УДК 681.32:007.5
DOI: 10.15587/1729-4061.2020.218660

Розробка просторово-часової структури методології моделювання поведінки антагоністичних агентів системи безпеки

О. В. Мілов, А. М. Гребенюк, А. Д. Наливайко, О. А. Нємкова, І. Р. Опірський, І. В. Пасько, Х. Н. Рзаєв, А. Г. Салий, Ю. П. Синиціна, О. И. Соловьева

Стрімкий розвиток обчислювальних технологій, поява сучасних кіберзагроз з ознаками гібридності та синергізму висуває жорсткі вимоги до економічної складової національної безпеки держави та особливо процесам забезпечення кібербезпеки функціонування економіки. Індустрія кібербезпеки намагається відповідати вимогам сьогодення, впроваджуючи нові і більш досконалі технології і методи гарантування безпеки, однак вважається, що такий універсальний підхід недостатній. Дослідження присвячено вирішенню об'єктивного протиріччя між зростаючими на практиці вимогами до забезпечення відповідного рівня кібербезпеки контурів бізнес-процесів при одночасному збільшені кількості та технологічній складності загроз кібербезпеці. При цьому слід враховувати набуття загрозами ознак гібридності з одного боку, та недосконалістю, а подекуди й відсутністю методології моделювання поведінки взаємодіючих агентів систем безпеки. Однак це не дозволяє своєчасно прогнозувати майбутні дії зловмисників, а як результат – визначати необхідний рівень інвестицій в систему безпеки, що забезпечить необхідний рівень кібербезпеки.

В роботі запропонована Концепція моделювання поведінки взаємодіючих агентів, базис якої становить трирівнева структура моделювання суб'єктів та бізнес-процесів контурів функціонування організації та системи безпеки, що базується на моделюванні поведінки антагоністичних агентів. Запропонована методологія моделювання поведінки взаємодіючих агентів, яка заснована на Концепції поведінки антагоністичних агентів, дозволяє оцінити та підвищити поточний рівень безпеки за рахунок зменшення у 1,76 разів кількості реалізації гібридних загроз, що забезпечує зменшення збитків у 1,65 рази та збільшення часу вибору засобів протистояння за рахунок скорочення на 38 % часу для ідентифікації загрози в онлайн режимі.

Ключові слова: кібербезпека, антагоністичні агенти, методологія моделювання, рефлексивний агент, мультиагентні системи, контур бізнес-процесів.

1. Вступ

Оскільки світ стає все більш технологічним і залежним від комп'ютерів для моніторингу життєвих функцій або ведення бізнесу, важливість забезпечення безпеки цих систем стає критично важливою в повсякденному житті.

Найбільш мінливий аспект кібератаки – це самі зловмисники. Моделювання тільки мережі може показати її слабки місця та потенційні атаки, які можуть бути реалізовани взагалі. Але це не дає ніякої інформації про те, які саме атаки можуть бути реалізовані зловмисниками, виходячи з їхньої точки зору. Оскільки кожна людина індивідуальна, процес, при якому зловмисник буде атакувати мережу, буде відрізнятися для кожного зловмисника. Розуміння відмінностей між зловмисниками і їх поведінкою можна використовувати для аналізу наслідків атак, а потім для раннього виявлення і прогнозування.

Моделюючи кібератаки, орієнтуючись на те, як реальний кібер-атакуючий буде приймати рішення, ґрунтуючись на навичках, правилах і знаннях, можна синтезувати дані про поведінку зловмисника, які інакше було б важко досягти. Поєднання генерації атак, заснованої на правилах і знаннях, забезпечує надійні і різноманітні покоління траєкторій атак, в той же час забезпечуючи реалістичні результати, оскільки правила і знання постійно координуються між собою. Це означає, що правила не можуть застосовуватися, якщо знання недостатньо розвинені, а гнучкість знань не може бути використана, якщо правила занадто обмежені. Застосування цієї схеми до імітаційного моделювання дозволяє глибше зрозуміти, як впливають багато різних типів зловмисників, аналізуючи типи виконуваних атак і маючи можливість дізнатися, що зловмисникові необхідно було знати для виконання атак. Потім, нарешті, слід звернутися до можливого кінцевого користувача, який намагається захистити свої мережі від атак, про які не думали тестери проникнення, або інших інструментів, які не мають інструментів для захисту. Це дає більш глибоке розуміння того, як використовуються вразливості і як вони можуть вплинути на мережу до того, як атака може статися, і тоді з цим можна щось зробити. Індустрія кібербезпеки намагається відповідати вимогам сьогодення, впроваджуючи нові і більш досконалі технології і методи забезпечення безпеки. Сучасні методи дослідження кіберзагроз зазвичай виконуються за допомогою статичного аналізу вразливостей мережі і системи. Але лише деякі звертаються до найбільш мінливої і найбільш важливої частини проблеми – самих зловмисників. Людський фактор, що лежить в основі кібербезпеки, дозволяє краще зрозуміти цю проблему і висуває на перший план поведінку осіб, як ключовий фактор, що викликає найбільшу стурбованість. Людський елемент в основі кібербезпеки – це те, що робить кіберпростір складною, адаптивною системою. Для підвищення кібербезпеки необхідний всеосяжний, міждисциплінарний, комплексний підхід, що поєднує технічний і поведінковий елементи. Тому створення науково-обґрунтованої методології моделювання процесів поведінки агентів у системах безпеки є актуальною науково-прикладною проблемою, що має теоретичне і практичне значення.

2. Аналіз літературних даних і формулювання проблеми

За останні роки були проведені дослідження, присвячені динаміці кібератак та проведення кібератак, щоб краще проаналізувати вплив цих зловмисників. Були

проведені дослідження з використання вразливостей в мережі для виявлення можливих і реалістичних шляхів атаки [1–6]. Так, у [1] наведені конкретні приклади проведення масштабних кібератак. У роботі [2] аналізується тенденція використання сторонніх постачальників послуг для отримання доступу до організацій-жертв. Нова парадигма аналізу графа атак, яка доповнює традиційне графоцентрическое уявлення, засноване на матрицях суміжності графів, представлена у [3]. Питанням прогнозування потенційних атак на основі атак, що спостерігаються, присвячена робота [4]. У [5] наведено приклад байєсовської мережі на основі поточної моделі графа безпеки. Марковська модель змінної довжини, яка фіксує особливості треків атак, що дозволяє прогнозувати ймовірні наступні дії при поточних атаках, аналізується у [6]. Слід зазначити, що недоліком наведених робіт є те, що ці методи враховують тільки вразливості в мережі, але не виявляють реальних відмінностей між типами зловмисників. В інших роботах це питання розглядалося шляхом моделювання можливостей противників [7] або застосування методології теорії ігор [8] для моделювання атакуючого і захисника. Жоден з цих методів не моделює зловмисника на основі інформації, яку зловмисник отримує в ході атаки, хоча вона грає важливу роль в прийнятті рішень щодо реалізації атаки. Ця концепцію добре реалізується в методах агентного моделювання в інструменті імітаційного моделювання поведінки зловмисника NeSSi2 (NeSSi – Network Security Simulator) [9] і в моделі поведінки атакуючого в моделюванні сценарію багатоступінчастої атаки (MASS – multistage attack scenario simulation) [10]. Однак методи агентного моделювання не забезпечують структуру, в якій зловмисник отримує конкретні деталі про цілі і зможе динамічно змінювати цілі та стратегії під час атаки. Цей вид заснованого на знаннях проектування для моделювання зловмисника дозволяє гнучко описувати кібератаки, що дає можливість моделювати проактивну і реактивну поведінка учасників кіберконфлікту.

В роботах [10, 11] моделювання виконувалось для аналізу можливих кібератак, які можуть статися в мережі. Основна увага в роботі приділяється моделюванню поведінки кібер-зловмисника таким чином, щоб можна було гнучко описати множину різних типів зловмисників, зберігаючи при цьому розумний реалізм в типах атак, які можуть бути виконані. Моделювання процесів прийняття рішень зловмисником з точки зору рефлексивного управління, більш схоже на те, як насправді думає зловмисник. Це дозволяє зрозуміти відмінності, які мають різні зловмисники в одній мережі, або те, як один зловмисник може вплинути на різні типи мереж. Така гнучкість може допомогти полегшити навички і час, необхідний для виконання такого типу аналізу. Основна мета полягає в розробці структури для моделювання процесу прийняття рішення зловмисником, заснованого як на детермінованих факторах, таких як мережа і знання, так і на імовірнісних факторах. Такая структура дозволяють враховувати випадковість при моделюванні. Хоча мета полягає не в тому, щоб мати можливість всебічно змоделювати кожен тип поведінки зловмисника, а в тому, щоб визначити, що саме необхідно моделювати для опису зловмисника.

Аналітика кіберзагроз є відносно молодою галуззю і різноманітна за типами підходів, що застосовуються для виконання прогнозованого аналізу кібератак. Ці підходи складаються з оцінки та пом'якшення вразливостей, аналітичних підходів, таких як використання графів атак і теорії ігор, а також математичного та імітаційного моделювання кібератак. Кожен з підходів має свої переваги і недоліки, і один підхід не обов'язково кращий за інший через складність прогнозування, в першу чергу, людської поведінки. В даний час для аналізу супротивника використовують математичні моделі, такі як графи атак, онтології атак або симуляції, моделі теорії ігор або мультиагентні моделі.

Метою тесту на проникнення в мережу є виявлення потенційних слабких місць в мережі, доступної для потенційного зловмисника. Знаючи уразливості мережі, тестувальник/зловмисник може використовувати їх для подальшого проникнення в мережу для отримання додаткової інформації. Тестер проникнення буде використовувати цю інформацію, щоб виявити більше вразливостей, поки зловмисники не вичерпали всі свої можливі варіанти. Для цього розробляється так званий граф атак, який являє собою сукупність всіх можливих шляхів, за якими зловмисник може слідувати в мережі. Цей процес традиційно виконувався вручну зловмисником або групою аналітиків і може виявитися процесом виснажливим. У [12] процес формалізовано, щоб автоматично генерувати вичерпний набір можливих графів атак для даної мережі. Графи атак генеруються з використанням опису мережі і знань зловмисника про цю мережі, а потім опису набору станів, які описують реальні атаки, які можуть статися. У [12] була змодельована мережа з двох хостів з IDS (IDS – Intrusion detecytion system) і фаєрволом. В результаті було отримано графік атаки з 5948 вузлів з 68364 ребрами, який надзвичайно великий для дуже небагатьох типів атак і нереально малої мережі. Цей метод аналізу не є гнучким, масштабованим або простим для використання, що необхідно для успішної оцінки слабких сторін мережі.

З огляду на розмір мережі, слід зазначити, що число можливих шляхів атаки може бути надзвичайно великою. В роботі [13] запропоновано два методи, щоб визначити, які графи атак найбільш критичні, а які найбільш ефективні. Автоматична генерація графа атак вимагає моделювання всіх можливих типів атак. У статті [13] розглянув всього 4 можливих типи атак.

В [14] описане використання графів атак для генерації шаблонів попереджень IDS, щоб допомогти в прогнозуванні майбутніх і триваючих атак. Використовуючи ці графи атак і знання області кібератак, можна оцінити ймовірність досягнення цілей атаки для прогнозування майбутніх атак. Цей метод вимагає, щоб кожен граф атак був перетворений в мережу, і експерт з кібербезпеки проаналізував її для визначення ймовірності успішного завершення кібератаки. У цього підходу є дві проблеми: перші атаки, які не строго слідують плану атаки, не можуть бути змодельовані, і ймовірність заснована виключно на досвіді експерта. У [13, 14] визначаються тільки різні шляхи, за якими може піти зловмисник, а не те, чи буде зловмисник реально реалізовувати цю атаку чи ні.

У [15] автори усунули невизначеність варіації атак, успішність і точність даних сенсорних попереджень шляхом об'єднання графів атак з байесовськими мережами. Це призвело до створення реальних баз даних про уразливість, таких як Національна База Даних Вразливостей (NVD – National Vulnerability Database) і Загальна Система Оцінки Вразливостей (CVSS – Common Vulnerability Scoring System). Використаннея реальних даних з цих баз дає основу для розрахунку ймовірності без необхідності експертних знань для кожної функції.

У [16, 17] оцінюється генерація графа атак в реальному часі для прогнозування ймовірності наступних кроків зловмисника на основі різних порушень безпеки. Виходячи з порушень безпеки, можна визначити базовий рівень навичок зловмисника, який потім можна використовувати з CVSS для визначення можливості наступних кроків на основі положення зловмисника в мережі. Загальною проблемою між вищезгаданими роботами є розробка графа базової атаки, який описує сценарій і цілі зловмисника. З використанням перерахування і класифікації шаблонів загальних атак (CAPEC – Common Attack Pattern Enumeration and Classification) від MITRE, в [18, 19] згенеровані графи атак на основі реальних сценаріїв. Ці сценарії використовуються для отримання більш реалістичних прогнозів і інших графів атак.

У роботах [12–19] аналізується безпека мережі на основі можливих атак, які можуть бути реалізовані в мережі при одному або декількох сценаріях. У цих випадках сценарії чітко визначено, і різні зловмисники можуть переслідувати одну і ту ж мету, і неважливо, успішні вони чи ні. Розуміння впливу зловмисника на мережу дуже важливе, тому що насправді не всі вразливості можуть бути закриті, а деякі можуть розставити пріоритети, які вразливості необхідно усунути з плином часу. Припустимо, що існує експлойт, який може бути виконаний будь-якою людиною і який може здійснити шкідливий вплив на мережу. У цьому випадку він повинен мати більш високий пріоритет, ніж експлойт, який тільки 1 % атакуючих може виконати на некритичній машині. У публікаціях [15, 17–19] показане використання загальнодоступних даних сценаріїв кібератак для створення шляхів атаки, які були визначені як реалістичні, але не враховували навички або поведінку зловмисника. Сучасні методи прогнозування кібератак стали більше уваги приділяти питанням поведінки зловмисників і процесам прийняття рішень, які зловмисник приймає під час здійснення атаки. Публікації в науковій періодиці можна умовно розділити на дві категорії. До першої катеогрії належать публікації, орієнтовані на методи моделювання поведінки взаємодіючих агентів. До другої – публікації, орієнтовані на поведінкові аспекти функціонування агентів систем безпеки, і більш точно – на процеси прийняття рішень. Увага до використання теорії ігор пояснюється тим фактом, що саме ця теорія є основою для агентного моделювання в умовах конфлікту [20, 21]. Рис. 1 демонструє результати аналізу сучасних підходів до моделювання поведінки агентів, до основних переваг яких відносяться наступні:

– відображення в моделі цілеспрямованості поведінки агентів, а також спроможності агентів формулювати свої цілі;

– можливість моделювати як поведінку окремого агенту, так і взаємодію між різними агентами, які становлять модель;

– здатність агентів до навчання.

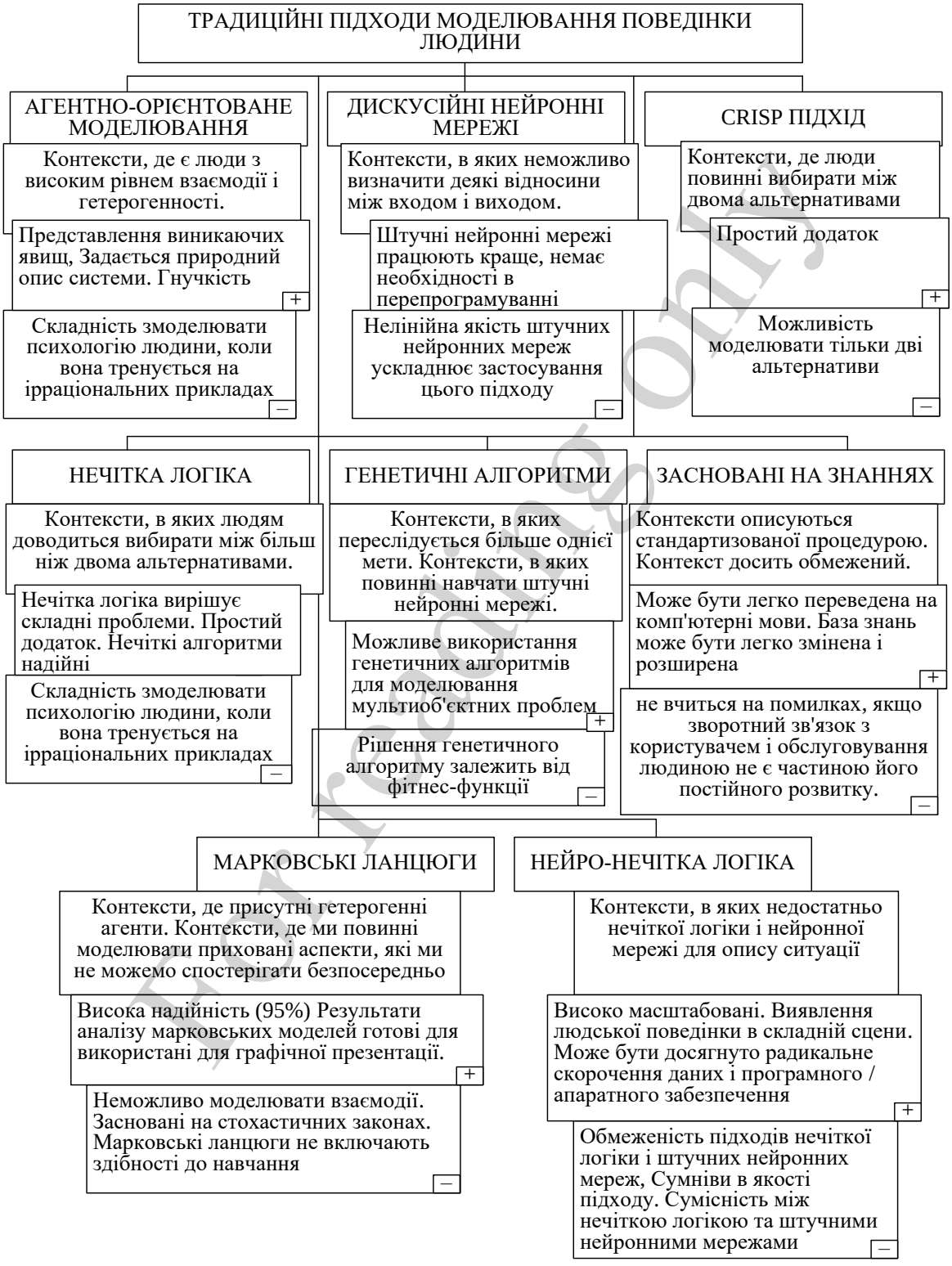

Рис. 1. Традиційні підходи моделювання поведінки людини

В роботах [22–24] авторами пропонуються підходи щодо оцінки якості обслуговування на основі багатофакторного аналізу та поточного стану інформаційної безпеки організації. Але при цьому не враховуються можливі превентивні дії на основі моделювання та оцінки можливостей як нападника, так и сторони захисту.

