштів на управління та безпеку підхід до модернізації чинний та створення перспективних інтелектуальних систем управління та безпеки об'єктів критичної інфраструктури держави.

В цілому, зазначимо, що сучасні об'єкти критичної інфраструктури та взаємодія між ними мають такий ступінь складності, що побудова ефективних систем управління та комплексної безпеки дедалі стає неможливою в межах лише традиційних підходів. Більш того, з неминучим переходом до Індустрії 4.0 складність всіх систем тільки наростатиме.

*Результати впроваджені у розробку та впровадження в складові систем управління та безпеки об'єктів критичної інфраструктури, які є важливі для: **національної безпеки та оборони** (складові комплексної системи захисту інформації ЄАСУ ЗС України – для побудови підсистеми захисту інформації в телекомунікаційній системі комплексу засобів автоматизації АСУ бойового управління силами та засобами авіації, протиповітряної оборони всіх видів ЗС України “Ореанда”, системи та засоби управління військами та зброєю РЕБ, системи військового зв'язку АСУ ракетних військ і артилерії, система забезпечення інформаційної безпеки оперативно-тактичного ракетного комплексу “Гром-2” (ОТРК “Сапсан”); **економіки** України (комплекс засобів захисту інформації телекомунікаційних каналів зв'язку “LDPC-CryptoSuite”, система Інтернет-банкінгу “ELPay” – для управління та безпечного дистанційного обслуговування клієнтів банків з будь-якої точки світу, системи управління розвитком великих енергохімічних комплексів, системи навігації та управління рухом мобільних об'єктів – для оцінювання варіантів побудови перспективних компонент згаданих комплексів.*

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Milov O. Процедурний базис систем кібербезпеки / O. Milov, S. Milevskiy, S. Pohasii, K. Rzaev // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2019. – Т. 5 (57). – С. 72-77. – doi:<https://doi.org/10.26906/SUNZ.2019.5.072>.
2. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
3. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. – Kharkiv: PC TECHNOLOGY CENTER, 2022. – 196 p.
4. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlov, S. Ostapov, O. Laptiev and others. – Kharkiv: PC TECHNOLOGY CENTER, 2023. – 168 p.
5. Захист інформації та економічна безпека підприємства /Євсєєв С.П., Кузнецов О.О., Кавун С.В. - Харків: Вид. ХНЕУ 2009. –360 с.
6. Milov O. Adaptive decision support systems for cyber security //Сучасні інформаційні системи. – 2019. – №. 3,№ 1. – С. 131-135.
7. Теорія сигнально-кодових конструкцій: монографія. Харків: ХУПС/ Наumenko M. I., Stashev Yu. B., Kuznetsov O. O., Yevseiev S. P. – 2008. – 541 с.
8. Yevseiev S., Kots H., Lekarev E. Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system // Eastern-European Journal of Enterprise Technologies. – Т. 6. – №. 4. – С. 84.
9. Yevseiev S. et al. Development of mceliece modified asymmetric crypto-code system on elliptic truncated codes // Eastern-European Journal of Enterprise Technologies. – 2016. – №. 4 (9). – С. 18-26.
10. Yevseiev S., Ponomarenko V., Rayevnyeva O. Assessment of functional efficiency of a corporate scientific-educational network based on the comprehensive indicators of quality of service // Eastern-European Journal of Enterprise Technologies. – 2017. – №. 6 (2). – С. 4-15.
11. Yevseiev S. P. et al. Construction of hybrid security systems based on the crypto-code structures and flawed codes // Eastern-European Journal of Enterprise Technologies. – 2017. 4/9(88). – P. 4–20.
12. Yevseiev S. P. et al. The development of the method of multifactor authentication based on hybrid cryptocode constructions on defective codes // Eastern-European Journal of Enterprise Technologies. – 2017. 5/9(89). С. 19 – 35.
13. Bezhtanko V. et al. Enhancement of productivity of random sequences generation for information protection systems // Eastern-European Journal of Enterprise Technologies. – 2018. 4/9(94). С. 50 –60.

14. Androshchuk A. et al. Improvement of project risk assessment methods of implementation of automated information components of non-commercial organizational and technical systems // *Physics and Engineering*. – 2020. – T. 1. – C. 48-55.
15. Yevseiev S. P. et al. Practical implementation of the Niederreiter modified crypto-code system on truncated elliptic codes // *Eastern-European Journal of Enterprise Technologies*. – 2018. 6/4(96). C. 24 –31.
16. Yevseiev S. et al. Development of Niederreiter hybrid crypto-code structure on flawed codes // *Eastern-European Journal of Enterprise Technologies*. – 2019. – №. 1 (9). – C. 27-38.
17. Yevseiev S. et al. Development of a methodology for building an information security system in the corporate research and education system in the context of university autonomy // *Eastern-European Journal of Enterprise Technologies*. – 2019. – №. 3 (9). – C. 49-63.
18. Milov O. V. et al. Development of the model of the antagonistic agents behavior under a cyber conflict // *Eastern-European Journal of Enterprise Technologies*. – 2019. 4/9(100). C. 6–19.
19. Milov O. V. et al. Development of the interacting agents behavior scenario in the cyber security system // *Eastern-European Journal of Enterprise Technologies* – 2019. 5/9(101). C. 46–57.
20. Milov O. V. et al. Development of a scenario modeling of conflict tools in a security system based on formal grammars // *Eastern-European Journal of Enterprise Technologies* – 2019. 6/9(102). C. 22–39.
21. Yevseiev S. et al. Development and analysis of game-theoretical models of security systems agents interaction // *Eastern-European Journal of Enterprise Technologies*. – 2020. – T. 2. – №. 4. – C. 104.
22. Yevseiev S. et al. Development of a concept for building a critical infrastructure facilities security system // *Eastern-European Journal of Enterprise Technologies*. – 2021. – T. 3. – №. 9. – C. 111.
23. Yevseiev S. et al. Development of a Method for Assessing the Security of Cyber-Physical Systems Based on the Lotka-Volterra Model // *Eastern-European Journal of Enterprise Technologies*. – 2021. – T. 5. – №. 9. – C. 113.
24. Yevseiev S. et al. Development of a method for assessing forecast of social impact in regional communities // *Eastern-European Journal of Enterprise Technologies*. – 2021. – T. 6. – №. 2. – C. 114.
25. Pohasii S. et al. Development of crypto-code constructs based on LDPC codes // *Eastern-European Journal of Enterprise Technologies*. – 2022. – T. 2. – №. 9. – C. 116.
26. Milov O. et al. Development of concepts for the cyber security metrics classification // *Eastern-European Journal of Enterprise Technologies*. – 2022. – T. 4. – C. 4.

27. Yevseiev S. Development of a hardware cryptosystem based on a random number generator with two types of entropy sources // Eastern-European Journal of Enterprise Technologies. 5/9 (119). 2022. P. 6–16.
28. Yevseiev S. et al. Development of the concept for determining the level of critical business processes security // Eastern-European Journal of Enterprise Technologies. – 2023. – Т. 1. – №. 9. – С. 121.
29. Yevseiev S. et al. Modeling the protection of personal data from trust and the amount of information on social networks // EUREKA: Physics and Engineering, (1). – 2021. – С. 24-31.
30. L. Lyubchik, A. Galuza, G. Grinberg. Semi-supervised Learning to Rank with Nonlinear Preference Model // Recent Developments in Fuzzy Logic and Fuzzy Sets: Dedicated to Lotfi A. Zadeh / Ed.: Shahbazova S. N., Sugeno M., and Kacprzyk J. - Cham: Springer International Publishing, 2020. - P. 81 - 103. doi: 10.1007/978-3-030-38893-5_5.
31. Yevseiev S. et al. Research of collision properties of the modified UMAC algorithm on crypto-code constructions // EUREKA: Physics and Engineering, (1). – 2022. – С. 34-43.
32. Petrivskiy V. et al. Development of a modification of the method for constructing energy-efficient sensor networks using static and dynamic sensors // Eastern-European Journal of Enterprise Technologies. – 2022. – Т. 1. – №. 9. – С. 115.
33. Yevseiev S. et al. Development of a Method for Ensuring Confidentiality and Authenticity in Wireless Channels // Eastern-European Journal of Enterprise Technologies. – 2022. – Т. 6. – №. 9. – С. 120.
34. Yevseiev S. et al. Development of an improved SSL/TLS protocol using post-quantum algorithms // Eastern-European Journal of Enterprise Technologies. 2023. 3/9 (123). P. 34–45.
35. Yevseiev S. et al. Development of a multiloop security system of information interactions in socio-cyberphysical systems // Eastern-European Journal of Enterprise Technologies. 2023. 5/9 (125). P. 53–74.
36. Мілов О. В., Євсєєв С. П., Алексєєв В. О. Розробка структурних моделей стійкості інвестиційних проєктів в кібербезпеці // Безпека інформації. – 2018. – Т. 24. – №. 3. – С. 181-194.
37. Yevseiev S. et al. Mathematical models of hybrid crypto code constructions on damaged codes // Сучасні інформаційні технології. – Харків. – 2019. Т.3, № 3. С. 87–103.
38. Yevseiev S., Khvostenko V., Bondarenko K. Розробка комплексного показника якості обслуговування на основі постквантових алгоритмів // Системи управління, навігації та зв'язку. Збірник наукових праць. – 2021. – Т. 3. – №. 65. – С. 82-88.

