КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.29.945
УДК 004.94:519.21

Шевченко Світлана Миколаївна
кандидат педагогічних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Жданова Юлія Дмитрівна
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Гаркушенко Аріна Максимівна
студентка Факультету інформаційних технологій та математики
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0009-0003-7568-7900
amharkushenko.fitm24m@kubg.edu.ua

КОГНІТИВНИЙ ПІДХІД В ІНФОРМАЦІЙНІЙ ТА КІБЕРБЕЗПЕЦІ

Анотація. У сфері інформаційної та кібербезпеки одним із найважливішим та найкритичнішим викликом є людський фактор, бо жоден програмний та технічний засіб не зможе повністю компенсувати відсутність усвідомлення інформаційних та кібернетичних ризиків, відповідної поведінки та відповідального ставлення до захисту інформації. Впровадження теорій когнітивних наук у сферу кіберзахисту дозволить підвищити рівень ефективності стратегій захисту. Когнітивне моделювання сприяє створенню математичних моделей, які імітують процеси людського мислення, прийняття рішень і поведінки, що наближає перехід від реактивного захисту до проактивного підходу. Дана стаття присвячена дослідженню впровадження когнітивного підходу в системи безпеки. На основі аналізу наукової літератури висвітлені основні дефініції когнітивної науки, зокрема, поняття когнітивного моделювання, когнітивного аналізу та синтезу, типів когнітивних моделей, нечіткої когнітивної карти. Окреслено переваги когнітивних теорій у різних галузях суспільства. Доведено, що когнітивне моделювання можливо застосовувати у сфері кібербезпеки для розуміння та передбачення поведінки як зловмисників, так і захисних систем. Охарактеризовано наступні когнітивні моделі в кіберсистемах: символічне моделювання (моделювання на основі правил) застосовують для побудови систем виявлення вторгнень (IDS), що аналізують мережевий трафік на предмет відомих атак; мережеве моделювання (моделювання з використанням нейронних мереж) включає системи виявлення аномалій, які аналізують типову поведінку мережі; баєсівські моделі (ймовірнісне моделювання) допомагають прогнозувати ризики та ймовірність успішного здійснення атаки на конкретну систему; моделювання на основі агентів використовується для симуляції кібератак і перевірки стійкості систем. Визначено, що ефективним є застосування гібридних моделей, які об'єднують вище вказані. Виділено виклики впровадження когнітивного моделювання у сферу безпеки. Це труднощі, пов'язані з потребою великих обсягів якісних даних про поведінку зловмисників, складність моделювання людської поведінки, етичні питання. Результати дослідження можуть бути використані в якості навчального матеріалу для студентів спеціальності F5 Кібербезпека та захист інформації.

Ключові слова: інформаційна безпека; кібербезпека; когнітивне моделювання; когнітивний аналіз; когнітивний синтез; нечітка когнітивна карта; когнітивні навички; захист інформації.

ВСТУП

Постановка проблеми. Сучасний ландшафт інформаційної та кібербезпеки дедалі стає все більш витонченим, складнішим, а інциденти, кіберзагрози та атаки зловмисників постійно удосконалюються та прогресують. Сучасні програмні та технічні засоби захисту інформації, безперечно, є потужним інструментом у боротьбі з кіберзагрозами. Вони забезпечують багаторівневий захист, автоматизують процеси та дозволяють оперативно реагувати на інциденти [1-3]. Однак, незважаючи на їхню ефективність, фундаментальною основою кібербезпеки залишається людина. Жодна технологія не зможе повністю компенсувати відсутність усвідомлення ризиків, належної поведінки та відповідального ставлення до інформаційної безпеки. Саме людина є найслабшою, але водночас і найсильнішою ланкою в системі захисту. «Когнітивні хаки, фішингові атаки, шкідливе програмне забезпечення, що розповсюджується через ботнети, та інші когнітивно-спрямовані атаки досягли значного успіху, реалізуючи свої експлойти, і, навпаки, корпоративні та урядові фахівці з безпеки витратили найменше часу, грошей, ресурсів та розумової енергії на розробку стратегій безпеки для захисту найслабшої ланки в організації» [4].