Таким чином, аналіз можливостей забезпечення як безпеки контуру бізнес-процесів, так і задач моделювання поведінки антагоністичних агентів, показав наступне – одночасно з великою кількістю робіт, присвячених питанням безпеки бізнес-процесів організації, залишається невирішеною проблема створення цілісної методології моделювання. Впровадження такої методології на практиці сприятиме стійкому та стабільному розвитку систем безпеки будь-якого рівня, на основі моделювання поведінкових характеристик функціонування агентів системи безпеки.

Відсутність на сьогодні відповідної методології обумовлено наявністю протиріччя, яке визначається наступним чином. Практика вимагає від теорії пошуку нових підходів до забезпечення кібернетичної та інформаційної безпеки контуру бізнес-процесів в умовах зростання кількості загроз при одночасному зростанні їх технологічної складності.

3. Мета і задачі дослідження

Метою роботи є розробка просторово-часової структури методології моделювання поведінки антагоністичних агентів системи безпеки на основі запропонованих моделей, методів та алгоритмів, які дозволяють 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.

Для досягнення мети роботи необхідно вирішити наступні завдання:

– виявити особливості моделювання поведінки взаємодіючих агентів систем безпеки в умовах кіберконфлікту;

– розробити концепцію моделювання поведінки взаємодіючих агентів;

– розробити просторово-часову структуру методології моделювання поведінки взаємодіючих агентів;

– провести верифікацію запропонованої методології на основі імітаційного моделювання.

4. Виявлення особливостей моделювання поведінки взаємодіючих агентів систем безпеки в умовах кіберконфлікту

При розробці програм імітації поведінки агентів необхідно відповісти на питання, як моделювати процеси прийняття рішень агентами в системі безпеки.

У обчислювальній соціальній науці в цілому і в області Агентного Соціального Моделювання (ABSM – agent-based social modeling), зокрема, ведеться постійна дискусія про те, як найкраще моделювати прийняття рішень людиною. Причина цього полягає в тому, що, більшість обчислювальних моделей процесу прийняття рішення

є досить простими [25]. Як і в будь-якій хорошій науковій моделі, при моделюванні поведінки людей об'єкти, що моделюються, повинні аналізуватися з точки зору тільки тих властивостей, які мають відношення до даного сценарію поведінки.

Тому виникає питання: "Що таке хороша (обчислювальна) модель людини (і прийняття рішень їм) для конкретного дослідницького питання?" Для ABSM було розроблено велику кількість архітектур і моделей, які намагаються представити процес прийняття рішень людиною. Незважаючи на спільну мету, кожна архітектура має дещо різні цілі і, як наслідок, включає різні припущення і спрощення. Тому знання цих відмінностей важливо при виборі моделі прийняття рішень агентом в ABSM.

Щоб мати можливість обговорити придатність різних архітектур агентів для різних типів ABSM, необхідно відповісти на питання, які типи ABSM існують і які з них представляють інтерес для спільноти ABSM.

Одна з попередніх спроб класифікації ABSM була зроблена у [26]. У роботі виділяються п'ять аспектів високого рівня, за якими можна класифікувати ABSM в цілому, в тому числі, наприклад, ступінь, в якій ABSM намагається включити деталізацію конкретних цілей. Останній з цих вимірів стосується агентів (і прийняття рішень), порівнюючи ABSM за складністю агентів, яких вони моделюють. Згідно Гілберту, ця складність агентів може варіюватися від «архітектур системи продукцій» (тобто агентів, які слідують простим правилам IF-THEN) до агентів зі складною когнітивною архітектурою, такими як SOAR (Security Orchestration, Automation and Response) символічна когнітивна архітектура) або ACT-R (Adaptive Control of Thought – Rational). Розглядаючи придатність різних архітектур для різних питань дослідження, у [27] робиться висновок, що більш прості моделі агентів стають в нагоді, коли метою є прогнозування поведінки організації в цілому. Тоді як для точного уявлення необхідні складні і більш когнітивні точні архітектури для прогнозування поведінкі на рівні окремих осіб або невеликих груп.

В роботі [28] пропонується три категорії моделей:

– фізичні моделі, які передбачають, що люди взаємно реагують на поточні (і/або минулі) взаємодії;

– економічні моделі, які передбачають, що люди реагують на свої майбутні очікування і приймають рішення егоїстичним чином;

– соціологічні моделі, які передбачають, що люди реагують на власні і чужі очікування (а також на свій минулий досвід).

У класифікації [28] прості архітектури агентів, такі як продукційні системи, засновані на правилах, найкраще підходять для фізичних моделей, а складність і можливості агентів повинні будуть зрости при переході до соціологічних моделей. У цих соціологічних моделях акцент на моделюванні соціальної (людської) взаємодії може зажадати, щоб агент міг сприймати соціальну мережу, в яку він вбудований, або навіть вимоги для більш складних соціальних концепцій.

Підводячи підсумок, слід виділити два основних виміри, які є корисними для розрізнення агентських архітектур:

– когнітивний рівень агентів, тобто вони є суто реактивними або натхненними психологічно або неврологічно (щоб моделювати прийняття рішеня людиною якомога точніше);

– соціальний рівень агентів, тобто ступінь, в якій вони здатні розрізняти відносини в соціальних мережах (і статус), на які рівні спілкування вони здатні, чи мають вони теорію мислення або в якій мірі вони здатні сприймати складні соціальні поняття.

Ще один спосіб класифікації ABSM з точки зору областей застосування наведено в [29]. У якості прикладів областей застосування наведені наступні: поява і колективна поведінка, розвиток, навчання, норми, ринки, інституційний дизайн і (соціальні) мережі.

Іншими кандидатами на розміри для розрізнення агентських архітектур є:

– здібність агентів міркувати про (соціальні) норми, інститути і організаційні структури; який вплив чинять норми, політика, інститути та організаційні структури на продуктивність системи на макрорівні; і як проектувати нормативні структури, які підтримують цілі розробника систем (або інших зацікавлених сторін);

– здатність агентів вчитися і, якщо так, на якому рівні вони можуть вчитися; наприклад, чи здатні агенти дізнаватися тільки про кращі значення своїх функцій прийняття рішень і чи можуть вони вивчати нові правила прийняття рішень.

Отже, слід додати ще два виміри: вимір норми і вимір навчання.

Останній вимір, який пропонується дослідниками для використання, це афективний рівень, який здатний висловити агент. Більшість знайдених категорій аналогічні [29]. Вони також включають емоції в якості області дослідження.

Підводячи підсумок, можна виділити п’ять основних вимірів, які наведені у рис. 2, для класифікації роботи ABSM в цілому і, отже, для визначення архітектури агентів.

На рис. 3 наведені основі архітектури ABSM, відповідні моделі та рівні їх застосування.

Системи продукційних правил є символьними системами [31], які складаються з набору поведінкових “IF-THEN-правил” [30], і являють собою архітектуру обробки інформації на основі зіставлення шаблонів.

Основні компоненти, з яких складаються системи продукційних правил та визначають, які дії вибираються агентом на основі вхідних даних (так званий цикл прямого розпізнавання [32]), наведено на рис. 3.

Переваги:

– простота з точки зору розуміння зв’язку між правилами і їх результатами;

– наявність зручних графічних засобів для представлення процесів прийняття рішень (наприклад, дерев рішень).

Недоліки:

– неповна адекватність для моделювання людської поведінки;

– агенти систем продукційних правил, як правило, не здатні до афективної поведінки, розуміння норм і реакції на них, розгляду соціальних структур (включаючи спілкування) або вивчення нових правил або оновлення існуючих;

– можливість моделювати поведінку агенту тільки за рахунок великої складності і використання багатьох правил;

– збільшення ймовірність виникнення конфліктів між правилами при зростання їх кількості;

– тривалий час обчислень в умовах великої кількості правил прийняття рішень.

Рис. 2. Основні виміри класифікації роботи ABSM

Модель “Віра-Бажання-Намір” (BDI) та емоційний BDI (eBDI) є однією з найпопулярніших моделей прийняття рішень агентами в агентському оточенні [33]. Модель особливо популярна для побудови систем міркувань для складних завдань в динамічних середовищах [34].

На відміну від системи продукційних правил, основна ідея BDI (Belief-Desire-Intention) полягає в тому, що у агентів “психічний стан” є основою для їх

міркувань. Як випливає з назви, модель BDI зосереджена навколо трьох психічних установок, а саме переконань, бажань і, особливо, намірів [35, 36].

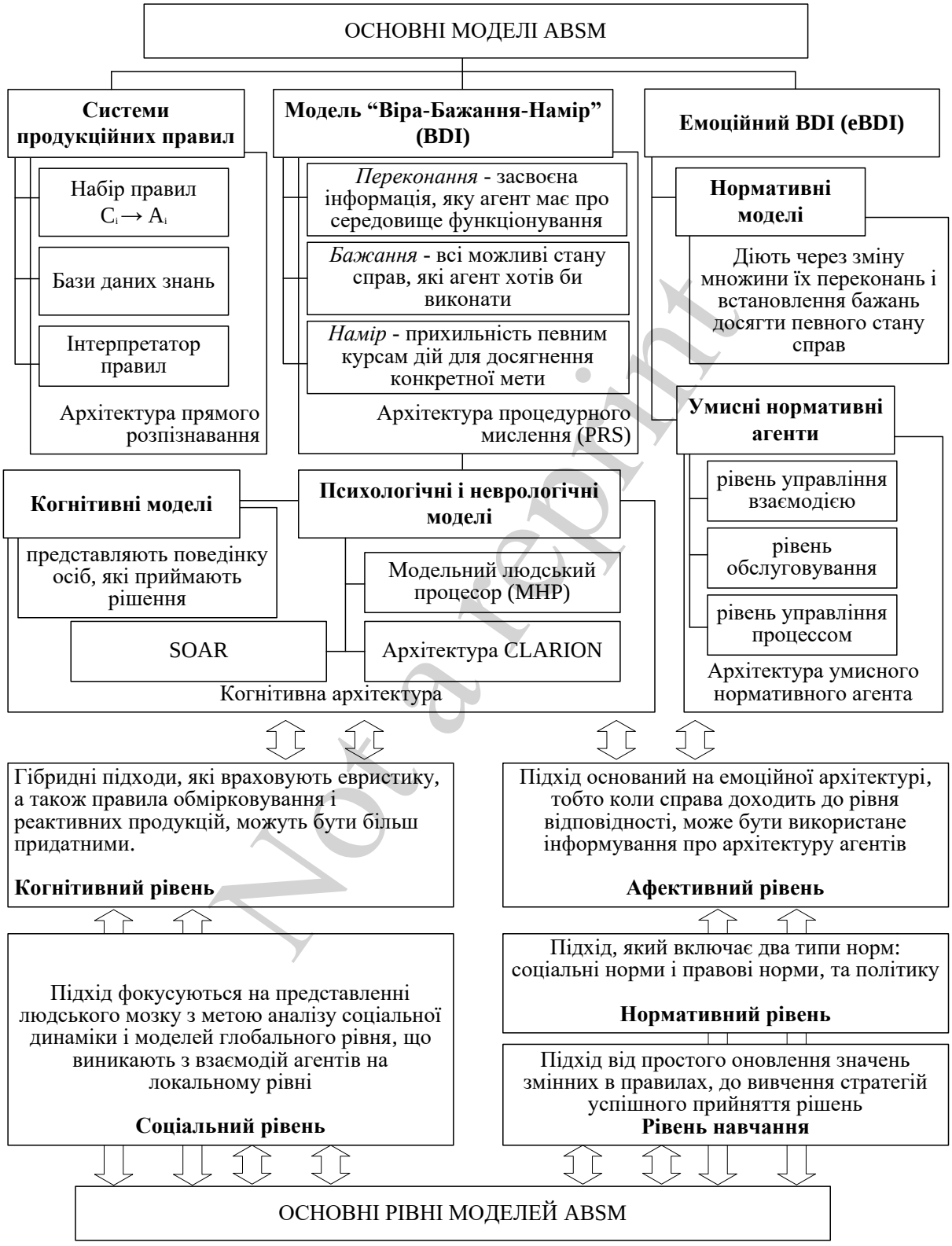

Рис. 3. Основі архітектури ABSM, відповідні моделі та рівні їх застосування

У табл. 1 наведені переваги та недоліки BDI-моделі в залежності від цілей використання (моделювання) [37-40].

Таблиця 1
Переваги та недоліки BDI-моделі в залежності від цілей використання

Ціль моделювання	Важливість BDI	Переваги	Недодіки
Прогнозування	Середня	Реалістичність, адаптується до поведінки на мікрорівні, можливо, ірраціональне індивідуальне пізнання	Складність, масштабованість Потрібні докладні дані
Виконання задачі	Висока	Правильний рівень абстракції людської поведінки Поінформованість, співробітництво в змішаних командах людина-агент Модульний, масштабований, гнучкий дизайн	Більш складний дизайн, незвичайна парадигма
Навчання	Висока	Точна реалістична поведінка для кращого занурення в гру Адаптивність до динамічного середовища Описовість	Більш складний дизайн, незвичайна парадигма
Використання теорії ігор	Середня	Правдоподібна людська поведінка: занурення, виклик Швидке рішення при невизначенності і неповної інформації Правильний рівень абстракції для відображення реальних стратегій гравців	Масштабованість, продуктивність Складніший дизайн в порівнянні зі сценаріями
Освіта	Середня	Інтуїтивне пояснення поведінки за допомогою вбудованих концепцій психології (B, D, I)	Непотрібний реалізм і складність для несуттєвих агентів
Докази	Низька	Реалістичне пізнання, необхідне для доказу мікро-, макро- зв'язків і складних соціально-когнітивних явищ	Не потрібен реалізм і складність для доказу більш простої гіпотези
Відкриття	Низька	Реалістична детальна модель поведінки для виявлення неінтуітивних ефектів і мікро-, макро- зв'язків в адаптивних динамічних складних системах	Більш складне розуміння і дедукція Складніша специфікація вирішальних правил

Нормативні моделі [41]. У BDI агенти діють через зміну множини переконань і встановлення бажань досягти певного стану справ (для якого агенти потім вибирають конкретні наміри у формі планів, які вони хочуть виконати). Поведінка агентів зумовлена виключно їхніми внутрішніми мотиваторами, такими як переконання і бажання. Перевагою нормативних моделей було використання додаткового елемента, що впливав на міркування агента. На відміну від переконань і бажань, цей елемент був зовнішніми по відношенню до агента, і він враховував норми поведінки, що були встановлені в середовищі, в якому знаходився агент. Тому такі елементи розглядалися як зовнішні мотиватори, а агентів в системі називали агентами, що регулювалися відповідними нормами.

Умисні нормативні агенти зосереджені на ідеї, що соціальні норми повинні бути залучені в процес прийняття рішень агентом [42]. Тобто автономні агенти повинні мати можливість міркувати, спілкуватися і вести переговори про норми, в тому числі вирішувати, чи порушувати соціальні норми, якщо вони несприятливі для комерційних агентів.

Перевагами цієї моделі є:

– можливість представлення соціальних норм не просто як обмеження та зовнішні фіксовані правила в архітектурі агента [43], а й як ментальних об’єктів. Ці об’єкти мають своє власне ментальне уявлення і взаємодіють з іншими ментальними об’єктами (наприклад, переконаннями і бажаннями) і планами агента [44];

– виділення окремих рівнів архитектури агента. Перший рівень становить рівень управління взаємодією, який управляє взаємодією агента з іншими агентами (за допомогою зв'язку), а також загальним середовищем. Другий рівень – рівень інформаційного обслуговування, в якому зберігається інформація агента про навколишнє середовище (інформація про світ), про інших агентів і про агентське суспільство в цілому. До третього рівня належить рівень управління процесом, на якому відбувається обробка інформації і обґрунтування рішень.

Це дозволяє з одного боку розглядати відповідні процеси як відносно незалежні, а з другого – як різні прояви одного загального процесу поведінки агенту;

– можливість відображати семантичні відмінності між різними видами інформації (три рівня інформації: один рівень об'єкта і два метарівня). Рівень об'єкта включає інформацію, в яку вірить агент. Перший метарівень містить інформацію про те, як обробляти вхідну інформацію на основі її контексту. Мета-метаінформація визначає, як внутрішні процеси агента можуть бути змінені і за яких обставин.