39. Milov O., Yevseiev S. Methodology of modeling the behavior processes of antagonistic agents in security systems //Ukrainian Scientific Journal of Information Security. – 2019. – Т. 25. – №. 3.
40. Євсєєв С. П. и др. Верифікація методики оцінювання функціональної ефективності передачі банківських інформаційних ресурсів в автоматизованих банківських системах. – 2018.
41. Євсєєв С. П. и др. Дослідження бойових можливостей засобів повітряного нападу противника //Військово-технічний збірник. – 2012. – №. 1. – С. 127-136.
42. Evseev S. P., Tomashevskyy B. P. Two-factor authentication methods threats analysis //Радіоелектроніка, інформатика, управління. – 2015. – №. 1 (32). – С. 52-59.
43. Євсєєв С. П., Остапов С. Е., Корольов Р. В. Використання міні-версій для оцінки стійкості блоково-симетричних шифрів //Ukrainian Scientific Journal of Information Security. – Т. 23. – №. 2. – С. 100-108.
44. Євсєєв С., Федорченко В., Андрощук О. Побудова систем безпеки інформаційно-телекомунікаційних систем на основі комплексного криптографічного підходу //Збірник наукових праць Національної академії Державної прикордонної служби України. Сер.: Військові та технічні науки. – 2017. – №. 2. – С. 258-268.
45. Гришук Р. В., Євсєєв С. П. Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах // Науково-технічний журнал “Безпека інформації”. том.23. № 3. Київ. – 2017. – с. 204 –214.
46. Євсєєв С., Циганенко О. Розробка несиметричної крипто-кодової конструкції Нідеррайтера на модифікованих еліптичних кодах //Системи обробки інформації. – 2018. – №. 2 (153). – С. 127-135.
47. A. Voronin, O. Akhiezer, A. Galuza, I. Lebedeva, Y. Zaitsev, S. Lebedev. Modeling Competitive Interaction “Predator-Prey” on the Example of Two Innovative Processes // 2023 13th International Conference on Advanced Computer Information Technologies (ACIT): Conference Proceedings, Deggendorf, Germany, 21-23 Sept. 2023, pp. 131-134. doi: 10.1109/ACIT58437.2023.10275538
48. Yevseiev S. et al. Research of crypto-code designs construction for using in post quantum cryptography //Development Management. – 2018. – Т. 4. – №. 4.
49. Yevseiev S. et al. Класифікатор кіберзагроз інформаційних ресурсів автоматизованих банківських систем //Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка». – 2018. – Т. 2. – №. 2. – С. 47-67.
50. Hryshchuk R., Yevseiev S. The synergetic approach for providing bank information security: the problem formulation //Безпека інформації. – 2016. – №. 22, № 1. – С. 64-74.

51. Євсєєв С.П. Структурна модель модифікованої системи спеціального призначення // Збірник наукових праць “Спеціальні телекомунікаційні системи та захист інформації”. Видавництво ІСЗЗІ КПІ ім. Ігоря Сікорського. Випуск 1 (35), 2021. С. 25–39.
52. Yevseiev S. et al. Methods of information systems protection // Advanced Information Systems. 2021. Vol. 5, No. 2, p. 131-135.
53. L. Lyubchik, G. Grinberg, M. Lubchick, A. Galuza, O. Akhiezer. Interval Evaluation of Stationary State Probabilities for Markov Set-Chain Models // 2020 10th International Conference on Advanced Computer Information Technologies (ACIT): Conference Proceedings, Deggendorf, Germany, 16-18 Sept. 2020, pp. 82-85. doi: 10.1109/ACIT49673.2020.9208932
54. Yevseiev S. P. Research of criteria of modified non-symmetric crypto-code construction of McEliece on extended elliptic codes // Наука і техніка Повітряних Сил Збройних Сил України. – Харків. – 2019. № 4(37). С. 80–92.
55. Theory and practice of the robotic systems development for military purposes : monograph / V. Zaluzhnyi, S. Shaptala, V. Koval, V. Nazarov, R. Hryshchuk, S. Baranov, O. Semenenko, S. Ostrovskiy : under general ed. Prof. O. Semenenko. – K. : 7BC, 2023. – 280 p.
56. Засади розвитку роботизованих систем у Збройних Силах України : монографія / В. Ф. Залужний, С. О. Шаптала, В. В. Коваль, В. М. Назаров, Р. В. Гришук, О. М. Семененко, С. М. Островський; за заг. ред. проф. О. М. Семененка – К. : 7БЦ, 2023. – 348 с.
57. Model of transformation threats to the state in the military sphere / R. Hryshchuk, O. Levchenko // Methodological aspects of ensuring state security in the mind hybrid threats : monograph. – Košice: Vysoká škola bezpečnostného manažérstva v Košiciach. – 2023. – P. 96 – 104.
58. Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Гришук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Гришука. – Житомир : ЖНАЕУ, 2019. – 280 с.
59. Hryshchuk R. Construction methodology of information security system of banking information in automated banking systems / Hryshchuk R., Yevseiev, S. Shmatko A. – Vienna.: Premier Publishing s. r. o., 2018. – 284 p.
60. Гришук Р. В. Основи кібернетичної безпеки : Монографія / Р. В. Гришук, Ю. Г. Даник ; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.
61. Еволюція поглядів на феномен кібербезпеки / Р. В. Гришук // Інформаційні технології в управлінні, освіті, науці: монографія [під ред. В. С. Пономаренко]. - Х.: ФОП Петров В.В., 2016. - С. 203-216.
62. Гришук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Гришук. – Житомир : РУТА, 2010. – 280 с.
63. Бурячок В. Л. Політика інформаційної безпеки [Текст] : підручник / В. Л.

Бурячок, Р. В. Грищук, В. О. Хорошко ; під заг. ред. проф. В. О. Хорошка. – К. : ПВП «Задруга», 2014. – 222 с.

64. Грищук Р. В. Прикладна криптологія : навчальний посібник / Р. В. Грищук, В. П. Сіденко, О. В. Самчишин ; під заг. ред. проф. Р. В. Грищука. – Житомир : ЖВІ, 2022. – 288 с.

65. Даник Ю. Г. Основи захисту інформації [Текст] : навч. пос. / Ю. Г. Даник, С. Г. Вдовенко, В. І. Шестаков, О.О. Писарчук, Р. В. Грищук, М. В. Куликівський, В. М. Ходаківський. – Житомир : ЖВІ ДУТ, 2015. – 220 с.

66. Бурячок В. Л. Політика інформаційної безпеки [Текст] : навч. пос. / В. Л. Бурячок, Р. В. Грищук, В. О. Хорошко ; під заг. ред. проф. В. О. Хорошка. – К. : ПВП «Задруга», 2014. – 134 с.

67. Determination and Evaluation of Negative Informational and Psychological Influence on the Military Personnel Based on the Quantitative Measure / I. Korobiichuk, P. Snitsarenko, V. Katsalap, R. Hryshchuk // Communities in Social Networking Services. CEUR Workshop Proceedings. – 2019. – Vol. 2392. – P. – 66–78. (Scopus).

68. Hryshchuk R. Method of improving the information security of virtual communities in so-cial networking services / R. Hryshchuk, K. Molodetska, Y. Syerov // Communities in Social Networking Services. CEUR Workshop Proceedings. – 2019. – Vol. 2392. – P. – 23–41. (Scopus).

69. Hryshchuk R. Microprocessor Means for Technical Diagnostics of Complex Systems / R. Hryshchuk, I. Korobiichuk, V. Horoshko, Y. Khokhlacheva // Computer Modeling and Intelligent Systems – 2019. – Vol. 2353. p. 1020–1029. (Scopus).

70. Hryshchuk R. Protection of Information from Leakage by Technical Channels for Sources with Non Range Distribution of Probability / R. Hryshchuk, I. Korobiichuk, S. Ivanchenko, O. Havrylenko, A. Golishevsky, S. Hnatiuk // Computer Modeling and Intelligent Systems – 2019. – Vol. 2353. p. 992–1003. (Scopus).

71. Hryshchuk R. The Throughput of Technical Channels as an Indicator of Protection Dis\crete Sources from Information Leakage / R Hryshchuk, I. Korobiichuk, S. Ivanchenk, O. Roma, A. Golishevsky // Computer Modeling and Intelligent Systems – 2019. – Vol. 2353. p. 523–532. (Scopus).

72. Stasiuk A.I. A mathematical model of cyber security computer network control in power supply of traction substations / A.I. Stasiuk, R. V. Hryshchuk, L.L. Goncharova // Kibernetika i sistemnyi analiz. 2017. Vol. 53, N 3. P. 476–484. (Scopus).

73. Hryshchuk R. Earth Remote Sensing Satellite Navigation Based on Optical Trajectory Measurements / R. Hryshchuk, A. Zavada // Recent Advances in Systems, Control and Information Technology : Springer International Publishing AG, 2017. – № 5. – P. 504–511. (Scopus).