Ефективність заходів кібербезпеки значною мірою залежить від людської поведінки, пізнання та процесу прийняття рішень. Когнітивні науки, які охоплюють різні сфери, зокрема, психологію, комп'ютерні науки, штучний інтелект, лінгвістику, нейронауку, антропологію, надали цінну інформацію про людське пізнання світу, а саме, як отримується, зберігається, обробляється та використовується інформація. Це стало поштовхом краще зрозуміти когнітивні упередження, евристики та вразливості осіб, які беруть на себе відповідальність за рішення у сфері кібербезпеки. Очевидно, що посилення кібербезпеки є можливим за рахунок впровадження теорій когнітивізму: розуміння психологічних аспектів кіберзагроз та процесів прийняття рішень як зловмисниками, так і захисниками дозволить передбачити поведінку і розробити більш ефективні захисні стратегії.

Аналіз останніх досліджень і публікацій. Сучасність характеризується широким спектром наукової літератури, яка присвячена впровадженням теорій когнітивізму у різні галузі, зокрема, у сферу інформаційної та кібербезпеки. Мультидисциплінарний підхід когнітивних наук до кібербезпеки включає психологію для розуміння людського фактора, антропологію для формування безпечної культури, штучний інтелект для автоматизації захисту, лінгвістику для аналізу поведінкового контексту та нейронауку для інновацій у технологіях. Про важливу роль когнітивного моделювання для поліпшення захисту інформації підкреслено в роботах [4-11].

Застосування когнітивних карт для управління ризиками інформаційної безпеки пропонується у роботах [5-7], де в орієнтованому графі множина вагів дуг (сила впливу) є число $w_i = r_i = p_i q_i$, $0 \le w_i \le 1$, де r_i – ступінь ризику, p_i – ймовірність реалізації кожної загрози; q_i – ймовірність відповідних збитків; дані значення розраховуються на основі експертного оцінювання та за допомогою SWOT-аналізу. Структура когнітивних ризиків для кібербезпеки представлена у роботі [8, 9]. Автор наголошує, що конвергенція технологій, науки про дані, поведінкові дослідження та обчислювальні потужності мають працювати сьогодні для управління ризиками компаній, імітуючи механізми людського мозку.

Представлена когнітивна модель безпеки у статті [10] оптимізує операції кібербезпеки шляхом інтеграції великих даних, машинного навчання та систем підтримки рішень з когнітивними процесами аналітиків, що дозволяє прискорити

генерацію знань, розуміння та виконання заходів реагування, а також автоматизувати когнітивні завдання, зберігаючи аналітика центральною ланкою для верифікації та прийняття рішень за допомогою MAPE-K, OODA та концепції Human in the Loop. Їхньою метою було інтегрувати кілька когнітивних теорій та моделей для підтримки обізнаності про ситуацію в кібербезпеці.

Розробляючи когнітивну структуру, автори [11] покращили процес сприйняття та розуміння моделей аналізу уразливостей на основі штучного інтелекту. Авторська методика включає: збір та категоризацію різнорідних даних з онлайн-репозиторіїв кібербезпеки, інтегруючи їх у локалізовану базу; далі, використовуючи машинне навчання, генеруються шаблони загроз, уразливостей та атак, а також оцінюється серйозність ризику; нарешті, експерти з безпеки оцінюють ці машинно згенеровані індекси, а їхній зворотний зв'язок враховується в процесі офлайн-навчання.

Значущість та багатогранність даної проблеми виправдовують розгляд та обговорення наукових джерел для подальшого дослідження можливостей когнітивного моделювання при розв'язанні нових завдань у сфері кібербезпеки.

Мета статті. Метою статті є аналіз розробок застосування когнітивного моделювання в інформаційній та кібербезпеці.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Когнітивна наука бере свій початок з середини минулого століття. Поштовхом її розвитку стало створення комп’ютерів та перші спроби розробити штучний інтелект, що імітує людське мислення, а також розвиток психологічних теорій, які розглядають пізнання як процес обробки інформації, та становлення генеративної граматики й інших пов’язаних з нею напрямів лінгвістики. Тому вважають [12], що когнітивна наука – це комплекс дисциплін, що вивчають методи пізнання світу: як отримується, зберігається, обробляється та використовується інформація. Основною ціллю когнітивізму є пошук розуміння, як саме процеси в мозку людини створюють усвідомлення та суб’єктний досвід, з подальшим розробленням методологічного апарату для застосування.