До недоліка слід віднести наступний:

– поява додаткового рівня складності, пов’язаного з тим, що норми, які засвоїв агент, можуть впливати як на генерацію, так і на вибір намірів.

Когнітивні моделі [45] і моделі соціального моделювання, незважаючи на те, що вони часто переслідують одну і ту ж мету (тобто представляють поведінку осіб, які приймають рішення), схильні мати інше уявлення про те, що є гарною моделлю для прийняття рішень людиною.

У якості недоліка зазначається, що дослідники соціальних симуляцій часто зосереджуються лише на моделях агентів, спеціально адаптованих до поставленого завдання, що обмежує реалізм і застосовність соціального моделювання.

Переваги цього класу моделей наглядно проявляються у вигляді результатів когнітивних процесів, а саме побудови так званих когнітивних карт:

– наочність факторів, які впливають на процес прийняття рішень;

– наочність зв’язків меж факторами (не тільки якісних, але й кількісних);

– можливість проводити так зване когнітивне моделювання, змінюючи вагу того чи іншого фактору, який впливає на кінцеве рішення.

Психологічні і неврологічні моделі часто називають когнітивними архітектурами. Однак, оскільки вони мають іншу спрямованість, ніж «когнітивні архітектури», які були згадані, вони виділені в окрему групу. Основна відмінність та перевага полягає в тому, що їх архітектури враховують передбачувані структурні властивості людського мозку.

Модельний людський процесор (MHP – model human processor) [46, 47] заснований на синтезі когнітивної науки і взаємодії людини з комп'ютером. Перевою Модельного Людського Процесора є те, що він включає в себе докладні специфікації тривалості дій і когнітивної обробки і розбиває складні дії на докладні маленькі кроки, які можна проаналізувати. Це дозволяє розробникам систем прогнозувати час, який потрібен людині для виконання завдання, уникаючи необхідності проводити експерименти з людьми-учасниками.

Перевагою архітектури CLARION [48] є наступне:

– використання гібридних нейронних мереж для моделювання задач в когнітивній та соціальній психології, а також для реалізації інтелектуальних систем штучного інтелекту. Це дозволяє відносно легко реалізувати архітектури даного класу на будь яких платформах штучних нейронних мереж;

– наявність вбудованої мотиваційної структури і метакогнітивних конструкцій;

– наявність двох дихотомій: явного та неявного уявлення, орієнтованого на дію, а не подання;

– об'єднання навчання як зверху вниз, так і знизу вгору;

– включення до складу ряду функціональних підсистем, які значно розширюють як сферу застосування архітектури, так і множини процесів, які підлягають моделюванню. Основними з таки підсистем є наступні. Підсистема, орієнтована на дію, яка виконує контроль всіх дій. Підсистема баз дій здійснює підтримку знань, як явних, так і неявних. Мотиваційна підсистема забезпечує основну мотивацію для сприйняття, дії і пізнання. Метакогнітивна підсистема здійснює динамічний моніторинг та управління і операцій всіх підсистем.

Таким чином, архітектура CLARION об'єднує реактивні процедури, загальні правила, навчання і прийняття рішень для розробки універсальних агентів, які навчаються в певних умовах і узагальнюють отримані знання в різних середовищах.

SOAR [49] – це символічна когнітивна архітектура, яка реалізує прийняття рішень як цілеспрямовану поведінку, що включає пошук в проблемному просторі і вивчення результатів.

Переваги цієї архитектури:

– розглядання процесів прийняття рішень як поєднання пошуку в проблемному просторі, так і вивчення отриманих результатів (тобто системи з зворотним зв’зком);

– поєднання результатів вивчення людської поведінки (дескриптивні моделі) та результатів штучного інтелекту (прескриптивні моделі);

– використання в архітектурі системи двох видів пам’яті: символічної довгострокової пам'яті (продукційні правила), і короткочасної (робочої) пам'яті (структура графа, щоб дозволяє подання об'єктів з властивостями, а також відносинами);

– можливість застосовувати правила паралельно, витягуючи кілька фрагментів знань одночасно;

– наявність додаткових контекстно-залежних знань для процесу прийняття рішень;

– розподіл операторів по декільком правилам, що дозволяє гнучко представляти знання про операторів, а також постійно оновлювати структури знань для операторів, дозволяючи перевизначати оператори, якщо цього вимагають обставини [50, 51].

Перераховані моделі можуть використовуватися на різних рівнях застосування, як наведено на рис. 3. Для більш детального ознайомлення з рівнями використання моделей можна звернутися за посиланнями [52–55].

5. Розробка концепцію моделювання поведінки взаємодіючих агентів

Для прогнозування можливої поведінки нападника, обґрунтування вибору засобів протидії на системному рівні кіберзагрозам та розрахунку необхідної суми інвестицій у кібербезпеку з відповідним розподілом на напрямках та часу інвестування запропонована концепція моделювання поведінки агентів систем безпеки, яка реалізується на трьох рівнях (рівень системи безпеки, рівень індивідуальних агентів, рівень групи агентів) та спрямована на гарантоване забезпечення безпеки бізнес-процесів організації, що дозволяє створити контур бізнес-процесів системи безпеки (рис. 4).

Для формального опису модельного базісу концепції моделювання поведінки агентів систем безпеки було використано наступні позначення.

Для моделі онотології: C – множина, елементи якої називаються поняттями; H^C – ієрархія концепцій; R – множина, елементи якої називаються відносинами; $rel: R \to C \times C$ – функція, яка співвідносить концепції не таксономічно; $dom: R \to C$ – функція, яка задає предметну область R, а $range(R): \prod_2(rel(R))$ задає його діапазон.

Для моделі прийняття рішень та навчання: w – конкретна ситуація; W – множина всіх можливих ситуацій; DM_i – рішення, яке приймається i-м агентом.

Для моделі самоорганізації: Σ – структура системи; Φ – функція системи; R_w – відносини емерджентності; G – множина цілей; A – відносини адаптивності; P – множина елементів пам’яті; Θ – множина моментів часу.

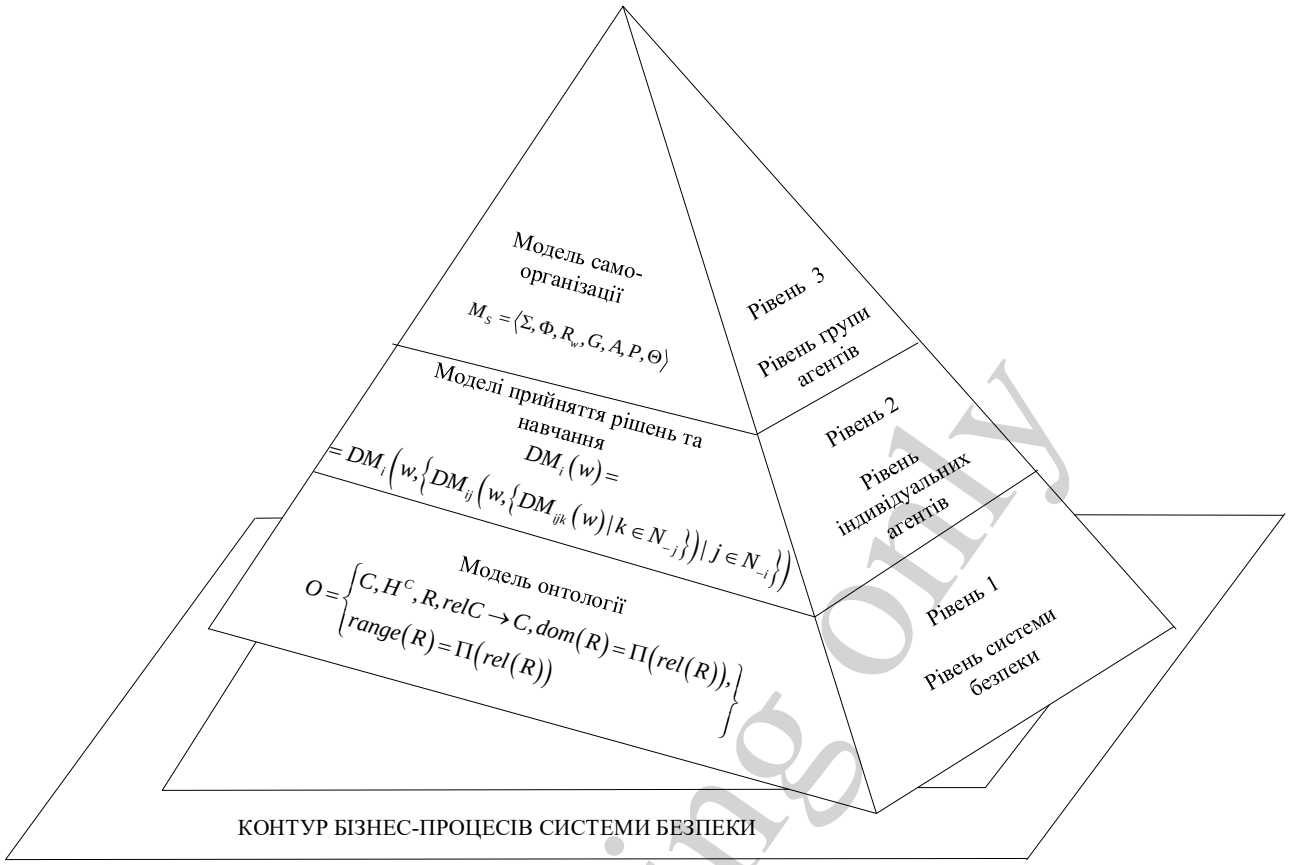

Рис. 4. Концепція моделювання поведінки агентів систем безпеки

Визначені такі дефініції:

– дефініція 1. Критичні бізнес-процеси – процеси, неналежні організації яких або недотримання вимог до їх виконання можуть становити фактичну або потенційну небезпеку для забезпечення якості продукції і, отже, для ефективності бізнесу;

– дефініція 2. Контур бізнес-процесів організації – сукупність інформаційних ресурсів та пов'язаних з ними бізнес-процесів, виконання яких у заданій послідовності забезпечує досягнення мети організації

$$S^{BC} = \left\{ \left\langle S^{BP_1}, IR^{BP_1}, T^{BP_1} \right\rangle, ..., \left\langle S^{BP_n}, IR^{BP_n}, T^{BP_n} \right\rangle \right\}, \quad (1)$$

де S^{BP} – контур бізнес-процесів як множина бізнес-процесів, кожен з яких являє собою: S^{Bpi} – i-й бізнес процес, заданий структурою зв'язків окремих бізнес-операцій, які виконуються в певній послідовності; IR^{BPi} – сукупність інформаційних ресурсів i-го бізнес-процесу; T^{BPi} – 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:

$$S^{BP} = \left\{ \left\langle S^{BP_1}, Rs^{BP_1}, T^{BP_1} \right\rangle, ..., \left\langle S^{BP_m}, Rs^{BP_m}, T^{BP_m} \right\rangle \right\}, \quad (2)$$

де S^{BP} – контур бізнес-процесів системи безпеки як множина бізнес-процесів, кожен з яких являє 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; T^{BSi} – сукупність загроз, захист від яких забезпечує i-й бізнес-процес системи безпеки.

Контур бізнес-процесів системи безпеки поєднує бізнес-процеси: управління безпекою, забезпечення безпеки, реалізацію, планування, перевірку та удосконалення.

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

$$O = \left\{ \begin{matrix} C, H^C, R, relC \to C, dom(R) = \\ = \Pi(rel(R)), range(R) = \Pi(rel(R)) \end{matrix} \right\}, \quad (3)$$

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; $rel : R \to C \times C$ – функція, яка співвідносить концепції не таксономічно; $dom : R \to C$ – функція, з $dom(R) := \prod_1 (rel(R))$ задає предметну область R, а $R \to C$ з $range(R) : \prod_2 (rel(R))$ 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, який запропонований в роботі [56], дозволив сформулювати відношення гібридності та синергетичності загроз залежно від їх типу та спрямованості. У класифікатор загроз введено платформу вартісних показників атак, що дозволяє оцінювати загрози з точки зору економічної ефективності їх використання та протидії їм. Запропонована шкала вимірювання вартості збитків для експертного оцінювання у вигляді: {незначний, низький, середній, високий, критичний}. Позначимо: i – поточний номер загрози $\left(\{i\}_1^N \right)$, k – поточний номер експерта, який виконував оцінку $\left(\{k\}_1^K \right)$. Середнє значення оцінки експертами вартості збитків за всіма загрозами для певного контуру бізнес-процесів для захісників, та вартості здійснення всієї множини атак для зловмисників можна записати таким чином:

$$P_k^A = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j p_{ijk}^A; \quad C_k^A = \frac{1}{KM}\sum_{j=1}^{M}\sum_{i=1}^{K}\alpha_j c_{ijk}^A, \tag{4}$$

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

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, p_{ijk} – оцінка k-м експертом вартості збитків від i-ї загрози j-му бізнес-процесу (верхній індекс визначає A – зловмисника, D – захисника), c_{ijk} – аналогічно для вартості здійснення загроз.

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

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

Таким чином, розроблена концепція моделювання поведінки взаємодіючих агентів, базис якої становить трирівнева структура моделювання суб'єктів та бізнес-процесів контурів функціонування організації та системи безпеки. Запропонована концепція відрізняється від існуючих використанням синергетичної моделі загроз при формуванні напрямків захисту інформаційних ресурсів контуру бізнес-процесів.

6. Розробка просторово-часової структури методології моделювання поведінки взаємодіючих агентів

Виходячи з цілі методології, вона повинна відображати процеси поведінки з двох боків. З одного боку відображати процеси, які пов’язані з поведінкою та особливостями окремого агенту системи безпеки. А з другого боку – поведінки та процесів, які виникають як результат сумісного функціонування агентів. При цьому необхідно приділити увагу моделюванню середовища функціонування агентів, бо таке оточення є носієм системоутворюючих функцій, що суттєво впливають на поведінку тієї чи іншої сторони конфлікту та їх характеристики.

В межах запропонованої концепції формується послідовність розробки моделей, методів та алгоритмів, що складають її. Процес побудови методології складається з 5 етапів.

Етап 1. Аналіз контурів БП та можливих атак на них

$$S^{BC} = \left\{\left\langle S^{BP_1}, IR^{BP_1}, Tr^{BP_1}\right\rangle, ..., \left\langle S^{BP_n}, IR^{BP_n}, Tr^{BP_n}\right\rangle\right\}, \tag{5}$$

де S^{BP} – контур бізнес-процесів як множина бізнес-процесів, кожен з яких представляє собою: S^{Bpi} – *i*-й бізнес процес. заданий структурою зв'язків окремих бізнес-операцій, які виконуються в певній послідовності; IR^{BPi} – сукупність інформаційних ресурсів *i*-го бізнес-процесу; T^{BPi} – сукупність загроз, що діють на *i*-й бізнес-процес.

Eman 2. Розробка моделей рівня індивідуальних агентів системи безпеки

$$M_A = \left\{ M_A^{DM}, M_A^L \right\}, \tag{6}$$

де M_A – модель окремого агента; M_A^{DM} – модель прийняття рішень агентом; M_A^L – модель навчання агента.

Eman 3. Розробка моделей рівня групи агентів системи безпеки

$$M_G = \left\{ M_R^B, M_R^L \right\},$$

де M_G – модель групи агентів; M_R^B – модель поведінки групи агентів; M_R^L – модель навчання групи агентів.

Eman 4. Розробка моделей загальносистемного рівня

$$M_S = \left\{ M_S^C, M_S^{SO} \right\},$$

де M_S – модель загальносистемного рівня; M_S^C – моделі координації; M_S^{SO} – модель самоорганізації.

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

$$Tr_l = \arg \max_{\forall Tr_l \in Tr_C^D} K_l^D \cdot K_l^A, \tag{7}$$

де K_i^A – рейтинговий коефіцієнт (важливості) реалізації загрози *i*-му інформаційному ресурсу; K_j^D – рейтинговий коефіцієнт (важливості) вибудовування захисту *j*-го інформаційного ресурса.

Далі будуть наведені відповідні множини моделей, методів та алгоритмів, які формують той чи інший рівень методології, з коротким описом контенту цього рівня. Зрозуміло, що на всі процеси, які відбуваються в контурах бізнес-процесів, безпеку яких забезпечують агенти системи безпеки, суттєво впливають загрози, які спрямовані на порушення нормального функціонування бізнес-процесів. Загрози реалізуються через здійснення атак на всі складові безпеки, а саме, кібербезпеки, інформаційної безпеки та безпеки інформації. Внаслідок цього аналіз ко-

нтурів бізнес-процесів як основної цілі спрямованих не неї загроз, необхідно починати з аналізу саме загроз, сукупність яких з відповідними показниками відображає класифікатор. Відповідність класифікатора загроз всім моделям, методам та алгоритмам методології визначає та гарантує ефективність використання методології моделювання поведінки агентів системи безпеки в цілому. Таким чином, аналіз контуру бізнес-процесів необхідно починати з аналізу та вдосконалення класифікатора загроз. В класифікатор загроз до існуючих платформ 1–4 додано нову платформу – платформу вартісних показників атак. Це дозволяє оцінювати загрози з точки зору економічної ефективності їх реалізації і протидії їм. Вдосконалений таким чином класифікатор загроз безпеці інформаційних ресурсів на відміну від існуючих містить показники вартості здійснення загрози та протидії загрозі. Використання вдосконаленого класифікатора дозволяє також оцінити ймовірність реалізації тієї чи іншої загрози та розробити ефективну оборонну стратегію (рис. 5).