74. Hryshchuk R. Synergetic control of social networking services actors' interactions / R. Hryshchuk, K. Molodetska // Recent Advances in Systems, Control and Information Technology : Springer International Publishing AG, 2017. – № 45. – P. 34–42. (Scopus).

75. Hryshchuk R. Verification Classifier Cyberattacks / R. Hryshchuk, V. Mamarev, V. Okhrimchuk, M. Kachniarz, I. Korobiichuk // *Advanced Solutions in Diagnostics and Fault Tolerant Control* : Springer International Publishing AG, 2017. – № 635. – P. 402–411. (Scopus)
76. Danik Y. Synergistic effects of information and cybernetic interaction in civil aviation / Y. Danik, R. Hryshchuk, S. Gnatyuk // *Aviation*. – 2016. – Vol. 20 (3). – P. 137–144. (Scopus).
77. Zaluzhnyi V. The Armed Forces of Ukraine unmanned systems future development / V. Zaluzhnyi, V., R. Hryshchuk, O. Solomytskyi, I. Hrachov // *Military Science Journal*. – К. : CRSI. – 2024. – Vol. 2 (No. 1). – P. 5–16.
78. Грищук О. М. Верифікація узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної кібератаки / О. М. Грищук, Р. В. Грищук, В. В. Охрімчук // *Телекомунікаційні та інформаційні технології*. – 2020. – № 1 (66). – С. 53–67.
79. Грищук Р. Метод ідентифікації динамічних образів в системах відеоспостереження об'єктів критичної інфраструктури / Р. Грищук, І. Гуменюк, В. Охрімчук // *Безпека інформації*. – 2019. – Том 25. – № 2 – С. 117–121.
80. Грищук Р. Узагальнена модель криптосистеми Фредгольма / Р. Грищук, О. Грищук // *Кібербезпека: освіта, наука, техніка*. – № 4 (4). – 2019. – С. 14–23.
81. Богданович В. Ю. Метод та методика оцінювання ефективності функціонування системи забезпечення інформаційної безпеки / В. Ю. Богданович, Р. В. Грищук, О. В. Левченко // *Зб. наук. пр. Труді університету* – 2018. – №1 (146). – С. 10–18.
82. Богданович В. Ю. Система критеріїв та показників оцінювання ефективності функціонування системи забезпечення інформаційної безпеки / В. Ю. Богданович, Р. В. Грищук, О. В. Левченко // *Зб. наук. пр. Національної академії Державної прикордонної служби України* – 2017. – № 4 (74). – С. 6–23.
83. Грищук Р. В. Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах / Р. В. Грищук, С. П. Євсєєв // *Безпека інформації*. – Том 23. – № 3 – С. 204–214.
84. Грищук Р. В. Проблемні питання створення та використання єдиного інформаційного простору для протистояння зовнішній інформаційній агресії / Р. В. Грищук, І. О. Канкін, Ю. І. Міхєєв // *Інформаційна безпека*. – 2017. – № 1 (25). – С. 5–9.
85. Грищук Р. В. Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування і захисту від неї / Р. В. Грищук, В. О. Хорошко // *Сучасна спеціальна техніка*. – К. : ДНДІ МВС України, 2016. – № 4 (47). – С. 30–36.
86. Грищук Р. В. Кібернетична зброя: класифікація, базові принципи побудови, методи та засоби застосування і захисту від неї / Р. В. Грищук // *Сучасна спеціальна техніка*. – К. : ДНДІ МВС України, 2016. – № 3 (36). – С. 94–101.

87. Гришук Р. В. Верифікація методу скорочення розмірності потоків вхідних даних систем інформаційної безпеки / Р. В. Гришук, В. О. Хорошко, В. М. Мамарєв // *Защита информации*. – К. : НАУ, 2015. – № 22. – С. 99–109.
88. Hryshchuk R. The Synergetic Approach for Providing Bank Information Security: The Problem Formulation / Ruslan Hryshchuk, Sergii Yevseiev // *Безпека інформації*. – 2016. – Том 22. – № 1 – С. 64–74. (Index Copernicus).
89. Гришук Р. В. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак / Р. В. Гришук, В. В. Охрімчук, В. С. Ахтирцева // *Захист інформації*. – 2016. – Том 18. – № 1 – С. 21–29.
90. Гришук Р. В. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак / Р. В. Гришук, В. В. Охрімчук // *Безпека інформації* – 2015. – Том 21. – № 3. – С. 276–282.
91. Гришук Р. В. Математичні комп'ютерно-орієнтовані моделі безпеки інформації обчислювальних мереж тягових підстанцій залізниць / Р. В. Гришук, О. І. Стасюк, Л. Л. Гончарова // *Захист інформації*. – 2015. – Том 17. – № 2 – С. 117–124.
92. Гришук Р. В. Метод побудови класифікатора кібератак на державні інформаційні ресурси / Р. В. Гришук, В. Л. Бурячок, В. М. Мамарєв // *Технологічний аудит та резерви виробництва*. – 2015. – № 1/2 (21). – С. 38–43.
93. Гришук Р. В. Науково-технічне обґрунтування вибору підходу до формування множини інформативних параметрів для систем захисту інформації / Р. В. Гришук, В. Л. Бурячок, В. М. Мамарєв // *Спеціальні телекомунікаційні системи та захист інформації*. – 2014. – № 2 (26). – С. 82–86.
94. Гришук Р. В. Синергія інформаційних та кібернетичних дій / Р. В. Гришук, Ю. Г. Даник // *Труди університету*. – К. : НУОУ, 2014. – № 6 (127). – С. 132–143.
95. Гришук Р. В. Диференціально-ігрове управління розподіленими системами захисту інформації / Р. В. Гришук, В. О. Хорошко // *Інформаційні процеси, технології та системи на транспорті*. – К. : НТУ, 2014. – № 1. – С. 151–157.
96. Гришук Р. В. Аналіз ефективності алгоритмів класифікації кібератак / Р. В. Гришук, В. М. Мамарєв // *Сучасна спеціальна техніка*. – К. : ДНДІ МВС України, 2014. – № 4 (39). – С. 83–89.
97. Grishchuk R. V. Synthesis and Analysis of Multicriterion Differential Gaming Models and Simulation Models of Process of Cyberfalling / Grishchuk R. V., Pilkevich I.A., Kotkov V.I., Bordiuf N.S. // *Science And Education*. – Munich, Germany : Vela Verlag Waldkraiburg, 2013. – Vol. I. – P. 93 – 97.
98. Гришук Р. В. Методика оцінювання рівня небезпеки кібернетичних загроз / Р. В. Гришук, С. В. Чернишук // *Сучасний захист інформації*. – 2013. – Спецвипуск. – С. 23–28.
99. Гришук Р. В. Методологія побудови багатокритерійних диференціально-ігрових моделей та методів / Р. В. Гришук // *Технологічний аудит та резерви виробництва*. – 2013. – № 5 (13). – С. 43–45.
100. Гришук Р. В. Використання диференціальних ігор для оптимізації

управління в системах захисту інформації / Р. В. Гришук, В. О. Хорошко, Ю. Є. Хохлячова // Сучасний захист інформації. – К. : ДУІКТ, 2012. – № 2 (11). – С. 21–27.

101. Гришук Р. В. Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси / Р. В. Гришук, О. Г. Корченко // Захист інформації. – 2012. – № 3 (56). – С. 115–122.

102. Гришук Р. В. Багатокритерійний синтез систем інформаційної безпеки / Р. В. Гришук, І. А. Пількевич, В. О. Хорошко [та ін.] // Східноєвропейський журнал передових технологій. – 2012. – № 5/9 (59). – С. 40–44.

103. Гришук Р. В. Синтез систем інформаційної безпеки за заданими властивостями / Р. В. Гришук // Вісник національного університету “Львівська політехніка”. Серія : Автоматика, вимірювання та керування : зб. наук. пр. – Львів : ЛП, 2012. – № 741. – С. 271–276.

104. Гришук Р. В. Ієрархічна диференціально-ігрова модель в задачах оцінювання ефективності систем захисту інформації / Р. В. Гришук // Інформатика та математичні методи в моделюванні. – Одеса : ОНПУ, 2011. – № 2. – С. 107–115.

105. Гришук Р. В. Диференціально-ігрова гарантовано захищена розподілена система захисту інформації / Р. В. Гришук // Захист інформації. – К. : ДУІКТ, 2011. – № 1 (50). – С. 20–28.

106. Гришук Р. В. Концепція побудови диференціально-ігрових гарантовано захищених розподілених систем захисту інформації / Р. В. Гришук // Сучасний захист інформації. – К. : ДУІКТ, 2011. – № 1 (6). – С. 4–9.

107. Гришук Р. В. Диференціально-ігровий метод аналізу надійності систем захисту інформації, на основі їх спектральних Р-моделей/ Р. В. Гришук // Захист інформації. – К. : ДУІКТ, 2010. – № 4 (49) – С. 66–73.