Одним із інструментів когнітивної науки є когнітивне моделювання. «Когнітивне моделювання — це моделювання процесів людського мислення в обчислювальній моделі, яка є поєднанням різних дисциплін. Воно є важливим, оскільки дає знання про процеси мозку, такі як сприйняття, пам'ять та прийняття рішень; отже, його використовують для оцінки та розуміння поведінки людей у різних ситуаціях» [13]. Когнітивне моделювання дозволяє розробляти ментальні процеси та вирішувати прикладні задачі за допомогою спрощених (графових, символьних, тощо) моделей, що можуть бути комп’ютеризовані і автоматизовані [14].

Когнітивне моделювання, що об'єднує різні підходи залежно від конкретних завдань і об'єктів дослідження, можна розділити на кілька основних типів (рис.1). Це дозволяє більш глибоко вивчати пізнавальні процеси [13]. Символічне моделювання (або моделювання на основі правил) використовують для створення моделей, які імітують людське мислення, прийняття рішень та інші когнітивні функції. Моделювання на основі мереж застосовує штучні нейрони, які об’єднані в мережу. Остання навчається та адаптується до нової інформації, що дозволяє моделювати процеси навчання. Баєсівські моделі (ймовірнісне моделювання) використовуються для моделювання процесів прийняття рішень та прогнозування, враховуючи попередній досвід, і рішення залежить від ймовірнісної інформації. Моделювання на основі агентів використовує різні

симуляції, де віртуальні гравці працюють у віртуальному середовищі імітуючи різні поведінкові дії. Існують і гібридні моделі, які об'єднують вище перераховані.

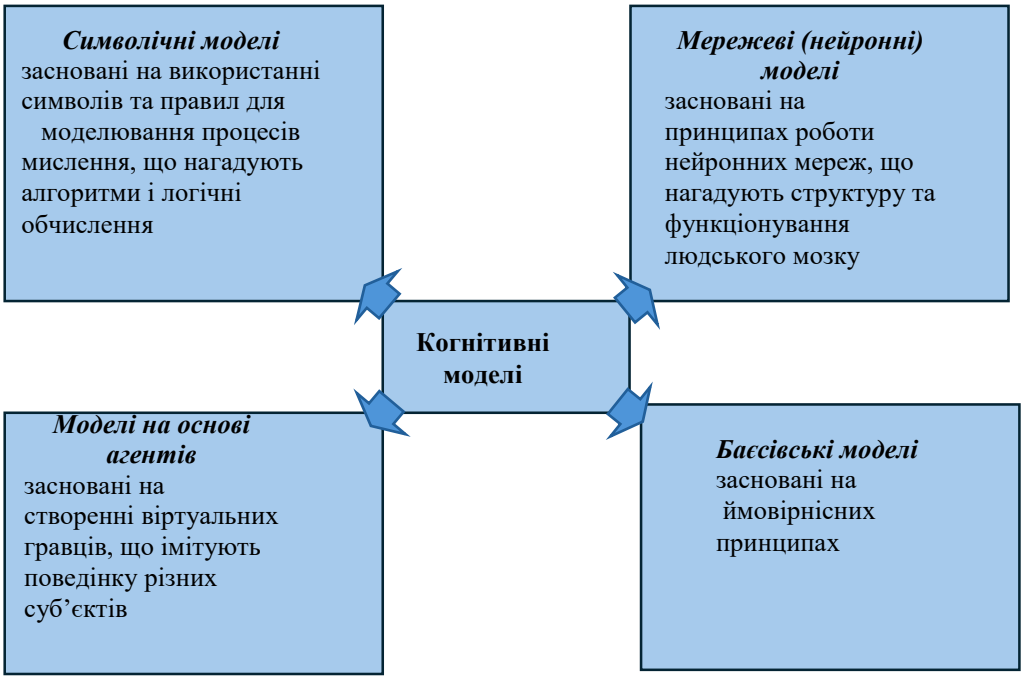

Рис.1. Основні типи когнітивних моделей

Аналіз наукової та методичної літератури [15-18] дозволив виділити у когнітивному моделюванні одночасне розв'язання двох взаємопов'язаних завдань: аналізу та синтезу пізнавальних систем, а саме, когнітивного аналізу та когнітивного синтезу. Дефініція цих понять та алгоритм виконання представлені у таблиці 1.