Позначки на рис. 5 мають наступний зміст:

– для моделі онтології: C – множина, елементи якої називаються поняттями; H^C – ієрархія концепцій; R – множина, елементи якої називаються відносинами; $rel: R \to C \times C$ – функція, яка співвідносить концепції не таксономічно; $dom: R \to C$ – функція, яка задає предметну область R, а $range(R): \prod_2(rel(R))$ задає його діапазон;

– для моделі контуру бізнес-процесів опис позначок було наведено раніше;

– для класифікатору загроз: i – поточний номер загрози $\left(\{i\}_1^N\right)$, k – поточний номер експерта, який виконував оцінку $\left(\{k\}_1^K\right)$;. P_k^A, C_k^A – середні значення оцінки експертами ймовірнгості та вартості здійснення атак за всіма загрозами; P_k^D, C_k^D – аналогічні оцінки для захісників; 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.

Результуючою моделлю першого рівня методології є модель онтології взаємин між агентами сторін кіберконфлікта, яку можна розглядати як носій знань щодо предметної області. Для побудови моделі було використано підхід автоматизованої побудови онтології на основі різних наукових джерел (планарних текстів) TextToOnto. Модель онтології поведінки агентів в умовах конфлікту містить базові поняття процесів взаємодії агентів систем безпеки, а також поняття, що відображають взаємодію агентів протистояння, а не технічні сторони кіберконфлікту. Така спрямованість онтологічної моделі дозволяє обґрунтувати вибір моделі поведінки антагоністичних агентів в умовах гібридних загроз.

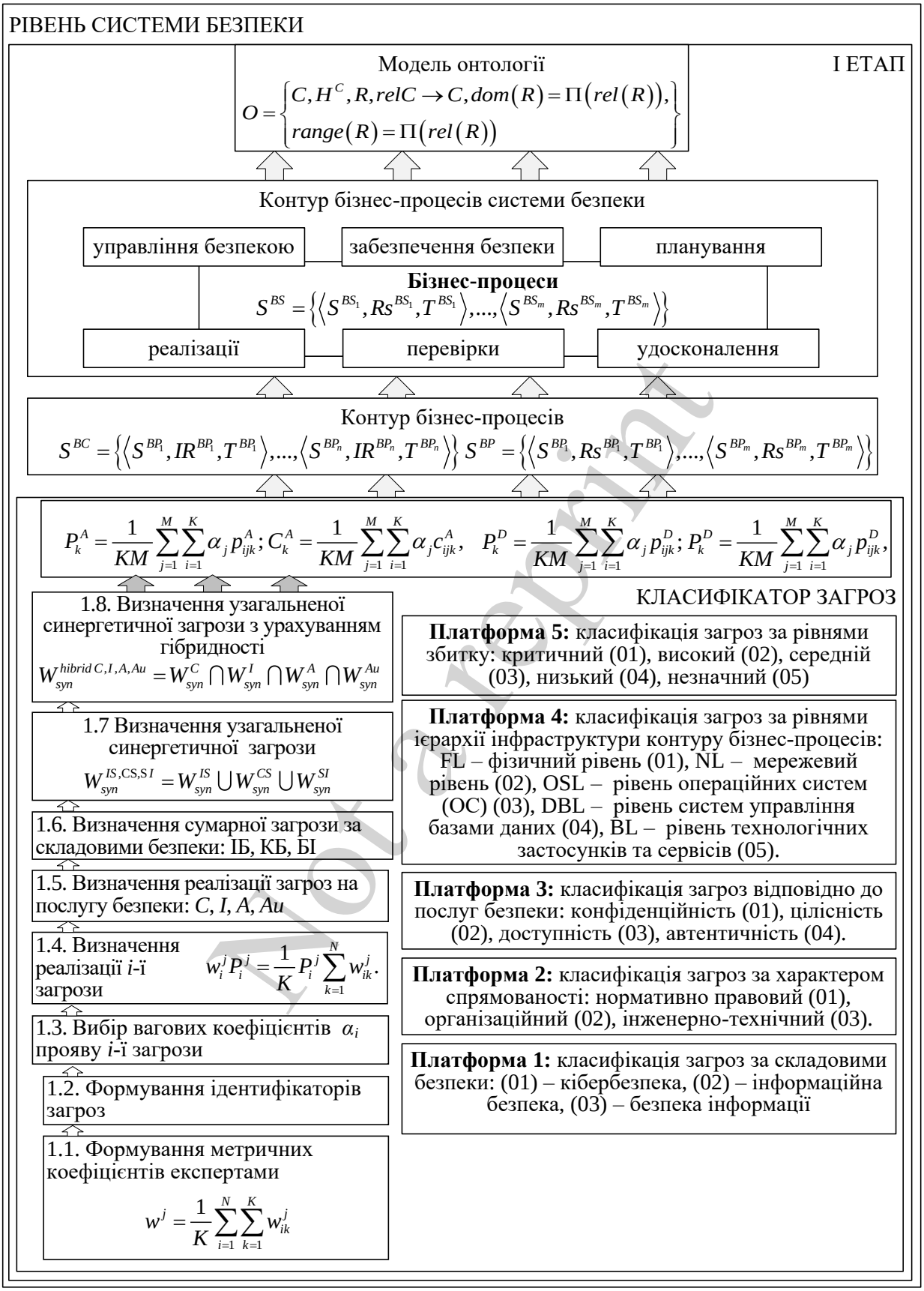

Рис. 5. Основні складові I етапу побудови методології (рівень системи безпеки)

На рівні індивідуальних агентів базової моделлю є модель рефлексивного агента (рис. 6). Основним припущеннім побудови моделі є припущення, що особо, що приймає рішення, розглядається як інформаційний канал. В цьому випадку основні показники його функціонування можна отримати за допомогою теорії інформації. До таких відносяться пропускна спроможність, генерування, блокування та координація інформації. Ці показники можуть використовуватися як для індивідуального агента, так і для групи агентів.

На рис. 6 використовуються наступні позначки: w – конкретна ситуація; W – множина всіх можливих ситуацій; DM_i – рішення, яке приймається i-м агентом; аі – дії i-го агента; G_i – цілі, які переслідує i-й агент; $e(DMi)$ – помилка агента, коли його рішення не відповідає його цілі; f_i – функція оцінки ситуації агентом; cf – функція координації рішення i-го агента з рішенням інших агентів оточення; h_i – функція вибору протидії загрозі; ch – функція координації вибору з вибором інших агентів.

Базовою функцією агента системи безпеки є функція прийняття рішень. Ці рішення можуть стосуватися як процесів оцінки ситуація та визначення типу загроз, так і визначення засобів протидії. Запропонована на цьому рівні базова модель прийняття рішення окремим агентом реалізує процес прийняття рішення на двох стадіях. Кожна з цих стадій (оцінка ситуації і вибір засобів протидії) передбачає узгодження сформованої оцінки з оцінками інших осіб, що приймають рішення. Присутність в динамічній моделі поведінки індивідуального агента процесів обміну інформацією на всіх стадіях прийняття рішення з іншими співпрацюючими агентами на відміну від існуючих моделей є суттєвою відмінністю. Врахування такої особливості поведінки при прийнятті рішення значно впливає на ефективність процесів захисту контуру бізнес-процесів від кібернападу в умовах гібридних загроз. Такий обмін можна розглядати як основу для формування сценаріїв групової поведінки.

Другою особливістю моделі є можливість призначення рівня рефлексії, що дозволяє стороні протистояння будувати у себе модель можливої поведінки протидії сторони конфлікту. Так, нульовий рівень рефлексії свідчить про те, що у агента безпеки немає ніякої інформації відносно агентського оточення протистояння. Тоді як вже перший рівень рефлексії вказує на те, що у агента є уявлення про функціонування в оточенні інших агентів. Другий рівень вказує, що протилежна сторона конфлікту також є рефлексивною, тобто моє модель поведінки протилежной сторони, і так далі. Рекурсивна модель рефлексивного агента містить моделі поведінки сторони нападу та дозволяє моделювати ймовірні дії зловмисників, і таким чином прогнозувати наслідки від прийнятих рішень стороною захисту. Аналіз рефлексивних здібностей агентів показую, що недоцільно реалізовувати рефлексію вище ніж за 2-й рівень.

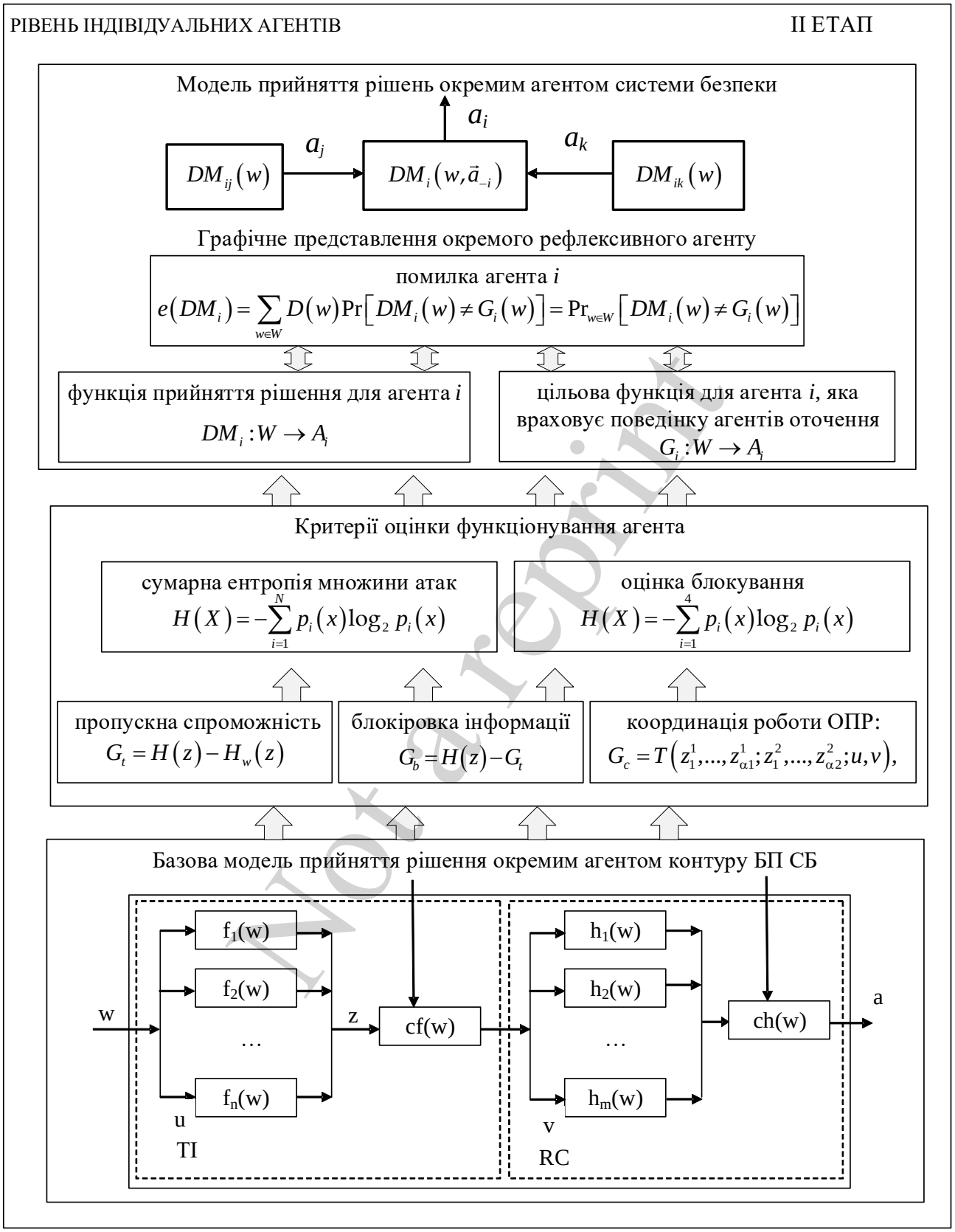

Рис. 6. Основні складові II етапу побудови методології (рівень індивідуальних агентів)

Другою особливістю моделі індивідуального агента системи безпеки є можливість врахування процесів навчання в процесі протидії кіберзагрозам. В процесах навчання також знаходять відображення рефлексивні властивості агентів. В традиційних моделях навчання можна накопичувати інформацію про зміну поведінки протилежної сторони конфлікту і будувати прогнози відносно дій протилежної сторони конфлікту. Тобто власна поведінка здійснюється в рамках формальної теорії прийняття рішень як гра проти пасивної природи. А навчання в умовах протидії активній стороні конфлікту враховує, що супротивник є активним агентом, має власні цілі і реагує, виходячи з власних цілей та враховуючи попередні дії супротивника. Тобто протилежна сторона є активною і також реалізує процес навчання, тобто вибір реакції повинен аналізуватися на базі теорії ігор та з урахуванням рефлексивних здібностей агента.

Таким чином, на рівні індивідуальних агентів запропоновано моделі навчання рефлексивних агентів, які відрізняються від моделей традиційного навчання тим, що враховують зміну поведінки агентів навколишнього середовища. Для оцінки якості навчання та динамічності процесів запропоновано використання наступних показників: швидкість змін рішень агенту, коефіцієнт змін, коефіцієнт утримання, та узагальнюючий коефіцієнт волатильності. Запропоновані коефіцієнти показують, як довго агент буде дотримуватися прийнятого рішення, готовність агенту переглянути прийняте раніше рішення та його здатність швидко реагувати на зміни в оточуючому середовище протистояння.

На відміну від існуючих, запропонована модель навчання агентів враховує мультиагентне середовище функціонування, що дозволяє реалізувати адаптацію поведінки агента у динамічному середовищі. Іншими словами, при навчанні агент враховує той факт, що він знаходиться в процесі протистояння з активним супротивником. Активний супротивник може мати свої цілі, характеризується відповідним рівнем раціональності, ита має здібності для навчання.

Для розробки моделей ІІІ-го рівня методології модель поведінки окремого агенту модифікована таким чином, щоб враховувати динаміку процесів і взаємодії окремих агентів. Тобто реакція агента формується не тільки під впливом отриманих результатів аналізу ситуації, а й з урахуванням аналогичних рішень, прийнятих агентами динамічного оточення (рис. 7).

На рис. 7 застосовано наступні позначення: $W=\{w_i\}$ – множина станів простору протистояння (інформація про кібератаки); $A=\{a_i\}$ – множина дій, які може здійснити агент; $Z=\{z_j\}$ – множина станів, в яких може перебувати агент; $z_i(t+1)=f_i\left(z_i(t),u_i(t),w_i(t)\right)$ – функція переходів; $u_{ij}(t)=g_{ij}\left(z_i(t)\right)$ – функція агрегування; $C=c_i\left(z_i(t),z_i(t+1),u_i(t),w_i(t)\right)$ – функція локальних витрат; $a_i(t)=h_i\left(z_i(t),u_{ji}(t)\right)$ – локальна функція виходу.

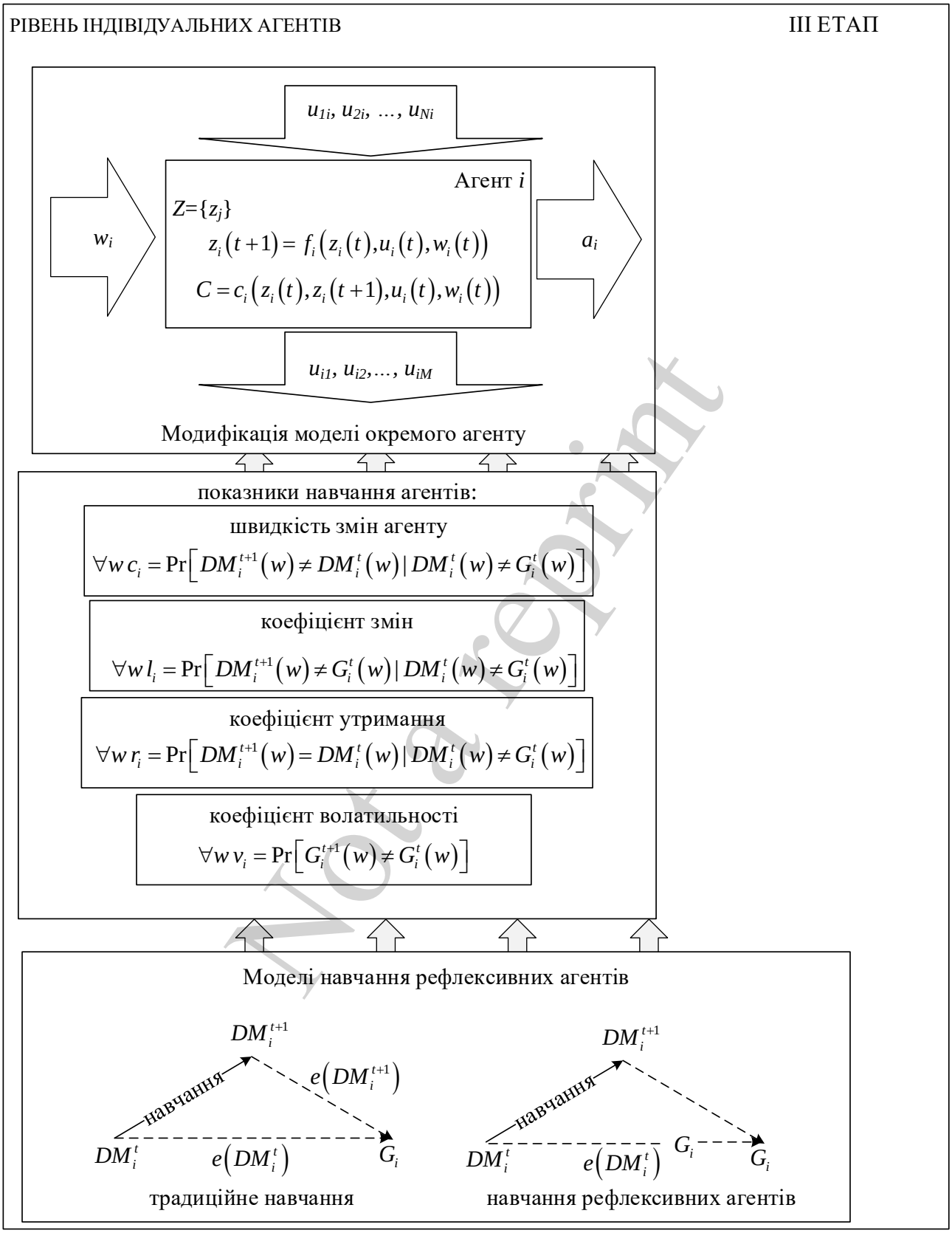

Рис. 7. Основні складові III етапу побудови методології (рівень індивідуальних агентів)

Рівень групи агентів повинен містити різноманітні методи координації у групах агентів безпеки. Різні методи координації поведінки агентів пояснюються тим фактом, що метод враховує рівень рефлексивності агента. Так метод координації без комунікації відображає той факт, що агент має 0-й рівень рефлексивності, тобто це агент, який ніяким чином не враховує функціонування серед подібних агентів. Метод координації з абстрацією, навпаки, використовується в тому випадку, коли агент будує у себе модель поведінки супротивника, який в свою чергу, також моє модель поведінки супротивника. Застосування різних методів координації дозволяє організувати співробітництво між агентами системи безпеки для забезпечення задач кіберзахисту в досить широкому діапазоні умов функціонування.