108. Гришук Р. В. Диференціально-ігрова модель шаблону атаки на Web-сервер / Р. В. Гришук // Збірник наукових праць ВІКНУ ім. Т. Шевченка. – К. : ВІКНУ ім. Т. Шевченка, 2010. – № 21. – С. 104–112.

109. Гришук Р. В. Диференціально-ігрова модель шаблону нормальної поведінки Web-сервера [Електронний ресурс] / Р. В. Гришук // Проблеми телекомунікацій. – 2010. – № 2 (2). – С. 96 – 106. – Режим доступу до журн. : http://pt.journal.kh.ua/2010/2/2/102_gryschuk_web.pdf.

110. Гришук Р. В. Диференціально-ігрові моделі векторної оптимізації процесів нападу на інформацію / Р. В. Гришук // Інформаційна безпека. – Луганськ : СЛУ ім. В. Даля, 2009. – № 1 (3). – С. 79–85.

111. Гришук Р. В. Диференціально-ігрова модель системи захисту інформації / Р. В. Гришук // Інформаційна безпека. – Луганськ : СЛУ ім. В. Даля, 2010. – № 2 (4). – С. 23–29.

112. Гришук Р. В. Неперервна дискретна диференціально-ігрова модель процесу нападу на інформацію / Р. В. Гришук // Вісник ЖДТУ. – Житомир : ЖДТУ, 2010. – № 51 (4). – С. 135–141.

113. Гришук Р. В. GIGW спектральна Р-модель процесу нападу на інформацію / Р. В. Гришук // Вісник СХУЯЕтаП. – Севастополь, СХУЯЕтаП, 2010. – № 1 (33). – С. 188–195.
114. Гришук Р. В. Метод диференціально-ігрового Р-моделювання процесів нападу на інформацію / Р. В. Гришук // Інформаційна безпека. – Луганськ : СХУ ім. В. Даля, 2009. – № 2 (2). – С. 128–132.
115. Гришук Р. В. Метод гібридного Р-L-моделювання процесів нападу на інформацію / Р. В. Гришук // Збірник наукових праць ВІКНУ ім. Т. Г. Шевченко. – К. : ВІКНУ ім. Т. Г. Шевченко, 2009. – № 46. – С. 90–94.
116. Гришук Р. В. Нетейлорівська модель процесу нападу на інформацію / Р. В. Гришук // Вісник Східноукраїнського національного університету ім. Володимира Даля. – Луганськ : СХУ ім. В. Даля, 2009. – № 6 (136). – С. 60–64.
117. Гришук Р. В. Р-моделювання процесів нападу на інформацію при нестационарній природі потоків захисних дій та інформаційних атак / Р. В. Гришук // Системи обробки інформації. – Х. : ХУПС ім. І. Кожедуба, 2009. – № 7 (79). – С. 98–101.
118. Гришук Р. В. GIGW гібридна Р-L-модель процесу нападу на інформацію / Р. В. Гришук, В. О. Хорошко // Вісник СХУЯЕтаП. – Севастополь, СХУЯЕтаП, 2009. – № 2 (30). – С. 153–160.
119. Гришук Р. В. Методика оцінювання гарантованого рівня захищеності технічних об'єктів / Р. В. Гришук, О. О. Хмара // Системи озброєння і військова техніка. – Х. : ХУПС ім. І. Кожедуба, 2009. – 2 (18). – С. 74–78.
120. Гришук Р. В. Верифікація і дослідження спектральних Р- та гібридних Р-L-моделей процесу нападу на інформацію / Р. В. Гришук // Вісник ЖДТУ. – Житомир : ЖДТУ, 2009. – № 49 (II). – С. 77–85.
121. Гришук Р. В. Багатокритеріальна модель процесу нападу на інформацію / Р. В. Гришук // Захист інформації. – К. : НАУ, 2009. – № 16. – С. 290–295.
122. Гришук Р. В. Застосування багатокритерійної моделі інтегральної оптимальності в задачах моделювання процесів нападу на інформацію Р-перетвореннями / Р. В. Гришук // Захист інформації. – К. : ДУІКТ, 2009. – № 3 (44). – С. 44–52.
123. Гришук Р. В. Спектральна модель процесу нападу на інформацію / Р. В. Гришук // Захист інформації. – К. : ДУІКТ, 2009. – № 2 (43). – С. 71–81.
124. Гришук Р. В. Диференціально-тейлорівська модель перебування технічного об'єкта під впливом методів несанкціонованого доступу / Р. В. Гришук // Захист інформації. – К. : ДУІКТ, 2009. – № 1 (42). – С. 19–27.
125. Гришук Р. В. Диференціально-ігрова розгалужена спектральна модель процесу нападу на інформацію / Р. В. Гришук // Вісник ЖДТУ. – Житомир : ЖДТУ, 2009. – № 48 (I). – С. 152–159.
126. Гришук Р. В. Диференціально-ігрова модель кількісної оцінки захищеності технічних об'єктів / Р. В. Гришук // Захист інформації. – К. : ДУІКТ,

2008. – № 40 (спец. випуск). – С. 24–29.

127. Патент на винахід (Україна): Пат. 103546 Україна, МПК7 H04K 3/00, H03B 29/00. Спосіб захисту інформації [Текст] / Грищук Р. В., Хорошко В. О., Рибальський О. В. (Україна) ; заявник та патентовласник Грищук Р.В. – № а201202038 ; заявл. 22.02.12 ; опубл. 25.05.13, Бюл. № 20. – 4 с. <http://uapatents.com/patents/grishhuk-ruslan-valentinovich>.

128. Пат. 123379 Україна, МПК51 (2018.01) G09C 1/00. Спосіб криптографічного перетворення інформації з використанням укорочених кодів [Текст] Євсєєв С. П., Грищук Р. В., Король О. Г., Коц Г. П., Корольов Р. В., Ковтун В. Ю. Ковтун М. Г., Охріменко А. О. (Україна) ; заявник та патентовласники Євсєєв С. П., Грищук Р. В., Король О. Г., Коц Г. П., Корольов Р. В., Ковтун В. Ю. Ковтун М. Г., Охріменко А. О. – №u201708995; заявл. 11.09.2017; опубл. 26.02.2018, 26.02.2018, Бюл. № 4. – 2 с.

129. Пат. 123375 Україна, МПК51 (2018.01) G09C 1/00. Спосіб криптографічного перетворення інформації з використанням подовжених кодів [Текст] Євсєєв С. П., Грищук Р. В., Король О. Г., Коц Г. П., Корольов Р. В., Ковтун В. Ю. Ковтун М. Г., Охріменко А. О. (Україна) ; заявник та патентовласники Євсєєв С. П., Грищук Р. В., Король О. Г., Коц Г. П., Корольов Р. В., Ковтун В. Ю. Ковтун М. Г., Охріменко А. О. – №u201708985; заявл. 11.09.2017; опубл. 26.02.2018, 26.02.2018, Бюл. № 4. – 2 с.

130. Патент на корисну модель 74414 Україна, МПК G06G 7/60. Нейромережевий пристрій для розпізнавання та класифікації динамічних процесів / В.Д. Дмитрієнко, О.Ю. Заковоротний; заявник та володар патенту НТУ «ХПІ». - № u 201 2 0 4749 ; заявл . 17.04.2012 ; опубл. 25.10.2012, бюл. №20. - 4 с.

131. Патент на корисну модель 93316 Україна, МПК G06G 7/60. Нейромережевий пристрій для розпізнавання зображень / В.Д. Дмитрієнко , О.Ю. Заковоротний; заявник та володар патенту НТУ «ХПІ». - № u 2014 04328 ; заявл. 22.04.2014; опубл. 25.09.2014, бюл. №18. - 4 с.

132. Заковоротний О.Ю. Дискретна нейронна мережа АРТ, яка використовує ідеї імунокомп'ютингу / В.Д. Дмитрієнко, О.Ю. Заковоротний // Вісник НТУ "ХПІ". – Харків: НТУ «ХПІ», 2012. – Вип . 62 (968). – С. 52 - 63 .

133. Заковоротний О.Ю. Дискретна нейронна мережа АРТ з використанням відстані Хеммінга / В.Д. Дмитрієнко , О.Ю. Заковоротний , М.В. Мезенців , Г.В. Гейко // Виник НТУ « ХПІ ». – Харків: НТУ « ХПІ», 2016. – Вип. 21. - С. 29 - 40 .

134. Заковоротний О.Ю. Нейронна мережа, що використовує відстань Хеммінга для розпізнавання зображень на межах кількох класів/ В.Д. Дмитрієнко, О.Ю. Заковоротний // Вісник НТУ "ХПІ". – Харків : НТУ «ХПІ», 2013. – Вип . 39 (1012). - С. 57 - 67.