Застосування запропонованих характеристик оцінки ефективності функціонування агентів може бути продемонстровано на прикладі двох структур взаємодії агентів. Перша структура – паралельна, коли агенти працюють спільно, можливо незалежно, координуючи свої дії самостійно.

У другій структурі – один з агентів займається координацією роботи двох других агентів. Знання конкретних характеристик агентів, зокрема їх ефективності приймати рішення і координувати роботу, дозволить зробити висновок – яка зі структур є більш ефективною з точки зору продуктивності групи агентів.

Методика оцінки ефективності структури взаємодії групи агентів безпеки дозволяє обґрунтувати вибір структури взаємодії, а також розподілити функції захисту ресурсів бізнес-процесів, що забезпечує підвищення рівня захищеності контуру бізнес-процесів. На відміну від існуючих, запропонована методика розглядає агента як переробника інформації з відповідними характеристиками та базується на процесах обробки інформації та відповідних характеристиках ефективності функціонування системи безпеки.

Завершуюча модель самоорганізації поєднує моделі структури та функцій системи безпеки, відношення емерджентності та адаптивності, а також такі множини як множини цілей, елементів пам’яті, моментів часу та вхідних впливів. Модель самоорганізації забезпечує побудову робастної системи безпеки в умовах синергетичних та гібридних загроз, базується на синергії удосконалених моделей, та забезпечує емерджентні властивості бізнес-процесів в контурі безпеки. Можливість агрегування моделей, які орієнтуються на гібридні та сінергетичні загрози, суттєво відрізняє її від відомих аналогічних моделей (рис. 8).

На рис. 8 для моделі самоорганізації використані наступні позначення: Σ – структура системи; Ф – функція системи; R_w – відноини емерджентності; G – множина цілей; A – відносини адаптивності; P – множина елементів пам’яті; Θ – множина моментів часу.

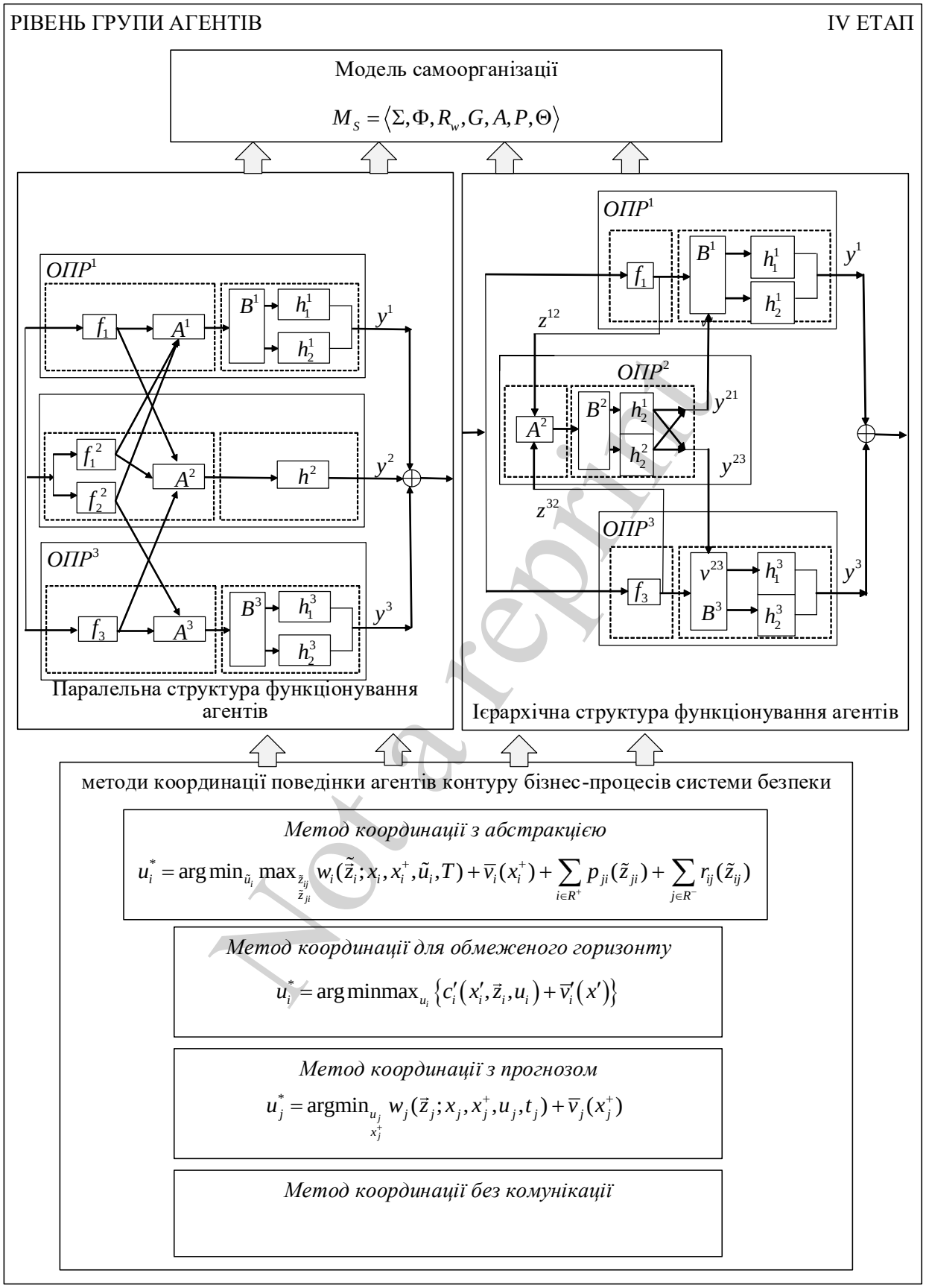

Рис. 8. Основні складові IV етапу побудови методології (рівень групи агентів)

Основною метою розробки методології моделювання поведінки агентів є підвищення рівня захищеності контуру бізнес-процесів організації. Це здійснюється за рахунок отримання оцінки ймовірності здійснення тієї чи іншої атаки на бізнес-процеси та інформаційні ресурси, що забезпечують їх функціонування. Запропонований алгоритм оцінювання економічної ефективності загрози то протидії їм дозволяє визначити найбільш ймовірні загрози, спрямовані на порушення безпеки інформаційних ресурсів. Як результат цього – економічно обґрунтувати розподіл обмежених коштів між різними інформаційними ресурсами та бізнес-процесами, які вимагають захисту. Запропонований алгоритм визначення найбільш вірогідної загрози дозволяє організувати ефективний розподіл обмежених коштів для захисту ресурсів контуру бізнес-процесів. Це здійснюється на основі використання результатів моделювання поведінки кооперативно-антагоністічних агентів, для визначення і оцінки ймовірності реалізації загрози. Модель визначення найбільш вірогідної загрози дозволяє організувати ефективний розподіл обмежених коштів для захисту ресурсів контуру бізнес-процесів на основі використання результатів моделювання поведінки кооперативно-антогоністічних агентів для визначення і розрахунку ймовірності реалізації загрози. Запропонований алгоритм оцінки враховує можливі рішення щодо проведення атаки та протидії їй, що приймаються всіма сторонами кіберконфлікту в умовах синергетичності та гібридності загроз. Тобто врахування рішень всіх сторін конфлікту, які мають рефлексивні властивості, та відображають вартісні показники ресурсів, що підлягають захисту, та вартості здійснення атаки, є суттєвою відмінністю запропонованого алгоритму. В результаті цього алгоритм дозволяє виявити той діапазон ресурсів, що є найбільш імовірним для здійснення кібератак (рис. 9). Метод оцінки безпеки грунтується на припущенні, що оцінка безпеки описується гаусовим законом.

Позначення на рис. 8 мають наступний сенс: 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; Tr_C^D – множина загроз, проти яких доцільно з точки зору вартості здійснювати захист; P_i^D – оцінка вартості втрати i-го інформаційного ресурсу для сторони захисту; C_i^D – вартість захисту i-го інформаційного ресурсу для сторони захисту; K_i^A – рейтинговий коефіцієнт (важливості) реалізації загрози i-му інформаційному ресурсу; M – потужність (кількість елементів) множини відібраних потенційно ефективних загроз для атакуючої сторони; K_j^D – рейтинговий коефіцієнт (важливості) вибудовування захисту j-го інформаційного ресурсу.

Запропонована методологія базується на сумісному використанні всієї наведеної множини моделей, методів та алгоритмів. Можна стверджувати, що сумісне

використання моделей, методів та алгоритмів призводить до синергетичного ефекту в процесі моделювання. 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 часом інвестування. Графічне зображення рівнів репрезентації моделей, методів та алгоритмів як складових методології моделюваннях поведінки агентів наведено на рис. 10.

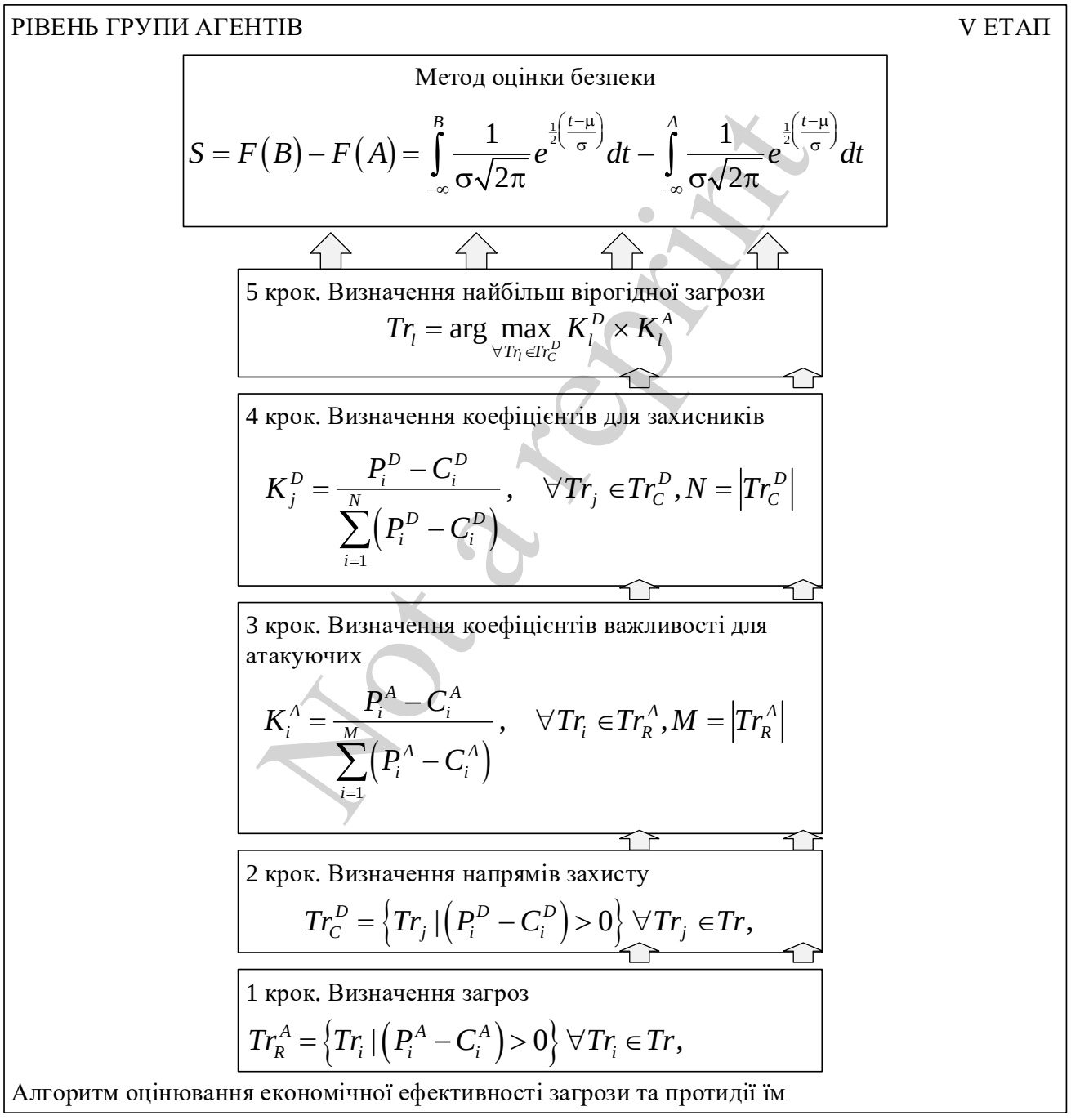

Рис. 9. Основні складові V етапу побудови методології (рівень групи агентів)

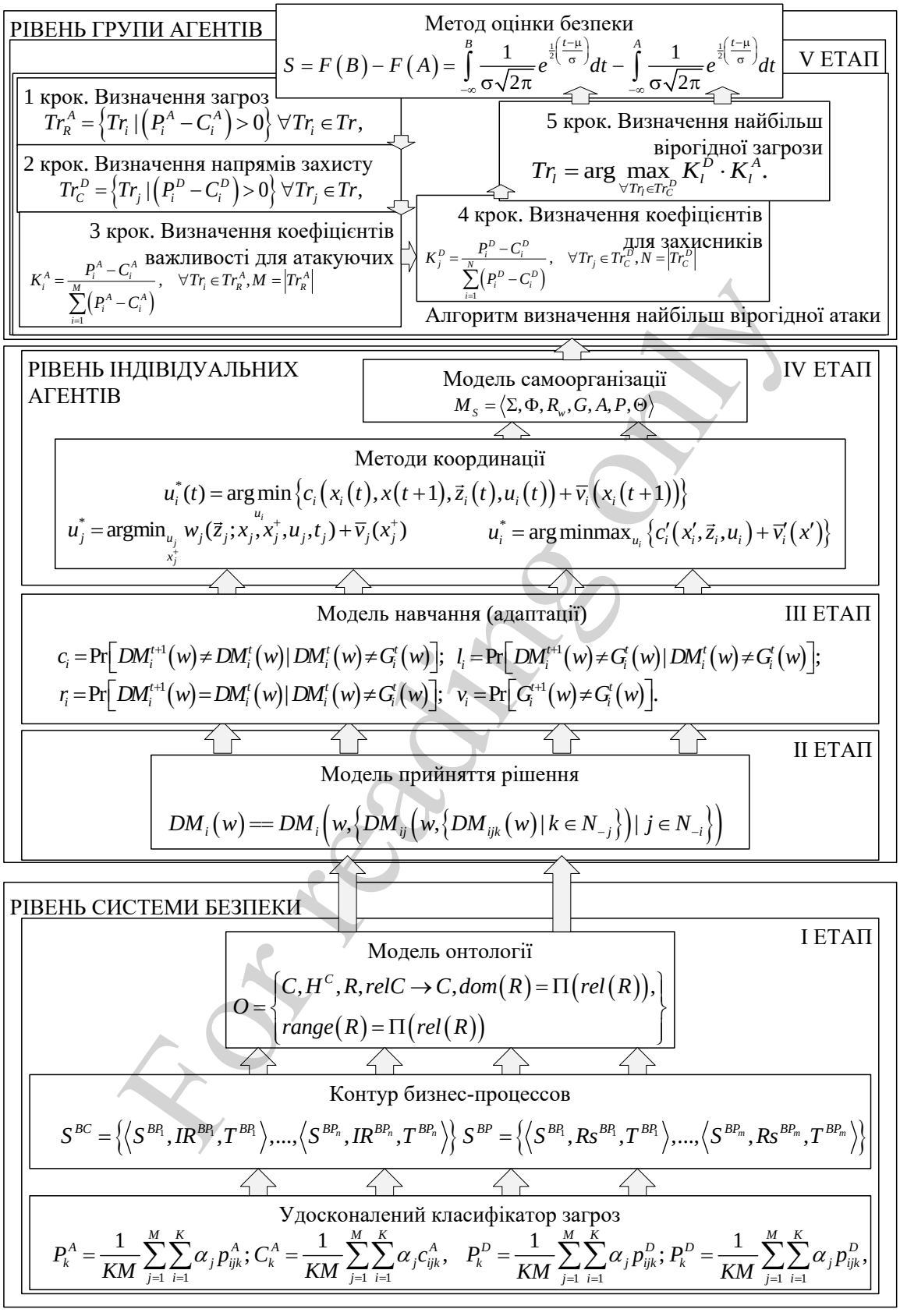

Рис. 10. Просторово-часова структура методології моделювання поведінки взаємодіючих агентів

Таким чином, запропонована методологія моделювання поведінки взаємодіючих агентів, базис якої становить трирівнева структура моделювання суб'єктів і бізнес-процесів контурів системи безпеки та функціонування організацій, дозволяє підвищити рівень захищеності контуру бізнес-процесів за рахунок зменшення у 1,76 разів кількості реалізації гібридних загроз, що забезпечує зменшення збитків у 1,65 рази та збільшення часу вибору засобів протистояння за рахунок скорочення на 38 % часу для ідентифікації загрози в онлайн режимі.

7. Проведення верифікації запропонованої методології на основі імітаційного моделювання

Для проведення верифікації моделей поведінки, розроблених в межах запропонованої методології моделювання були використані різні умови проведення та протидії атакам на контур бізнес-процесів. Імітаційне моделювання виконувалось для бізнес-процесів банківської, як однієї з систем, яка з одного боку є найбільш привабливою для здійснення атак, а з другого боку має детально розроблені бізнес-процеси здійснення основних функцій системи.

В якості підстави імітаційного моделювання розглядалися умови, які визначають так званий базовий прогін. Ці умови мають на увазі, перш за все, рівність можливостей для нападників і захисників і певне базове значення часу перемикання на інший вектор атак. Умови для кожного сценарію формувалися на основі базового прогону, інформаційної асиметрії можливостей захисника/атакуючого і значень вектору безпеки. Ці три умови були обрані з наступних причин.

По-перше, базовий сценарій показує поведінку системи, коли можливості сторін і значення цінності векторів атаки рівні. Це дозволяє реалізовувати стратегії "найслабкішої ланки" (WL – weakest link), а також "чекай та спостерігай" (WAS – wait and see) як в умовах визначеності, так і невизначеності при прийнятті рішень.

По-друге, можливості захисників і зловмисників визначають, наскільки ймовірно, що зловмисники будуть використовувати вектори атак в рамках стратегії WL, і наскільки ймовірно, що захисники будуть реагувати на порушення, ґрунтуючись на стратегії WAS. Якщо у атакуючого ресурси вище, ніж у захисника, він зможе реалізувати атаки за різними векторами. З іншого боку, більш високі можливості захисників означають, що захисники зможуть блокувати всі вхідні атаки. Це означає відсутність реакції на порушення (так як вони ніколи не реалізуються) і, отже, відсутність використання стратегії WAS.

Нарешті, асиметрія в значенні векторів атак надає аналізу більшу реалістичність, оскільки в дійсності вектори безпеки мають різні значення вагових коефіцієнтів, що визначають цінність того ресурсу, на який спрямована відповідна атака. Тому, коли порушення відбуваються по вектору з великою вагою, це може призвести до більшої або меншої шкоди в продуктивності захисника в залежності від значення такого вектору.

Простір сценаріїв являє собою множину альтернативних умов по відношенню до умов базового прогону. Зазначений простір включає умови базового сценарію,

асиметричні можливості і значення асиметричного вектору щодо базового сценарію з невизначеністю, яка дорівнює нулю і трьох рівнів невизначеності, класифікованих як низька, середня і висока невизначеність.

У якості об'єкту захисту банківської системи розглядалися контури бізнес-процесів системи стратегичного управляння бінку, системи управління бізнес-процесами банку, системи управління персоналом та організаційної структури банку, системи менеджмента якості банку, системи управління проектами, системи управління ризиками та системи управляння маркетингом.

Опис основних змінних, що використовуються в імітаційних моделях сценаріїв поведінки агентів контурів бізнес-процесів, та обмеження запропонованих моделей наведені в [57]. Детальний опис множини сценаріїв, які моделювалися в межах запропонованої методології, наведено в [58].

Значно скоротити фінансові витрати на організацію захисту об'єктів критичної інфраструктури як від звичайних, так і від гібридних атак, можливо наступним чином. По-перше, при запобіганні помилок при організації заходів з протидії кібератакам, по-друге, при виявленні помилок при виборі неадекватного методу протистояння атаки та поведінки протидіючої сторони на етапах, що передують реалізації атаки. Цільова установка, яка виникає при цьому, повинна зосереджуватися на пошуку адекватних моделей поведінки конфліктуючих агентів в умовах можливого кіберконфлікту, не чекаючи його реалізації.

Моделювання сукупності сценаріїв поведінки агентів системи безпеки було проведено за допомогою середовища візуального системного моделювання PowerSim.

Прогін базового сценарію показує, що атаки успішні, починаючи з вектору А, як показує початковий період (рис. 11). Однак зловмисники перемикаються на наступну найслабшу ланку, коли захисник виправляє недоліки безпеки, а нападник отримує інформацію про найбільш успішні атаки.

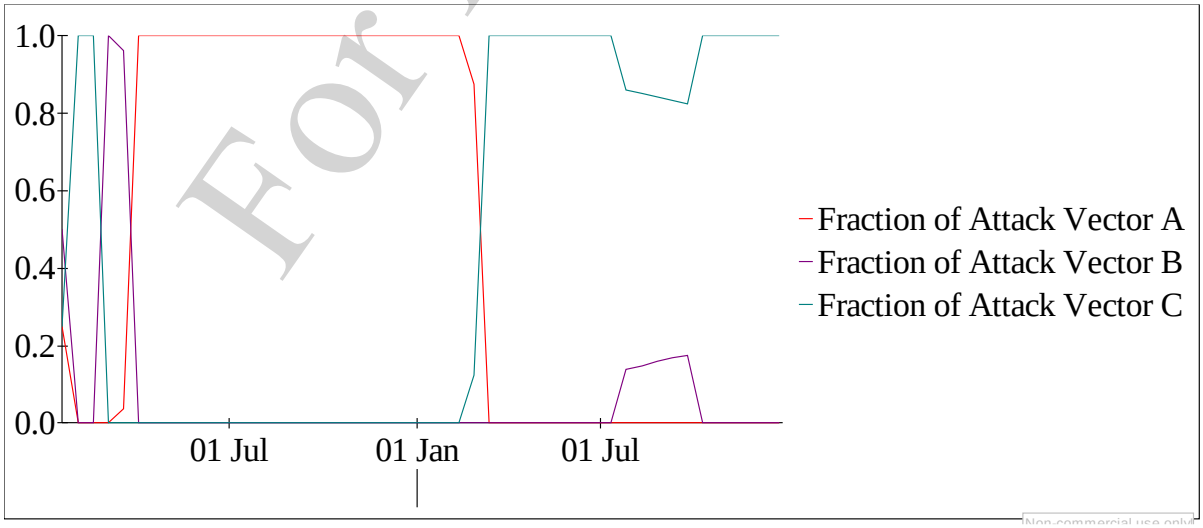

Рис. 11. Базовий прогін. Розподіл атак по векторах (частка від загальної кількості)

Мета сценарію асиметричних можливостей показати поведінку агентів, коли у одного з супротивників більше ресурсів, ніж у іншого, і який вплив цієї поведінки на успішні атаки і фінансові результати обох сторін. Нижче наведені припущення, які розглядаються в сценарії асиметричних можливостей:

– можливості захисників – 1000 одиниць;

– можливості атакуючих – 100±20;

– значення векторів безпеки однакові і дорівнюють одиниці.

При подальшому моделюванні і аналізі поведінки взаємодіючих агентів будемо враховувати, що для успішного відбиття атаки потрібно набагато більше можливостей, ніж для її організації та проведення. Для параметрів, використаних в процесі моделювання сценаріїв поведінки, це співвідношення становить приблизно 10 до 1.

У разі успішних атак, якщо можливості захисників значно перевершують можливості атакуючих, успішних атак не відбувається. Навпаки, коли можливості зловмисників перевершують деякий рівень, відповідний граничного рівня можливого відображення захисниками, атакуючі будуть постійно використовувати всі вектори атак.

Особливий інтерес представляє поведінка взаємодіючих агентів при перетині зазначеного рівня співвідношення засобів атакуючих та захисників.

При співвідношенні можливостей атакуючі-захисники 125:1000 можливостей атакуючих досить для проведення успішних атак по всім векторам. При цьому перемикання між векторами атак відбувається досить інтенсивне, що не дає можливості стороні захисту своєчасно реагувати, визначити і забезпечити захист найслабшої ланки (рис. 12). Точку перетину фінансових показників захисників та зловмисників можна трактувати як точку критичності зламу системи безпеки. Вона відповідає стану протистояння, коли фінансові показники захисників починають різки зменьшуватися у той час, коли прибуток сторони нападу хочь і повільно, але зрозрає. Іншими словами, можливостей захісників не вистачає для захисту будь якого ресурсу контуру бізнес-процесів.

При збільшені засобів сторони захисту стає можливим здійснювати захист все більшої кількості ресурсів. Рис. 13 демонструє виникнення точки критичності відновлення системи захисту, коли фінансові показники системи безпеки починають перевищувати показники сторони нападу і демонструють стійку тенденцію на збільшення.

Рис. 14–16 наочно демонструє динаміку співвідношення фінансових показників сторін протистояння. При збільшенні можливостей сторони захисту проміжок часу, коли здійснюються успішні атаки, стає все меншим. А при певному співвідношенні настає переломний момент, коли захисники спроможні відбивати все більше атак, а цей момент настає все раніше (рис. 14–16).

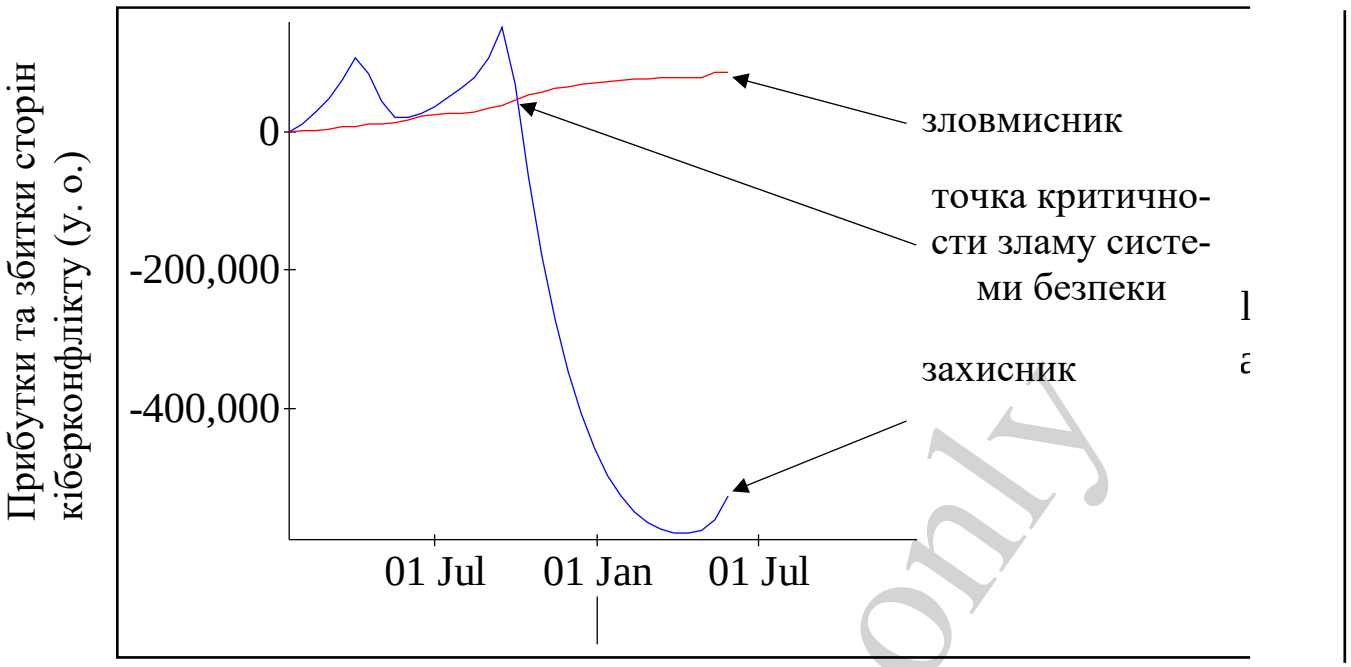

Рис. 12. Виникнення точки критичності зламу системи безпеки при недостатніх ресурсах

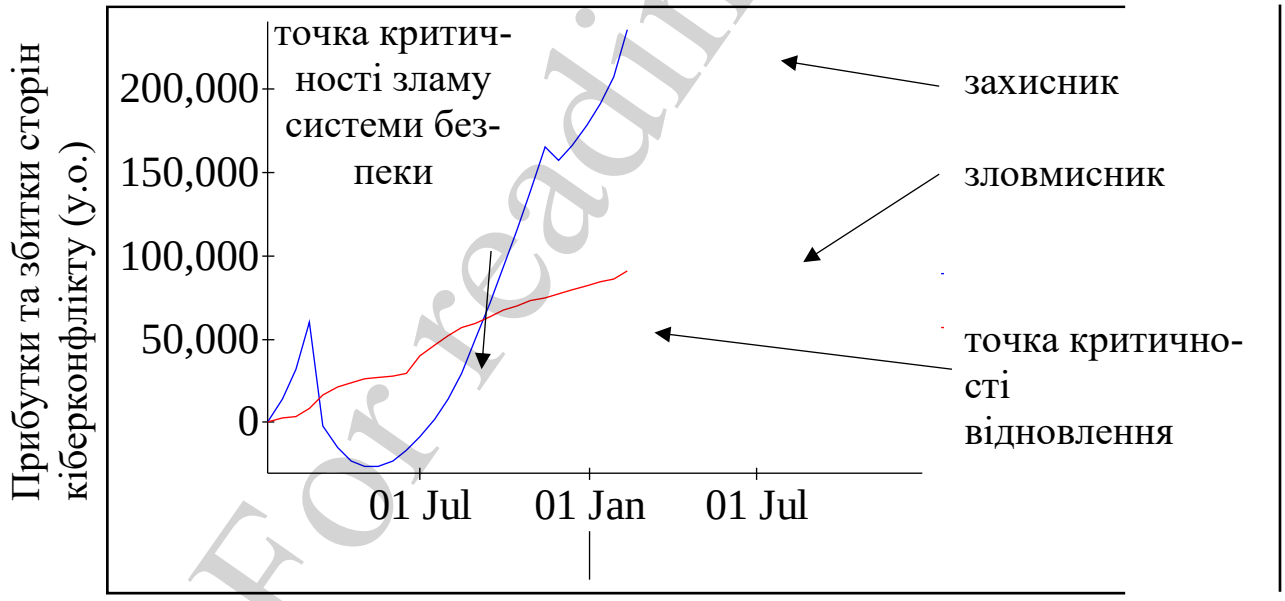

Рис. 13. Виникнення точки критичності відновлення системи безпеки при достатніх ресурсах

Отримані співвідношення дозволяють оцінити необхідний рівень інвестицій в кіберзахист для часткового або повного блокування атак на систему. Можна припустити, що отримані співвідношення (при налаштуванні моделі на конкретні

умови проведення кібератак) можуть використовуватися для оцінки можливостей сторони атаки, виходячи з наявних засобів захисту і динаміки відбиття атак.