135. Основи нейрокомп'ютингу / В.Д. Дмитрієнко, О.Ю. Заковоротний, В.І. Носков, М.В. Мезенцев // Навчальний посібник. - Харків: НТМТ, 2014. - 140 стор .
136. Zakovorotnyi O.Y. Neural Networks Art: Solving Problems with Multiple Solutions and New Teaching Algorithm / V.D. Dmitrienko, O.Y. Zakovorotnyi, S.Yu. Leonov, I.P. Khavina // The Open Neurology Journal . - 2014. - № 8. - P. 15 - 21.
137. Заковоротний О.Ю. Нейронна мережа Хеммінгу для вирішення задач з кількома рішеннями / В.Д. Дмитрієнко , О.Ю. Заковоротний, С.Ю. Леонов // Вісник НТУ "ХПІ". – Харків: НТУ «ХПІ», 2017. – Вип. 50 (1271).
138. Заковоротний О.Ю. Архітектури та алгоритми функціонування нейронних мереж Хеммінга та Хебба, здатних донавчатися та розпізнавати нову інформацію / В.Д. Дмитрієнко, О.Ю. Заковоротний // Радіоелектроніка, інформатика, управління. Науковий журнал. - Запоріжжя: ЗНТУ, 2014. - №2/2014. - С. 100 - 109.
139. Zakovorotnyi O.Y. Stable-plastic neural network, which defines several solutions and new information on its inputs / V.D. Dmitrienko, O.Y. Zakovorotniy, S.Y. Leonov // International Journal of Computer Aided Engineering and Technology. Volume 16, Issue 4, Pages 468 – 477. 2022.
140. Патент на корисну модель 93317 Україна, МПК G06G 7/00. Нейромережевий пристрій класифікації динамічних процесів з можливістю блокування частини вхідного зображення / В.Д. Дмитрієнко, О.Ю. Заковоротний; заявник та володар патенту НТУ «ХПІ». - № u 2014 04346; заявл. 22.04.2014; опубл. 25.09.2014, бюл. №18. - 9 с.
141. Заковоротний О.Ю. Розробка багатонаправленої асоціативної пам'яті на основі дискретних нейронних мереж адаптивної резонансної теорії / О.Ю. Заковоротний // Збірник наукових праць Харківського університету Повітряних сил. - Х.: ХУПС і мені Івана Кожедуба, 2016. - Вип. 2(47). - С. 91 - 96.
142. Заковоротний О.Ю. Нейронні мережі Хеммінга і Хебба, здатні донавчатися / В.Д. Дмитрієнко, О. Ю. Заковоротний, В.О. Бречко // Вісник НТУ "ХПІ". – Харків : НТУ «ХПІ», 2013. – Вип . 19. - С. 30 - 45.
143. Патент на винахід 108009 Україна , МПК G06K 9/00. Нейромережевий пристрій для розпізнавання та класифікації зображень на кордоні кількох класів / В.Д. Дмитрієнко , О.Ю. Заковоротний, І.П. Хавіна; заявник та володар патенту НТУ «ХПІ». - №a2013 08531; заявл. 08.07.2013; опубл. 10.03.2015, бюл. №5. - 7 с.
144. Комп'ютерна програма інтелектуального розпізнавання зображень / О.Ю. Заковоротний , Д.О. Пелих , М.С. Шаповалов // Свідectво про реєстрацію авторського права на твір № 66142. – Зареєстр. у Держ. службі інтелектуальної власності України 17.06.2016.
145. Патент на корисну модель 100498 Україна , МПК G06 K 9/00. Пристрій багатонаправленої нейромережевої пам'яті / О.Ю. Заковоротний;

заявник та володар патенту НТУ «ХПІ». - № u201501554; заявл. 23.02.2015; опубл. 27.07.2015, бюл. №14 . - 8 с.

146. Патент на винахід 108949 Україна, МПК G06 G 7/60. Пристрій *N*-направленої асоціативної пам'яті / В.Д. Дмитрієнко, О.Ю. Заковоротний, В.О. Бречко; заявник та володар патенту НТУ «ХПІ». - №a201402642; заявл. 17.03.2014; опубл. 25.06.2015, бюл. №12 . - 8 с.

147. Заковоротний О.Ю. Багатошарова нейромережева пам'ять, що зберігає ланцюжки асоціацій / В.Д. Дмитрієнко, Р.П. Мігущенко, О.Ю. Заковоротний, В.О. Бречко // Вісник НТУ «ХПІ». – Х.: НТУ «ХПІ», 2015. – Вип. 33. - С. 48 - 58.

148. Патент на винахід 108947 Україна, МПК G06 G 7/60. Пристрій багатошарової двонаправленої асоціативної пам'яті / В.Д. Дмитрієнко, О.Ю. Заковоротний, І.П. Хавіна, В.О. Бречко; заявник та володар патенту НТУ «ХПІ». - № а 201402402; заявл. 11.03.2014; опубл. 25.06.2015, бюл. №12. - 8 с.

149. Комп'ютерна програма «Комп'ютерна програма для дослідження нейромережевої багатошарової двонаправленої асоціативної пам'яті» / В.Д. Дмитрієнко, О.Ю. Заковоротний, В.О. Бречко // Свідectво про реєстрацію авторського права на твір № 57996. - Зареєстр. у Держ . службі інтелектуальної власності України 05.01.2015.

150. Заковоротний О.Ю. Розробка архітектури та алгоритмів функціонування нейромережевої пам'яті з можливістю корекції результатів / О.Ю. Заковоротний // Науково-технічний журнал «Наука і техніка повітряних сил Збройних сил України». - Харків: ХУПС , 2016. - Вип . 2 (23). - С. 145 - 1 49 .

151. Патент на винахід 108712 Україна, МПК G06 G 7/60. Пристрій багатошарової асоціативної пам'яті з керуючими нейронами / В.Д. Дмитрієнко, О.Ю. Заковоротний, І.П. Хавіна, В.О. Бречко; заявник та володар патенту НТУ «ХПІ». - № а 201404330 ; заявл. 22.04.2014; опубл. 25.05.2015, бюл . №10 . - 11 с.

152. Патент 33321 Україна, МПК G06G 7/00. Пристрій двонаправленої аналого-дискретної асоціативної пам'яті / Дмитрієнко В.Д., Заковоротний О.Ю. Романов О.Ю.; заявник та володар патенту НТУ «ХПІ». -№ u 200800804; заявл. 23.01.2008; опубл. 10.06.2008, Бюл . №11.

153. Патент 18624 Україна, МПК G06G 7/00. Пристрій двонаправленої асоціативної пам'яті / Дмитрієнко В.Д. , Заковоротний О.Ю.; заявник та володар патенту НТУ «ХПІ». -№ u200605460; заявл. 19.05.2006; опубл. 15.11.2006, Бюл . № 11. - 5

154. Заковоротний О.Ю. Розробка *N*-направленої дискретної асоціативної пам'яті / О.Ю. Заковоротний // Міжнародний науково-технічний журнал «Вимірювальна та обчислювальна техніка в технологічних процесах». – Хмельницький: ХНУ, 2016. – №1 (54). - С. 101 - 108.

155. Патент на корисну модель 68375 Україна, МПК G06K9/00. Пристрій розпізнавання класифікації образів / В.Д. Дмитрієнко , О.Ю. Заковоротний , І.І.

Котов; заявник та володар патенту НТУ «ХПІ». - № у 2011 10107; заявл. 16.08.2011; опубл. 26.03.2012, бюл. № 6. - 6 с.

156. Патент на корисну модель 93337 Україна, МПК G06G 7/00. Нейрозетковий пристрій класифікації динамічних процесів / В.Д. Дмитрієнко О.Ю. Заковоротний; заявник та володар патенту НТУ «ХПІ». - № у 2014 04567; заявл. 28.04.2014; опубл. 25.09.2014, бюл. № 18. - 9 с.

157. Патент на корисну модель 47481 Україна, МПК G06G7/00. Пристрій аналогової двонаправленої асоціативної пам'яті / В.Д. Дмитрієнко, О.Ю. Заковоротний, Р.С. Мазурика; заявник та володар патенту НТУ «ХПІ». - № у 2009 07222; заявл. 10.07.2009; опубл. 10.02.2010, Бюл. № 3. - 7 с.

158. Патент на корисну модель 62606 Україна, МПК G06G7/00. Пристрій безперервної двоспрямованої асоціативної пам'яті / В.Д. Дмитрієнко, О.Ю. Заковоротний, І.О. Білевцов; заявник та володар патенту НТУ «ХПІ». - № у 201015230; заявл. 17.12.2010; опубл. 12.09.2011, бюл. № 17. - 11 с.

159. Кучук Г. А. Інформаційні технології управління інтегральними потоками даних в інформаційно-телекомунікаційних мережах систем критичного призначення. Харків. ун-т Повітр. Сил ім. Івана Кожедуба, 2013. 263 с. ISBN 978-617-7188-18-5. Номер НБУВ: ВА779315

160. Kuchuk H., Datsenko S. Biometric authentication utilizing convolutional neural networks. *Сучасні інформаційні системи*. 2023. Т. 7, № 2. С. 87-91. DOI: <https://doi.org/10.20998/2522-9052.2023.2.12>

161. Kuchuk H., Yaloveha, V., Podorozhniak, A., Garashchuk, N. Performance comparison of cnns on high-resolution multispectral dataset applied to land cover classification problem. *Radioelectronic and Computer Systems*. 2023, 2023(2(106)). P. 107–118. DOI: <https://doi.org/10.32620/reks.2023.2.09>

162. Kuchuk H., Kuchuk, N., Mozhaiev, O., Mozhaiev, M., Semenov, S., Brusakova, O., Gnusov, Y. Devising a method for balancing the load on a territorially distributed foggy environment. *Eastern-European Journal of Enterprise Technologies*. 2023, 1(4-121). P. 48–55. DOI: <https://doi.org/10.15587/1729-4061.2023.274177>

163. Kuchuk H., Semenov, S., Mozhaiev, O., Kuchuk, N., Mozhaiev, M., Gnusov, Y., Chyrva, Y. Devising a procedure for defining the general criteria of abnormal behavior of a computer system based on the improved criterion of uniformity of input data samples. *Eastern-European Journal of Enterprise Technologies*. 2022. 6(4-120). P. 40–49. DOI: <https://doi.org/10.15587/1729-4061.2022.269128>

164. Kuchuk H., Kuchuk, N., Kovalenko, A., Levashenko, V., Zaitseva, E. Mathematical Methods of Reliability Analysis of the Network Structures: Securing QoS on Hyperconverged Networks for Traffic Anomalies. *Lecture Notes in Electrical Engineering*, 2022, 831, pp. 223–241. DOI: https://doi.org/10.1007/978-3-030-92435-5_13

165. Kuchuk H., Kovalenko, A. Methods to Manage Data in Self-healing Systems. *Studies in Systems, Decision and Control*, 2022, 425, pp. 113–171, DOI: https://doi.org/10.1007/978-3-030-96546-4_3
166. Kuchuk H., Ruban, I., Kovalenko, A., Lukova-Chuiko, N., Martovytsky, V. Method for Determining the Structural Reliability of a Network Based on a Hyperconverged Architecture. *Studies in Computational Intelligence*, 2021, 976, pp. 147–163. DOI: https://doi.org/10.1007/978-3-030-74556-1_
167. Kuchuk H., Terenyk, D. SQL & NOSQL database comparison by case designing affiliate system report. *Radioelectronic and Computer Systems*. 2020. No 1, pp. 83-89. DOI: <https://doi.org/10.32620/reks.2020.1.08>
168. Kuchuk H., Mukhin, V., Kuchuk, N., Kosenko, N., Kosenko, V. Decomposition Method for Synthesizing the Computer System Architecture. *Advances in Intelligent Systems and Computing*, 2020, No. 938, p. 289-300. DOI: https://doi.org/10.1007/978-3-030-16621-2_27
169. Kuchuk H., Kovalenko A., Bnar Fareed Ibrahim, Ruban I. Adaptive Compression method for Video Information. *International Journal of Advanced Trends in Computer Science and Engineering*. 2019. Vol. 8, No. 1.2, pp. 66-69. DOI: <https://doi.org/10.30534/ijatcse/2019/1181.22019>
170. Kuchuk H., Kovalenko A., Komari, I.E., Svyrydov, A., Harchenko V.S. Improving big data centers energy efficiency: Traffic based model and method. *Studies in Systems, Decision and Control*. Springer, 2019, pp. 161-183. DOI: https://doi.org/10.1007/978-3-030-00253-4_8
171. Kuchuk H., Kovalenko, A., Kharchenko, V., Shamraev, A. Resource-oriented approaches to implementation of traffic control technologies in safety-critical I&C systems. *Studies in Systems, Decision and Control*, 2017, 105, pp. 313–337. DOI: https://doi.org/10.1007/978-3-319-55595-9_15
172. Кучук Г.А., Бондаренко Б. В. Метод взаємодії компонентів комп'ютерних систем при сповіщенні про надзвичайну ситуацію. *Системи управління, навігації та зв'язку*. 2023. Вип. 1 (71). С. 167-170. doi: <https://doi.org/10.26906/SUNZ.2023.1.167>
173. Кучук Г.А., Петровська І. Ю. Розподіл обчислювальних ресурсів у хмарних системах. *Системи управління, навігації та зв'язку*. 2022. Вип. 2 (68). С. 75-78. doi: <https://doi.org/10.26906/SUNZ.2022.2.075>
174. Kuchuk H., Petrovska I. Static allocation method in a cloud environment with a service model IAAS. *Сучасні інформаційні системи*. 2022. Том 6, № 3. С. 99-106. DOI: <https://doi.org/10.20998/2522-9052.2022.3.13>
175. Kuchuk H., Rezanov B. Modelling the process of two-factor authentication. *Сучасні інформаційні системи*. 2022. Том 6, № 2. С. 10-15. DOI: <https://doi.org/10.20998/2522-9052.2022.2.02>
176. Кучук Г.А., Ткачов В. М., Коваленко А. А., Ні Я. С. Метод забезпечення живучості високомобільної комп'ютерної мережі.

Сучасні інформаційні системи. 2021. Том 5, № 2. С. 159-165. DOI: <https://doi.org/10.20998/2522-9052.2021.2.22>

177. Кучук Г.А., Пустовойтов П. Є., Лебедев О. Г., Лимаренко В. В. Метод розрахунку коефіцієнта кореляції фрактального трафіка. Системи управління, навігації та зв'язку. 2021. Вип. 2 (64). С. 148-152. doi: <https://doi.org/10.26906/SUNZ.2021.2.148>

178. Кучук Г.А., Коваленко А. А., Ткачов В. М. Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання. Системи управління, навігації та зв'язку. 2021. Вип. 1 (63). С. 90-95. doi: <https://doi.org/10.26906/SUNZ.2021.1.090>

179. Кучук Г.А., Ліберг І. Г., Можаяєв О. О. Короткострокове прогнозування трафіка при статистичному мультиплексуванні. Системи управління, навігації та зв'язку. 2020. Вип. 4 (62). С. 47-50. doi: <https://doi.org/10.26906/SUNZ.2020.4.047>

180. Кучук Г.А., Левашенко В. Г., Ляшенко О. С. Побудова системи підтримки прийняття рішень на основі нечітких даних. Сучасні інформаційні системи. 2020. Т. 4, № 4. С. 48-56. DOI: <https://doi.org/10.20998/2522-9052.2020.4.07>

181. Кучук Г.А., Коваленко А.А., Рубан І.В. Використання часових шкал при апроксимації довжини черг комп'ютерних мереж. Сучасний стан наукових досліджень та технологій в промисловості. 2018. № 2 (6). С. 12-16. DOI: <https://doi.org/10.30837/2522-9818.2018.4.012>

182. Кучук Г.А., Бульба С. С. Давидов В. В. Метод розподілу ресурсів між композитними застосунками. Системи управління, навігації та зв'язку. – Полтава. ПНТУ, 2018. – Вип. 4(50). – С. 99-104. DOI: <https://doi.org/10.26906/SUNZ.2018.4.099>

183. Кучук Г.А., Коваленко А.А., Свиридов А.С. Метод перерозподілу пропускної здатності критичної ділянки мережі на основі удосконалення ON/OFF-моделі трафіку. Сучасні інформаційні системи. 2018. Том 2, № 2. С. 139-144. DOI: <https://doi.org/10.20998/2522-9052.2018.2.24>

184. Кучук Г.А., Коваленко А.А. Методи синтезу інформаційної та технічної структур системи управління об'єктом критичного застосування. Сучасні інформаційні системи. 2018. Том 2, № 1. С. 22-27. DOI: <https://doi.org/10.20998/2522-9052.2018.1.04>

185. Кучук Г.А., Коваленко А.А. Сучасний стан та тенденції розвитку комп'ютерних систем об'єктів критичного застосування. Системи управління, навігації та зв'язку. Полтава. ПНТУ, 2018. Вип. 1(47). С. 110-113. DOI: <https://doi.org/10.26906/SUNZ.2018.1.110>

186. Ruban I., Kuchuk H., Kovalenko A. Redistribution of basic stations in mobile communication networks. Сучасний стан наукових досліджень та технологій в промисловості. 2017. № 1 (1). С. 75-81. DOI:

<https://doi.org/10.30837/2522-9818.2017.1.075>

187. Кучук Г.А., Кассем Халіфе, Криховецький Г.Я. Оцінка вразливості системного програмного забезпечення. Системи управління, навігації та зв'язку. Полтава. ПНТУ, 2017. Вип. 6(46). С. 141-144. URL: http://nbuv.gov.ua/UJRN/suntz_2017_6_33

188. Кучук Г.А., Коваленко А.А., Лукова-Чуйко Н.В. Метод мінімізації середньої затримки пакетів у віртуальних з'єднаннях мережі підтримки хмарного сервісу. Системи управління, навігації та зв'язку. Полтава. ПНТУ, 2017. – Вип. 2(42). С. 117-120. URL: <https://journals.nupp.edu.ua/sunz/article/view/733>

189. Кучук Г.А., Коваленко А.А. Використання методів зміни простору рішень для оптимізації управління трафіком мультисервісних мереж. Системи обробки інформації. 2016. Вип. 5 (142). С. 128-132. URL: http://nbuv.gov.ua/UJRN/soi_2016_5_27

190. Кучук Г.А., Раковська Н. Х., Загайнов С. О., Савченко О. С. Метод розподілу потоків даних в мультисервісній мережі з безпро Системи обробки інформації. 2014. Вип. 4(120). С. 164-169. URL: http://nbuv.gov.ua/UJRN/soi_2014_4_35 виходовою компонентою.