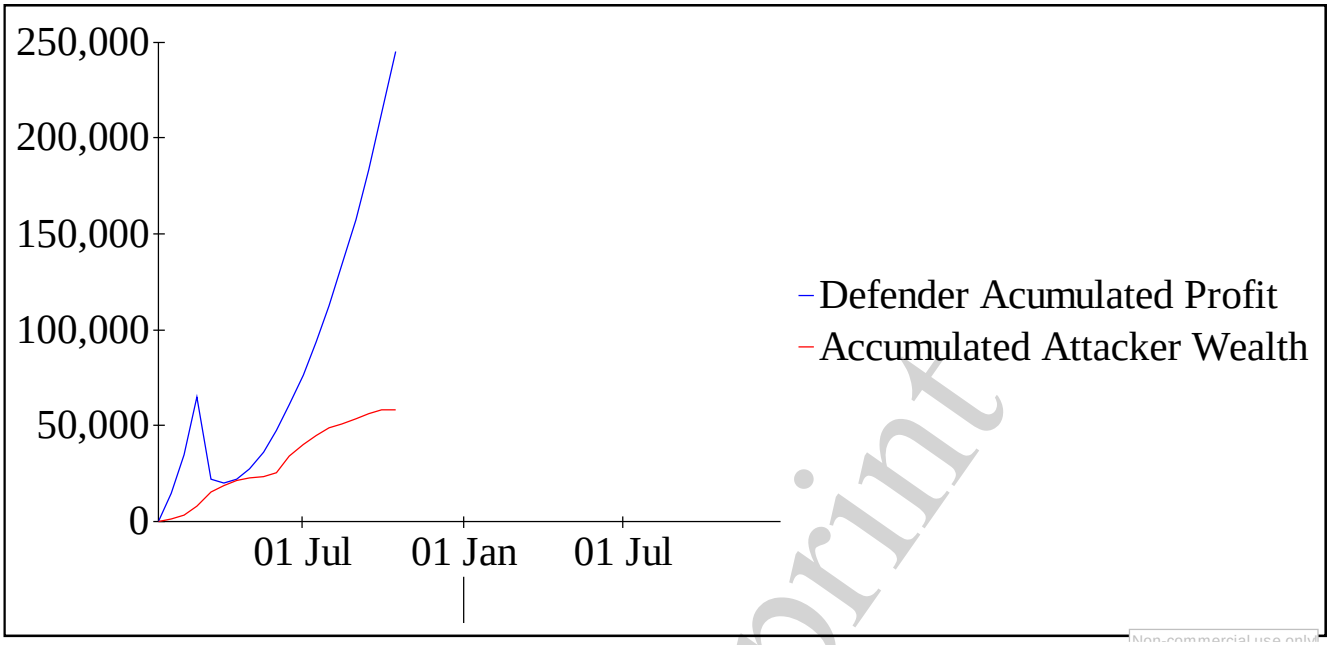

Рис. 14. Динаміки фінансових показників сторін протистояння (у. о.), співвідношення можливостей 92:1000

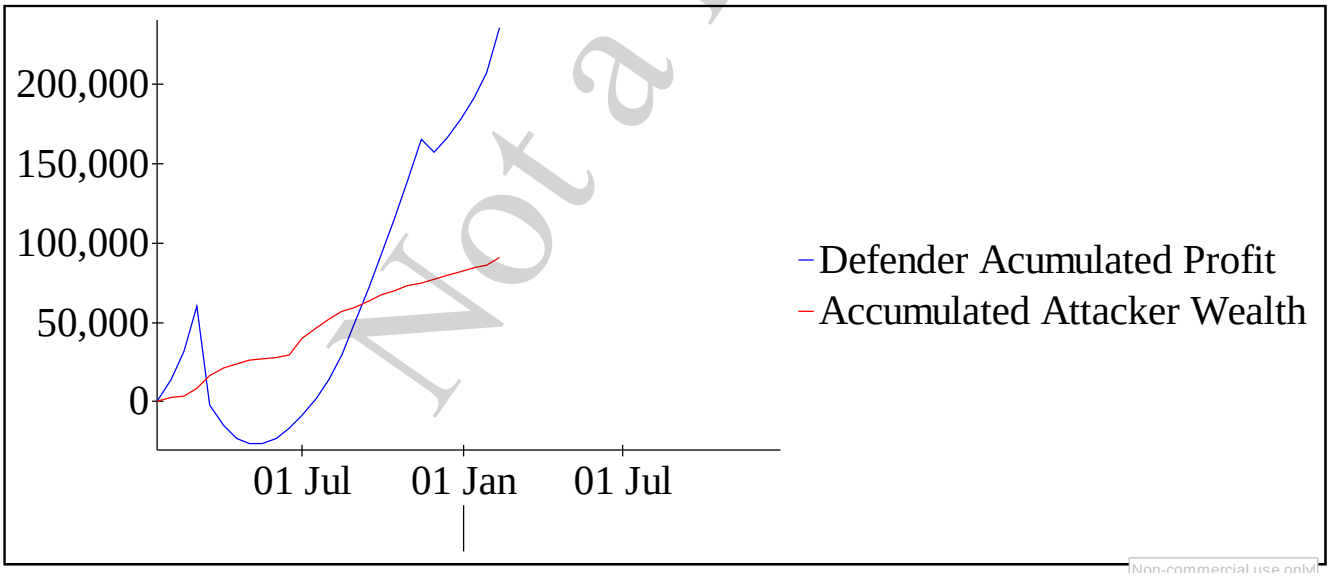

Рис. 15. Динаміки фінансових показників сторін протистояння (у. о.), співвідношення можливостей 93:1000

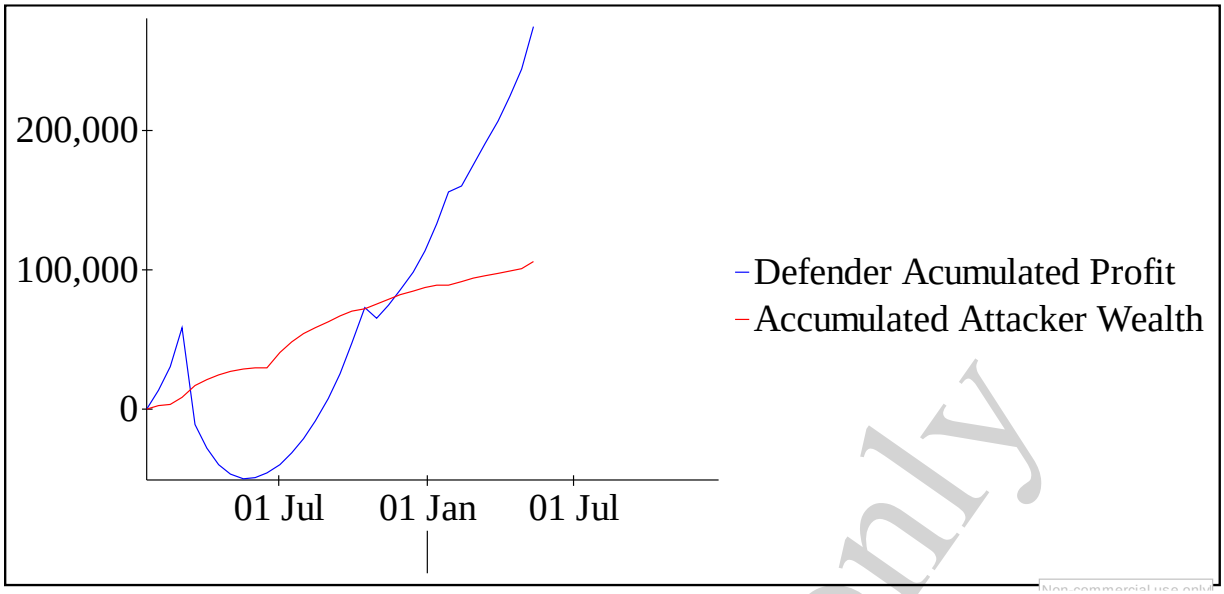

Рис. 16. Динаміки фінансових показників сторін протистояння (у. о.), співвідношення можливостей 94:1000

8. Обговорення результатів дослідження методології з використанням запропонованих моделей, методів та алгоритмів

Запропонована методологія з наведеною просторово-часовою структурою дозволяє підвищити рівень захищеності контуру бізнес-процесів за рахунок зменшення кількості реалізації гібридних загроз. Захисники приймають інвестиційні рішення, ґрунтуючись на даних про успішні атаки. Це означає, що атаки повинні бути припинені через деякий час або тому, що вони були відбиті, або робляться спроби знайти чергову уразливість в системі захисту (рис. 17).

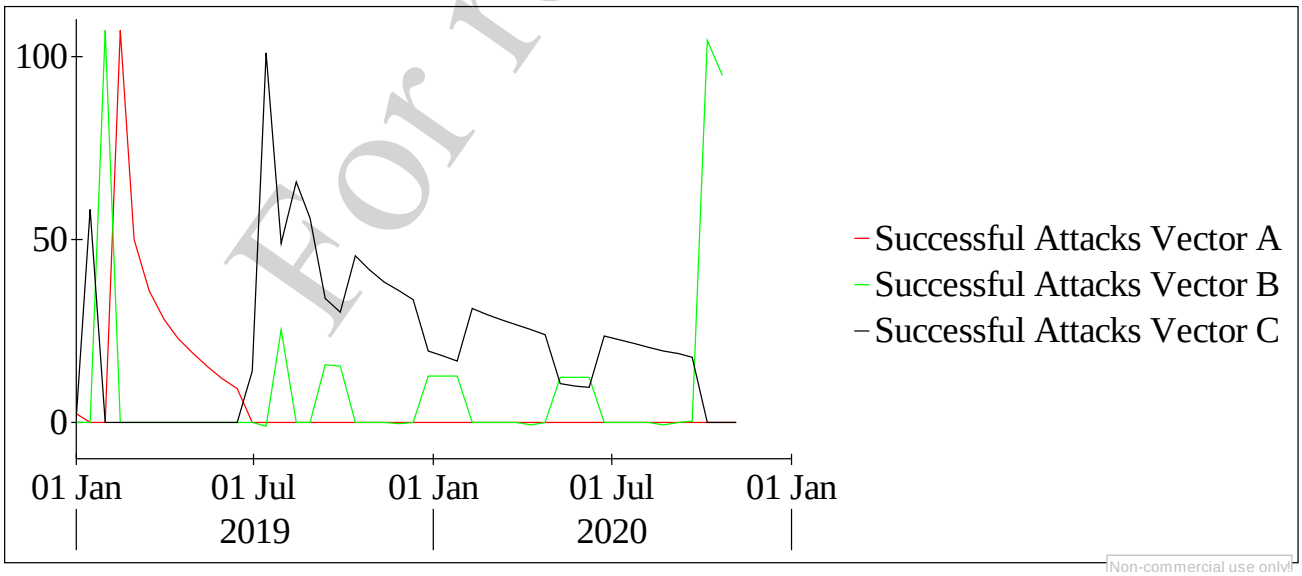

Рис. 17. Реактивне реагування на кіберзагрози

Основна мета сценарію збільшення часу перемикання між атаками полягає в тому, щоб збільшити час перемикання на інший вектор атак. Тому захисник “зберігає” звіти про успішні атаки протягом більш тривалого часу, щоб витягти з них більше інформації і в результаті зменшити невизначеність, пов'язану з майбутніми атаками (рис. 18).

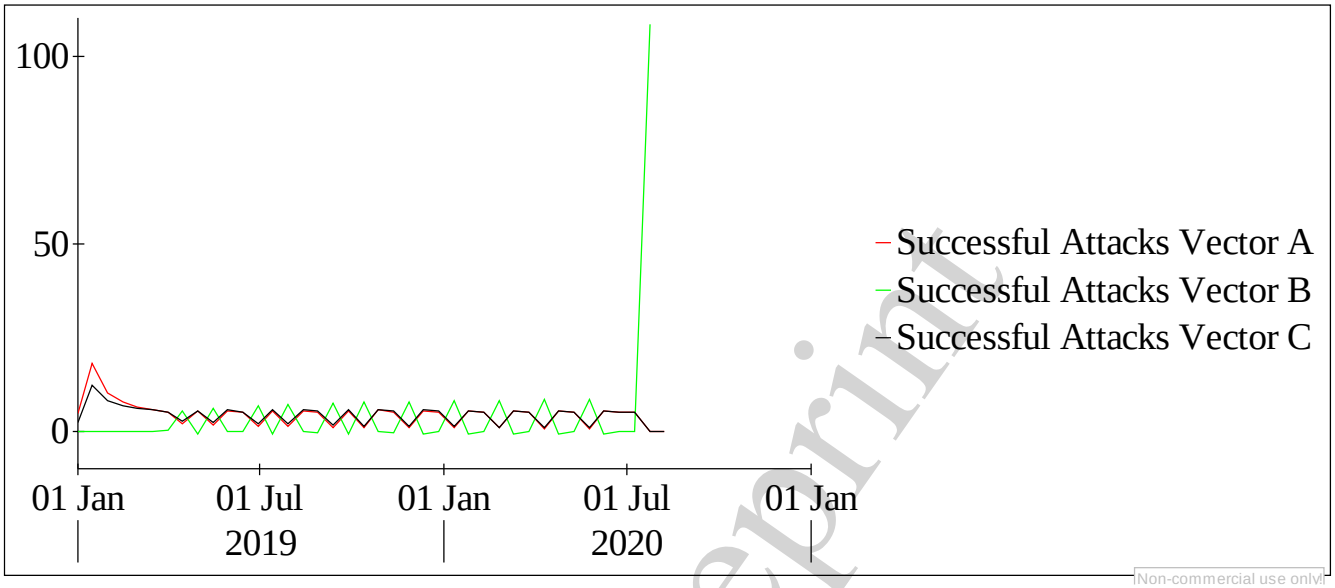

Рис. 18. Проактивне реагування на кіберзагрози

На рис. 19 наведені дані, які демонструють, що при збільшенні інтервалу на перемикання з одного вектора загроз на інший у 2 рази, кількість успішних атак зменшується у 1,76 разів. Подальше збільшення часу перемикання практично не впливає на зменшення кількості успішних атак.

При збільшені рівня безпеки контуру бізнес-процесів за рахунок додаткового фінансування час перемикання може бути збільшено до 3 разів (рис. 20).

Рис. 19. Зведені дані про успішні атаки в залежності від часу перемикання між векторами загроз

Рис. 20. Зведені дані про успішні атаки в залежності від часу перемикання між векторами загроз при збільшені рівня безпеки

Основна мета сценарію збільшення часу перемикання між атаками полягає в тому, щоб збільшити час перемикання на інший вектор атак. Тому захисник "зберігає" звіти про успішні атаки протягом більш тривалого часу, щоб витягти з них більше інформації і в результаті зменшити невизначеність, пов'язану з майбутніми атаками.

Це досягається за рахунок скорочення часу для ідентифікації загрози в онлайн режимі при використанні множини моделей та методів методології для прогнозування найбільш ймовіриних загроз. Як результат, це забезпечує зменшення збитків та збільшення часу на вибір засобів протистояння.

Запропонована методологія дозволяє знайти той мінімальний рівень інвестування в засоби захисту, який забезпечує появу точки критичності відновлення системи безпеки (рис. 9). Виконання сценарного моделювання дозволяє продемонструвати зв'язок між співвідношенням коштів у сторін протистояння та динамікою критичних точок зламу та відновлення системи безпеки (рис. 14–16).

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. Було виявлено залежність рівня захищеності контуру бізнес-процесів системи безпеки від часу перемикання з захисту одного вектора безпеки на інший. Виявлена залежність існує в інтервалі співвідношення ресурсів сторін захисту та протидії, при якому можуть здійснюватися атаки та застосовуватися засоби протидії їм. Найбільш явно це проявляється в невеликому діапазоні рівноваги можливостей захисників та зловмисників. На рис.17 показана динаміка успішних атак у разі реактивного реагування на атаки, а на рис. 18 – при проактивному реагуванні, коли інтервал перемикання з одного вектора атак на інший зростає. На рис. 19 наведені дані, які демонструють, що при збільшенні інтервалу на перемикання з одного вектора загроз на інший у 2 рази, кількість успішних атак зменшується у 1,76 разів (з 3485 до 1975). Подальше збільшення часу перемикання практично не впливає на зменшення кількості успішних атак.

Таким чином, запропонована 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 часом інвестування.

Однак для її використання потрібно володіння навичками не тільки математичного моделювання, але й імітаційного моделювання. Сценарії поведінки агентів вбудовані в наведені моделі, і тому для реалізації нових сценаріїв поведінки необхідно розробити нові, чи модифікувати існуючи моделі, що не завжди буває можливим.

В якості напрямку продовження наведеного дослідження можна запропонувати використання підходу, пов'язаного з ситуаційним управлінням. На відміну від існуючої системи управління безпекою системи бізнес-процесів, в основу якої покладені моделі як бізнес-процесів, так і моделі атак, поведінки агенті та ін., ситуаційне уп-

равління можна розглядати як управління по прецедентам. Центральним об'єктом становиться поняття ситуації, яке поєднує поточний стан системи, наявні ресурси та можливі дії тієї чи іншої сторони. Модель ситуації покладена основу побудови бази ситуацій, для якої необхідно розробити відповідні методи поповнення опису ситуацій, узагальнення та класифікацію ситуацій, а також розробку мови опису ситуацій. Поняття сценарію та його опис є невід'ємною частиною управління по прецедентам. Питання процедур прийняття рішень, планування в просторі задач та ситуацій потребують практичного втілення в системах безпеки. При цьому слід вказати, що методи ситуаційного управління орієнтовані на використання в таких умовах, коли побудова математичної моделі об'єкта чи суб'єкта управління неможлива чи є вкрай трудомісткою. При цьому ці методи від самого початку враховують присутність людини у контурі управління та його суб'єктивність сприйняття процесів, що відбуваються, та його характеристик при прийнятті рішень і поведінки в системах безпеки.

В умовах постквантового періоду, появи повномасштабного квантового комп'ютера гостро становіться питання які механізми зможуть забезпечити превентивні мери. Однім з перспективних напрямків, на думку фахівців НІСТ США, є використання крипто-кодових конструкцій Мак-Еліса і Нідеррайтера. Практичні алгоритми забезпечення основних послуг безпеки: конфіденційність, цілісність і автентичність запропоновані в роботах [59–61]. Такий підхід з урахуванням їх комерційної реалізації не містить кріптозакладок і забезпечує не тільки необхідний рівень криптостійкості, але і вірогідність, оперативність переданих даних. Таким чином, синтез заснований на запропонованій методології з перспективними алгоритмами забезпечення послуг безпеки дозволить істотно знизити можливості реалізації загроз на контур безпеки бізнес-процесів організації.