191. Кучук Г.А., Давікоза О.П. Синтез стратифікованої інформаційної структури інтеграційної компоненти гетерогенної складової Єдиної АСУ Збройними Силами України. Наука і техніка Повітряних Сил Збройних Сил України: науково-технічний журнал. Х.: ХУ ПС, 2013. № 3(12). С. 154-158. URL: http://nbuv.gov.ua/UJRN/Nitps_2013_3_36

192. Кучук Г.А., Косенко В.В., Давікоза О.П. Метод управління розподілом ресурсів багатосерверного вузла обробки інформації. Збірник наукових праць Харківського університету Повітряних Сил. Х.: ХУ ПС, 2013. Вип. 3(36). С. 111-115. URL: http://nbuv.gov.ua/UJRN/ZKhUPS_2013_3_24

193. Кучук Г.А. Метод синтезу інформаційної структури зв'язного фрагменту корпоративної мультисервісної мережі. Збірник наукових праць Харківського університету Повітряних Сил. Х.: ХУ ПС, 2013. – Вип. 2(35). С. 97-102. URL: http://nbuv.gov.ua/UJRN/ZKhUPS_2013_2_26

194. Кучук Г.А., Косенко В.В., Давікоза О.П., Калкаманов С.А. Методика синтезу інформаційної технології управління мережевим трафіком. Системи управління, навігації та зв'язку: збірник наукових праць. – Полтава. ПНТУ, 2013. Вип. 2(26). С. 105-110. URL: http://nbuv.gov.ua/UJRN/suntz_2013_2_27

195. Кучук Г.А., Рубан І.В., Давікоза О.П. Концептуальний підхід до синтезу структури інформаційно-телекомунікаційної мережі. Системи обробки інформації: збірник наукових праць. Х.: ХУ ПС, 2013. Вип. 7 (114). С. 106 – 112. URL: http://nbuv.gov.ua/UJRN/soi_2013_7_28

196. Кучук Г.А., Косенко В.В., Давікоза О.П. Математична модель технічної структури інформаційно-телекомунікаційної мережі. Системи обробки інформації: збірник наукових праць. Х.: ХУ ПС, 2013. Вип. 6 (113). С. 234 – 237.

URL: http://nbuv.gov.ua/UJRN/soi_2013_6_46

197. Кучук Г.А. Управління трафіком ланки мультисервісної мережі. Авіаційно-космічна техніка и технологія: науковий журнал. 2013. № 10/107. С. 236 – 239. URL: http://nbuv.gov.ua/UJRN/aktit_2013_10_44

198. Кучук Г.А. Синтез топології гібридного хмарного сховища даних у гетерогенному середовищі. Авіаційно-космічна техніка и технологія : науковий журнал. 2013. № 9/106. С. 280 – 284. URL: http://nbuv.gov.ua/UJRN/aktit_2013_9_49

199. Кучук Г.А. Метод оптимального розподілу ресурсів CLOUD-системи. Системи обробки інформації: збірник наукових праць. Х.: ХУ ПС, 2013. Вип. 5 (112). С. 125 – 129. URL: http://nbuv.gov.ua/UJRN/soi_2013_5_30

200. Кучук Г.А. Метод синтезу структури зв'язного фрагменту інформаційно-телекомунікаційної мережі Єдиної автоматизованої системи управління Збройними Силами України. Системи озброєння і військова техніка : науковий журнал. 2013. № 2(34). С. 114-119. URL: http://nbuv.gov.ua/UJRN/soivt_2013_2_29

201. Кучук Г.А., Куфлієвський О.А. Моделювання розподіленого вузла концентратора послуг NGN-мережі. Системи обробки інформації. Х.: ХУ ПС, 2011. Вип. 3 (93). С. 52–55. URL: http://nbuv.gov.ua/UJRN/soi_2011_3_14

202. Кучук Г.А., Моміт Р.В., Дяченко С.А., Животовський Р.М., Шишацький А.В. Пристрій обробки різнотипних даних в системах підтримки прийняття рішень. Патент на корисну модель пат. 148275, Україна. № 202101288 / О.С. Моміт, Г.А. Кучук; заявл. 15.03.2021; опубл. 21.07.2021, бюл. № 29/2021.

203. Кучук Г.А., Яловега В.А., Главчева Д.М., Подорожняє А.О. Комп'ютерна програма для обробки мультиспектральних зображень та навчання загорткових та капсульних нейронних мереж. Свідectvo про реєстрацію авторського права на твір, від 01.04.2019 № 87363

204. Кучук Г.А., Шишацький А.В., Кучук Н.Г., Зубрицький Г.М., Прокопенко Є.М., Животовський Р.М. Спосіб формування топології мережі. Патент на корисну модель UA 125698 (U) МПК від 25.05.2018; № заявки u201711310 від 20.11.2017

205. Кучук Г.А., Шишацький А.В., Кучук Н.Г. Спосіб вибору топології мережі. Патент на корисну модель UA 124344 (U) МПК від 10.04.2018; № заявки u201708810 від 04.09.2017

206. Кучук Г.А., Третьак В.Ф., Карлов Д.В. Спосіб оптимального планування розподілу задач в системі підтримки прийняття рішень. Патент на корисну модель № заявки u201403581 від 7.04.2014; № патенту 92926 (51) МПК від 10.09.2014

207. Кучук Г.А., Третьак В.Ф., Карлов Д.В. Спосіб оптимізації паралельної обробки великих масивів даних в кластерних системах. Патент на корисну модель № заявки u201403986 від 14.04.2014; № патенту 92965 (51) МПК від

10.09.2014

208. Кучук Г.А., Третьак В.Ф., Карлов Д.В. Спосіб рішення задачі планування паралельного розподілу задач в GRID-системах. Патент на корисну модель № заявки и201403988 від 14.04.2014; № патенту 92966 (51) МПК від 10.09.2014

209. Voitko O., Onishchuk V. Концепція реалізації державної інформаційної політики та забезпечення інформаційної безпеки України (в умовах конфлікту з російською федерацією). Theoretical and practical aspects of development of legal knowledge, national security and physical education of citizens (1st ed.). 2021. URL: <https://doi.org/10.36074/tpadlknspec.ed-1.01>

210. Voitko, O., Rakhimov, V. Analysis of the use of social networks in the interests of conducting an information operation while forecasting the spread of the adversary's information influence. Theoretical and Applied Aspects of the Russian-Ukrainian War: Hybrid Aggression and National Resilience : Monograph / ed. by M. Koval. Kharkiv, 2023. P. 232-243. (Monograph Scopus, 372 p.). URL: <https://doi.org/10.15587/978-617-8360-00-9>

211. Special features of the designation of the necessary number of inputs (information channels) in the interests of realizing the strategic narrative of the state on the basis of an analytical model of the development of information / O. Voitko et al. International Scientific And Practical Conference “Information Security And Information Technologies” : Conference Proceedings, Odesa, 13–19 September 2021. Kharkiv, 2021. P. 87–92. URL: https://drforum.science/wp-content/uploads/2021/12/proceedings_ibit-2021.pdf

212. Peculiarities of Implementing the State’s Strategic Narrative based on the Public Opinion / O. Voitko et al. International Journal of Emerging Technology and Advanced Engineering. Volume 11, Issue 7 : Conference Proceedings, Kyiv, July 2021. Bhopal, 2021. P. 48-59. URL: https://doi.org/10.46338/ijetae0721_07

213. Counteraction to information influence in social networking services by means of fuzzy logic system / O. Voitko et al. International Journal of Electrical and Computer Engineering (IJECE). 2021. Vol.11, no. 7. P. 2490–2499. URL: <https://doi.org/10.11591/ijece.v11i3.pp2490-2499>

214. Special Features of the Designation of the Necessary Number of Inputs (Information Channels) in the Interests of Realizing the Strategic Narrative of the State on the Basis of an Analytical Model of the Development of Information / O. Voitko et al. III International Scientific And Practical Conference “Information Security And Information Technologies”: Conference Proceedings, Odesa, 13–19 September 2021. Kharkiv, 2021. Vol. 3200. P. 74-79. URL: <https://ceur-ws.org/Vol-3200/paper11.pdf>

215. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems / O. Voitko et al. Eastern-European Journal of Enterprise Technologies. 2019. Vol. 2, no. 9(98). P. 56–66. URL: <https://doi.org/10.15587/1729-4061.2019.164730>

216. Development of a method for ensuring confidentiality and authenticity in wireless channels / O. Voitko et al. *Eastern-European Journal of Enterprise Technologies*. 2022. Vol. 6, no. 9 (120). P. 15–27. URL: <https://doi.org/10.15587/1729-4061.2022.268368>
217. Equations of periodic modes, which take into account features of the dynamics of their course in nonlinear automatic systems with computers in control system / O. Voitko et al. *Системи обробки інформації*. 2021. № 1(164). P. 12-20. URL: <https://doi.org/10.30748/soi.2021.164.02>
218. Особливості застосування методу фрактального аналізу сталості процесу розвитку громадської думки при реалізації стратегічного наративу держави / О. Войтко та ін. / *Системи обробки інформації*. 2020. Том 38, № 2. С. 145-150. URL: <https://doi.org/10.33099/2311-7249/2020-38-2-145-150>
219. Войтко О. Модель розповсюдження інформації при реалізації стратегічного наративу держави. Сучасні інформаційні технології у сфері безпеки та оборони. 2021. Т. 41, № 2. С. 47–52. URL: <https://doi.org/10.33099/2311-7249/2021-41-2-47-52>
220. Войтко О. Особливості проведення аналізу відкритих джерел при розробленні паспорту цільових аудиторій в інтересах реалізації стратегічного наративу держави. Сучасні інформаційні технології у сфері безпеки та оборони. 2021. Т. 40, № 1. С. 169-174. URL: <https://doi.org/10.33099/2311-7249/2021-40-1-169-174>
221. Войтко О. та інш. SIR-модель розповсюдження та врахування результатів негативного впливу інформаційних каналів на громадську думку населення / О. Войтко та ін. / *Системи обробки інформації*. 2022. Том 43, № 1. С. 115-120. URL: <https://doi.org/10.33099/2311-7249/2022-43-1-115-120>
222. Koval M., Ivashchenko A., Telelym V. Hybrid Warfare: Strategies and Countermeasures. Theoretical and Applied Aspects of the Russian-Ukrainian War: Hybrid Aggression and National Resilience Monograph / ed. by M. Koval. Kharkiv, 2023. P. 232–243. (Monograph Scopus, 372 p.). URL: <https://doi.org/10.15587/978-617-8360-00-9>
223. М. Коваль та ін. Основи інженерного захисту об'єктів критичної інфраструктури енергетичної галузі України від засобів повітряного нападу противника: монографія / М. Коваль та ін. Київ: НУОУ, 2023. 182 с.
224. Теоретико-прикладні аспекти російсько-української війни: гібридна агресія та національна стійкість: монографія / М. В. Коваль та ін. Київ: НУОУ, 2023. 316 с.
225. “Wagner” Private Military Company: from its formation to the present day : Monograph / M. Koval et al. Kyiv : National Defence University of Ukraine, 2023. 128 p.
226. Збройний конфлікт на Сході України: воєнно-історичний аспект. Частина V. 2018 рік : монографія / М. В. Коваль та ін. Київ : НУОУ, 2023. 240 с.
227. Методика комплексного управління ресурсами систем зв'язку спеціального призначення / М. Коваль et al. *Moderní aspekty vědy: XXV. Díl*

mezinárodní kolektivní monografie : Monograph. 25th ed. Prague, 2022. P. 404–425. URL: <http://perspectives.pp.ua/public/site/mono/mono-25.pdf>

228. Improvement of complex resource management of special-purpose communication systems / M. Koval et al. Eastern-European Journal of Enterprise Technologies. 2022. Vol. 5, no. 9(119). P. 34–44. URL: <https://doi.org/10.15587/1729-4061.2022.266009>

229. Improving the method for increasing the efficiency of decision-making based on bio-inspired algorithms / M. Koval et al. Eastern-European Journal of Enterprise Technologies. 2022. Vol. 6, no. 4 (120). P. 6–13. URL: <https://doi.org/10.15587/1729-4061.2022.268621>

230. Determining the deterrence forces composition to prevent the unleashing of enemy aggression based on the principles of system analysis / M. Koval et al. Eastern-European Journal of Enterprise Technologies. 2023. Vol. 1, no. 3 (121). P. 15–24. URL: <https://doi.org/10.15587/1729-4061.2023.274472>

231. Розвиток концептуальних засад забезпечення оборони України: від воєнної організації держави до всеохоплюючої оборони / М. Коваль та ін. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2024. № 3 (79). С. 8–14. URL: <https://doi.org/10.33099/2304-2745/2023-3-79/8-14>

232. Передбачення можливостей держави щодо відбиття збройної агресії / М. Коваль та ін. Наука і оборона. 2023. № 3. С. 25 – 32. URL: <https://doi.org/10.33099/2618-1614-2023-22-3-25-32>

233. Ідентифіковані уроки з розроблення доктрин планування: кількісний підхід до вимірювання повноти інформації / М. Коваль та ін. Наука і оборона. 2023. № 2. С. 28 – 37. URL: <https://doi.org/10.33099/2618-1614-2023-22-2-28-37>

234. Коваль М., Наливайко А. Обґрунтування підходу до вдосконалення стратегічного планування в силах оборони. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ. 2022. С. 61–66. URL: <https://doi.org/10.33099/2304-2745/2022-2-75/61-66>

235. Організаційно-технічні засади побудови системи інженерного захисту об'єктів критичної інфраструктури енергетичної галузі України / М. Коваль та ін. Наука і оборона. 2022. № 3-4. С. 11 – 16. URL: <https://doi.org/10.33099/2618-1614-2022-20-3-4-11-16>

236. Методичний підхід до визначення критичних об'єктів ураження противника непрямыми діями / М. Коваль та ін. Наука і оборона. 2022. № 2. С. 32 – 36. URL: <https://doi.org/10.33099/2618-1614-2022-19-2-32-36>

237. Стратегічний характер Київської оборонної операції (24 лютого – 2 квітня 2022 р.) / М. Коваль та ін. Український історичний журнал. 2023. № 3 (570). С. 5 – 29. URL: <https://doi.org/10.33099/2618-1614-2022-19-2-32-36>

238. Гришук Р. В. Постановка наукового завдання з розроблення шаблонів потенційно небезпечних кібератак / Р. В. Гришук, В. В. Охрімчук // Безпека інформації – 2015. – Том 21. – № 3. – С. 276–282.

239. Грищук Р. В. Джерела первинних даних для розроблення шаблонів потенційно небезпечних кібератак / Р. В. Грищук, В. В. Охрімчук, В. С. Ахтирцева // Захист інформації. – 2016. – Том 18. – № 1 – С. 21–29.
240. Грищук Р. В. Диференціально-ігрова модель шаблону нормальної поведінки Web-сервера [Електронний ресурс] / Р. В. Грищук // Проблеми телекомунікацій. – 2010. – № 2 (2). – С. 96 – 106. – Режим доступу до журн. : http://pt.journal.kh.ua/2010/2/2/102_gryschuk_web.pdf.
241. Грищук Р. В. Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень : монографія / Р. В. Грищук. – Житомир : РУТА, 2010. – 280 с.
242. Грищук Р. В. Диференціально-ігрова модель шаблону атаки на Web-сервер / Р. В. Грищук // Збірник наукових праць ВІКНУ ім. Т. Шевченка. – К. : ВІКНУ ім. Т. Шевченка, 2010. – № 21. – С. 104–112.
243. Грищук О. М. Верифікація узагальненої диференційно-ігрової моделі шаблону потенційно небезпечної кібератаки / О. М. Грищук, Р. В. Грищук, В. В. Охрімчук // Телекомунікаційні та інформаційні технології. – 2020. – №1 (66). – С. 53–67.
244. Грищук Р. В. Основи кібернетичної безпеки : Монографія / Р. В. Грищук, Ю. Г. Даник ; за заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.
245. Hryshchuk R. Construction methodology of information security system of banking information in automated banking systems / Hryshchuk R., Yevseiev, S. Shmatko A. – Vienna.: Premier Publishing s. r. o., 2018. – 284 p.
246. Грабар І. Г. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир : ЖНАЕУ, 2019. – 280 с.
247. Грищук Р. В. Верифікація методу скорочення розмірності потоків вхідних даних систем інформаційної безпеки / Р. В. Грищук, В. О. Хорошко, В. М. Мамарев // Защита информации. – К. : НАУ, 2015. – № 22. – С. 99–109.
248. Грищук Р. В. Верифікація і дослідження спектральних Р- та гібридних Р-L-моделей процесу нападу на інформацію / Р. В. Грищук // Вісник ЖДТУ. – Житомир : ЖДТУ, 2009. – № 49 (II). – С. 77–85.
249. Hryshchuk R. The Synergetic Approach for Providing Bank Information Security: The Problem Formulation / Ruslan Hryshchuk, Sergii Yevseiev // Безпека інформації. – 2016. – Том 22. – № 1 – С. 64–74. (Index Copernicus).
250. Гешування даних в інформаційних системах. Харків: Вид. ХНЕУ/Євсєєв С.П., Йохов О.Ю., Король О.Г., 2013. – 312 с.
251. Євсєєв С. П., Погасій С. С., Хвостенко В. С. Development of a protocol for a closed mobile internet channel based on post-quantum algorithms // Системи обробки інформації. – 2021. – №. 3 (166). – С. 35-40.
252. Yevseiev S. et al. Research of collision properties of the modified UMAC algorithm on crypto-code constructions // EUREKA: Physics and Engineering, (1). –

2022. – C. 34-43.