9. Висновки

1. Виявлені особливості моделювання поведінки взаємодіючих агентів систем безпеки в умовах кіберконфлікту, що дозволило визначити мінімально необхідні множини моделей, методів та алгоритмів, які забезпечують ефективне моделювання для оцінки необхідних засобів забезпечення відповідного рівня безпеки контуру бізнес-процесів. Множини моделей, методів та алгоритмів дозволяють прогнозувати можливу поведінку нападника та необхідні суми інвестицій щодо обґрунтування вибору засобів протидії сучасним загрозам.

2. Розроблена концепцію моделювання поведінки взаємодіючих агентів, базис якої становить трирівнева структура моделювання суб'єктів та бізнес-процесів контурів функціонування організації та системи безпеки, що базується на моделюванні поведінки антагоністичних агентів. Концепція може застосовуватися для прогнозування можливої поведінки нападника, обґрунтування вибору засобів протидії на системному рівні кіберзагрозам та розрахунку необхідної суми інвестицій у кібербезпеку з відповідним розподілом на напрямках та часу інвестування.

3. Розроблена методологія моделювання поведінки антагоністичних агентів систем безпеки, яка дозволяє прогнозувати можливу поведінку нападаючої сторо-

ни, обґрунтувати вибір засобів протидії на системному рівні кіберзагрозам та розрахувати необхідні суми інвестицій у кібербезпеку з відповідним розподілом за складовими безпеки та часом інвестування. Просторово-часова структура методології моделювання поведінки антагоністичних агентів системи безпеки визначає відповідні моделі, методи та алгоритми.

4. Проведено верифікацію запропонованої методології на основі імітаційного моделювання трьох сценаріїв поведінки агентів системи безпеки: базового сценарію, сценарію асиметричних можливостей та сценарію зміни часу перемикання з одного вектору загроз на інший. Верифікація продемонструвала практичну можливість застосування розробленої методології для забезпечення необхідного рівня захисту контуру бізнес-процесів при обмежених коштах на інвестування засобів захисту.

Література

1. Riley, M., Elgin, B., Lawrence, D., Matlack, C. (2014). Missed alarms and 40 million stolen credit card numbers: How target blew it. Bloomberg. URL: http://www.bloomberg.com/news/articles/2014-03-13/target-missed-warnings-in-epic-hack-of-credit-card-data
2. M-trends 2016. Mandaint: A FireEye Company. URL: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-mtrends-2016.pdf
3. Jajodia, S., Noel, S. (2010). Advanced cyber attack modeling analysis and visualization. Final Technical Report. URL: https://apps.dtic.mil/dtic/tr/fulltext/u2/a516716.pdf
4. Qin, X., Lee, W. (2004). Attack Plan Recognition and Prediction Using Causal Networks. 20th Annual Computer Security Applications Conference. doi: https://doi.org/10.1109/csac.2004.7
5. Xie, P., Li, J. H., Ou, X., Liu, P., Levy, R. (2010). Using Bayesian networks for cyber security analysis. 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN). doi: https://doi.org/10.1109/dsn.2010.5544924
6. Fava, D. S., Byers, S. R., Yang, S. J. (2008). Projecting Cyberattacks Through Variable-Length Markov Models. IEEE Transactions on Information Forensics and Security, 3 (3), 359–369. doi: https://doi.org/10.1109/tifs.2008.924605
7. Stotz, A., Sudit, M. (2007). Information fusion engine for real-time decision-making (INFERD): A perceptual system for cyber attack tracking. 2007 10th International Conference on Information Fusion. doi: https://doi.org/10.1109/icif.2007.4408113
8. Wang, B., Cai, J., Zhang, S., Li, J. (2010). A network security assessment model based on attack-defense game theory. 2010 International Conference on Computer Application and System Modeling (ICCASM 2010). doi: https://doi.org/10.1109/iccasm.2010.5620536
9. Grunewald, D., Lutzenberger, M., Chinnow, J., Bye, R., Bsufka, K., Albayrak, S. (2011). Agent-based network security simulation. In Proceedings of The 10th International

Conference on Autonomous Agents and Multiagent Systems, 3, 1325–1326. URL: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.387.1315&rep=rep1&type=pdf

10. Moskal, S., Wheeler, B., Kreider, D., Kuhl, M. E., Yang, S. J. (2014). Context Model Fusion for Multistage Network Attack Simulation. 2014 IEEE Military Communications Conference. doi: https://doi.org/10.1109/milcom.2014.32

11. Moskal, S., Kreider, D., Hays, L., Wheeler, B., Yang, S. J., Kuhl, M. (2013). Simulating attack behaviors in enterprise networks. 2013 IEEE Conference on Communications and Network Security (CNS). doi: https://doi.org/10.1109/cns.2013.6682726

12. Sheyner, O., Haines, J., Jha, S., Lippmann, R., Wing, J. M. (2002). Automated generation and analysis of attack graphs. Proceedings 2002 IEEE Symposium on Security and Privacy. doi: https://doi.org/10.1109/secpri.2002.1004377

13. Jha, S., Sheyner, O., Wing, J. (2002). Two formal analyses of attack graphs. Proceedings 15th IEEE Computer Security Foundations Workshop. CSFW-15. doi: https://doi.org/10.1109/csfw.2002.1021806

14. Moskal, S. F. (2016). Knowledge-based Decision Making for Simulating Cyber Attack Behaviors. Rochester Institute of Technology.

15. Kotenko, I., Man'kov, E. (2003). Experiments with Simulation of Attacks against Computer Networks. Computer Network Security, 183–194. doi: https://doi.org/10.1007/978-3-540-45215-7_15

16. Kotenko, I. (2005). Agent-based modeling and simulation of cyber-warfare between malefactors and security agents in internet. Proceedings 19th European Conference on Modelling and Simulation.

17. Kotenko, I. (2010). Agent-Based Modeling and Simulation of Network Infrastructure Cyber-Attacks and Cooperative Defense Mechanisms. Discrete Event Simulations. doi: https://doi.org/10.5772/46961

18. Kotenko, I., Doynikova, E. (2014). Security Assessment of Computer Networks Based on Attack Graphs and Security Events. Lecture Notes in Computer Science, 462–471. doi: https://doi.org/10.1007/978-3-642-55032-4_47

19. Kotenko, I., Doynikova, E. (2015). The CAPEC based generator of attack scenarios for network security evaluation. 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). doi: https://doi.org/10.1109/idaacs.2015.7340774

20. Мілов, О. В., Костяк, М. Ю., Мілевський, С. В., Погасій, С. С. (2019). Засоби моделювання поведінки агентів в інформаційно-комунікаційних системах. Системи управління, навігації та зв'язку, 6 (58), 63–70. doi: https://doi.org/10.26906/sunz.2019.6.063

21. Yevseiev, S., Milov, O., Milevskyi, S., Voitko, O., Kasianenko, M., Melenti, Y. et. al. (2020). Development and analysis of game-theoretical models of security systems agents interaction. Eastern-European Journal of Enterprise Technologies, 2 (4 (104)), 15–29. doi: https://doi.org/10.15587/1729-4061.2020.201418

22. Yevseiev, S., Karpinski, M., Shmatko, O., Romashchenko, N., Gancarczyk, T., Falat, P. (2019). Methodology of the cyber security threats risk assessment based on the fuzzy-multiple approach. 19th International Multidisciplinary Scientific GeoConference SGEM2019, Informatics, Geoinformatics and Remote Sensing. doi: https://doi.org/10.5593/sgem2019/2.1/s07.057

23. Yevseiev, S., Aleksiyev, V., Balakireva, S., Peleshok, Y., Milov, O., Petrov, O. et. al. (2019). 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, 3 (9 (99)), 49–63. doi: https://doi.org/10.15587/1729-4061.2019.169527

24. Yevseiev, S., Ponomarenko, V., Ponomarenko, V., Rayevnyeva, O., Rayevnyeva, O. (2017). 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, 6 (2 (90)), 4–15. doi: https://doi.org/10.15587/1729-4061.2017.118329

25. Sun, R. (2007). The importance of cognitive architectures: an analysis based on CLARION. Journal of Experimental & Theoretical Artificial Intelligence, 19 (2), 159–193. doi: https://doi.org/10.1080/09528130701191560

26. Gilbert, N. (2004). Agent-based social simulation: dealing with complexity. URL: http://wiki.commres.org/pds/AgentBasedModeling/AbssDealingWithComplexity.pdf

27. Carley, K. M., Prietula, M. J., Lin, Z. (1998). Design versus cognition: The interaction of agent cognition and organizational design on organizational performance. Journal of Artificial Societies and Social Simulation, 1 (3). URL: http://jasss.soc.surrey.ac.uk/1/3/4.html

28. Helbing, D., Balietti, S. (2011). How to do agent-based simulations in the future: From modeling social mechanisms to emergent phenomena and interactive systems design. Santa Fe Institute. URL: https://sfi-edu.s3.amazonaws.com/sfi-edu/production/uploads/sfi-com/dev/uploads/filer/bf/ee/bfee7621-d34e-438c-ae9a-cbe9346b7d85/11-06-024.pdf

29. Axelrod, R., Tesfatsion, L. (2006). Appendix A A Guide for Newcomers to Agent-Based Modeling in the Social Sciences. Handbook of Computational Economics, 1647–1659. doi: https://doi.org/10.1016/s1574-0021(05)02044-7

30. Nilsson, N. J. (1977). A production system for automatic deduction. Technical Note 148. URL: http://www.sri.com/sites/default/files/uploads/publications/pdf/743.pdf

31. Chao, Y. R. (1968). Language and Symbolic Systems. Journal of the American Oriental Society, 88 (2), 386. doi: https://doi.org/10.2307/597363

32. Ishida, T. (1994). Parallel, Distributed and Multiagent Production Systems. Lecture Notes in Computer Science. doi: https://doi.org/10.1007/3-540-58698-9

33. Georgeff, M., Pell, B., Pollack, M., Tambe, M., Wooldridge, M. (1999). The Belief-Desire-Intention Model of Agency. Lecture Notes in Computer Science, 1–10. doi: https://doi.org/10.1007/3-540-49057-4_1

34. Bordini, R. H., Hbner, J. F., Wooldridge, M. (2007). Programming Multi-Agent Systems in AgentSpeak usingJason. Wiley Series in Agent Technology. doi: https://doi.org/10.1002/9780470061848

35. Dignum, F., Kinny, D., Sonenberg, L. (2002). From desires, obligations and norms to goals. Cognitive Science Quarterly, 2 (3-4), 407–430. URL: https://dspace.library.uu.nl/bitstream/handle/1874/19827/dignum_02_from.pdf?sequence=1

36. Cohen, P. R., Levesque, H. J. (1990). Intention is choice with commitment. Artificial Intelligence, 42 (2-3), 213–261. doi: https://doi.org/10.1016/0004-3702(90)90055-5

37. Adam, C., Gaudou, B. (2016). BDI agents in social simulations: a survey. The Knowledge Engineering Review, 31 (3), 207–238. doi: https://doi.org/10.1017/s0269888916000096

38. Pereira, D., Oliveira, E., Moreira, N., Sarmento, L. (2005). Towards an Architecture for Emotional BDI Agents. 2005 Purtuguese Conference on Artificial Intelligence. doi: https://doi.org/10.1109/epia.2005.341262

39. Jiang, H., Vidal, J. M. (2006). From rational to emotional agents. In: Proceedings of the AAAI Workshop on Cognitive Modeling and Agent-based Social Simulation. URL: http://jmvidal.cse.sc.edu/papers/jiang06b.pdf

40. Kennedy, W. G. (2011). Modelling Human Behaviour in Agent-Based Models. Agent-Based Models of Geographical Systems, 167–179. doi: https://doi.org/10.1007/978-90-481-8927-4_9

41. Kollingbaum, M. J. (2005). Norm-Governed Practical Reasoning Agents. University of Aberdeen. URL: https://d1wqtxts1xzle7.cloudfront.net/4122560/10.1.1.140.9830.pdf?response-content-disposition=inline%3B+filename%3DNorm_governed_practical_reasoning_agents.pdf&Expires=1607609016&Signature=P7DWElEw3dWe3euGRJ8xm-3qVPj2zdQlNaUGqdC5RtoBYy~8r4ZTUf9iS-TyX7bnpLguKyGqdiuR964YWWpct8VTqzbUcbtfgjEJUy7LQqO4LnE7o3Gi9Jk48GGZZJJ1WTls4rdcJxbEIuV36edq~LW9NiKb1tVynLylL7EaJHuE3HixkysL26g37vixaHuysBefxcgtXmmLNB3JDs0GR-7lqn0c70LRzedugOdTGAAfbpcWIrsMEhG8jp39S4XUxjTgdU4czRuQOaBOcsRsoR8MPAL27CTg~2tvp9rBSXOu1SWurL4AgRxohSleQI0i9bt5~VZtwDtvm3u0gwTwwg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

42. Dignum, F. (1999). Autonomous agents with norms. Artificial Intelligence and Law, 7, 69–79. doi: http://doi.org/10.1023/A:1008315530323

43. Castelfranchi, C., Dignum, F., Jonker, C. M., Treur, J. (2000). Deliberative Normative Agents: Principles and Architecture. Lecture Notes in Computer Science, 364–378. doi: https://doi.org/10.1007/10719619_27

44. Conte, R., Castelfranchi, C. (1995). Cognitive and Social Action. Taylor & Francis, 224. doi: https://doi.org/10.4324/9780203783221

45. Sun, R. (2009). Cognitive Architectures and Multi-agent Social Simulation. Lecture Notes in Computer Science, 7–21. doi: https://doi.org/10.1007/978-3-642-03339-1_2

46. Card, S. K. (Ed.) (1983). The Psychology of Human-Computer Interaction. CRC Press, 488. doi: https://doi.org/10.1201/9780203736166

47. Byrne, M. (2007). Cognitive Architecture. Human Factors and Ergonomics, 93–113. doi: https://doi.org/10.1201/9781410615862.ch5

48. Sun, R., Peterson, T., Sessions, C. (2002). Beyond Simple Rule Extraction: Acquiring Planning Knowledge from Neural Networks. Neural Nets WIRN Vietri-01, 288–300. doi: https://doi.org/10.1007/978-1-4471-0219-9_32

49. Laird, J. E., Newell, A., Rosenbloom, P. S. (1987). SOAR: An architecture for general intelligence. Artificial Intelligence, 33 (1), 1–64. doi: https://doi.org/10.1016/0004-3702(87)90050-6

50. Laird, J. E. (2012). The SOAR Cognitive Architecture. MIT Press. doi: https://doi.org/10.7551/mitpress/7688.001.0001

51. Laird, J. E. (2012). The SOAR cognitive architecture. AISB Quarterly, 134, 1–4. URL: https://pdfs.semanticscholar.org/a065/0855634a156db81a01dcdceff931e9f1ac04.pdf

52. Wooldridge, M., Jennings, N. R. (1995). Agent theories, architectures, and languages: A survey. Intelligent Agents, 1–39. doi: https://doi.org/10.1007/3-540-58855-8_1

53. Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., Vlaev, I. (2012). Influencing behaviour: The mindspace way. Journal of Economic Psychology, 33 (1), 264–277. doi: https://doi.org/10.1016/j.joep.2011.10.009

54. Adam, C. (2007). Emotions: from psychological theories to logical formalization and implementation in a BDI agent. Institut de Recherche en Informatique de Toulouse. URL: https://oatao.univ-toulouse.fr/7612/1/adam.pdf

55. Steunebrink, B. R., Dastani, M., Meyer, J.-J. C. (2010). Emotions to control agent deliberation. AAMAS '10: Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems, 1 (1), 973–980. URL: http://dl.acm.org/citation.cfm?id=1838206.1838337

56. Shmatko, O., Balakireva, S., Vlasov, A., Zagorodna, N., Korol, O., Milov, O. et. al. (2020). Development of methodological foundations for designing a classifier of threats to cyberphysical systems. Eastern-European Journal of Enterprise Technologies, 3 (9 (105)), 6–19. doi: https://doi.org/10.15587/1729-4061.2020.205702

57. Milov, O., Yevseiev, S., Aleksiyev, V., Berdnik, P., Voitko, O., Dyptan, V. et. al. (2019). Development of the interacting agents behavior scenario in the cyber security system. Eastern-European Journal of Enterprise Technologies, 5 (9 (101)), 46–57. doi: https://doi.org/10.15587/1729-4061.2019.181047

58. Milov, O., Yevseiev, S., Ivanchenko, Y., Milevskyi, S., Nesterov, O., Puchkov, O. et. al. (2019). Development of the model of the antagonistic agents behavior under a cyber conflict. Eastern-European Journal of Enterprise Technologies, 4 (9 (100)), 6–19. doi: https://doi.org/10.15587/1729-4061.2019.175978

59. Yevseiev, S., Korol, O., Kots, H. (2017). Construction of hybrid security systems based on the crypto-code structures and flawed codes. Eastern-European Journal of Enterprise Technologies, 4 (9 (88)), 4–21. doi: https://doi.org/10.15587/1729-4061.2017.108461

60. Yevseiev, S., Hryhorii, K., Liekariev, Y. (2016). Developing of multi-factor authentication method based on niederreiter-mceliece modified crypto-code system. Eastern-European Journal of Enterprise Technologies, 6 (4 (84)), 11–23. doi: https://doi.org/10.15587/1729-4061.2016.86175

61. Yevseiev, S., Tsyhanenko, O., Ivanchenko, S., Aleksiyev, V., Verheles, D., Volkov, S. et. al. (2018). Practical implementation of the Niederreiter modified crypto-code system on truncated elliptic codes. Eastern-European Journal of Enterprise Technologies, 6 (4 (96)), 24–31. doi: https://doi.org/10.15587/1729-4061.2018.150903