Таблиця 1.

Аналіз та синтез у когнітивному моделюванні

	Когнітивний аналіз	**Когнітивний синтез**
Поняття	Процес розкладання складної системи на її основні компоненти для визначення взаємодії між ним.	Процес об'єднання окремих компонент складної системи у цілісну модель з метою імітації поведінки всієї системи.
Процес виконання (на основі	1. Розробка когнітивної моделі (зокрема, когнітивної карти). 2. Аналіз шляхів і циклів когнітивної моделі. 3. Аналіз спостережуваності і керованості системи. 4. Аналіз стійкості і можливості катастроф. 5. Аналіз чутливості та/або сценарний аналіз. 6. Аналіз складності і зв'язності системи. 7. Аналіз можливостей адаптації та самоорганізації. 8. Прогнозування. 9. Прийняття рішень експертом.	Декомпозиція і композиція моделей. 2. Оптимізація параметрів. 3. Синтез системи з заданими властивостями з простих когнітивних структур шляхом декомпозиції або добудовування вихідної структури. 4. Прийняття рішень експертом.

	Когнітивний аналіз	**Когнітивний синтез**
Приклад. Імітація мислення оператора з кібербезпеки у системі виявлення загроз	Дослідження та вивчення різних типів загроз. Система аналізує, як зловмисники отримують доступ до мережі, як вони маскуються та викрадають дані. Здійснюється це за допомогою сканування портів, уразливостей, визначення привілеїв тощо.	Створення моделі, яка поєднує знання для прогнозування та вивчення нових інцидентів. Модель імітує зловмисника, прогнозуючи наступні дії та ідентифікуючи аналогічну поведінку в мережі, що може вказувати на початок атаки.

Якісні когнітивні моделі дозволяють забезпечувати кількісну оцінку конкретних когнітивних процесів за допомогою математичних обчислень [18]. Математичні моделі пізнання вимірюють індивідуальні відмінності в таких когнітивних процесах, як швидкість обробки інформації, обсяг робочої пам'яті та виконавчі функції, які можуть бути основою загального інтелекту [17]. Завдяки цьому когнітивні моделі дозволяють виявляти зв'язки між конкретними пізнавальними процесами і відстежувати, як експериментальні втручання, спрямовані на поліпшення інтелекту, впливають на параметри цих процесів. Опис переваг когнітивних моделей представлено у таблиці 2 [17].

Таблиця 2

Переваги когнітивних моделей

Переваги	**Опис та основні характеристики**
Пояснювальна сила	Когнітивні моделі не просто прогнозують результат, а й надають конкретне пояснення когнітивних процесів, які є джерелом майбутньої поведінки, і це пояснення можливо перевірити за допомогою математичних теорій. На відміну від статистичних моделей, які можуть показати лише кореляцію, когнітивні моделі пропонують фальсифіковані гіпотези про те, як працює мозок.
Інтерпретованість параметрів	Кожен параметр у когнітивній моделі має чітке та об'єктивне значення, що відповідає певному аспекту когнітивного процесу (наприклад, швидкість обробки інформації або обсяг пам'яті). Це дозволяє дослідникам розуміти, що саме вимірює модель.
Оцінка індивідуальних відмінностей	Когнітивні моделі дозволяють кількісно оцінити, як саме індивіди відрізняються один від одного у певних когнітивних процесах. Це допомагає не лише виявити відмінності, а й зрозуміти, які конкретні аспекти пізнання (наприклад, швидкість уваги, швидкість прийняття рішень) лежать в основі цих відмінностей.

Серед методів когнітивного моделювання виділяють побудову нечіткої когнітивної карти, перевагами якої є простота, наочність, визначення структури причинно-наслідкових зв’язків між елементами складної системи [5-7, 15]. Нечітка когнітивна карта – це орієнтований граф, вершини (концепти) якого представляють системні змінні, а зважені дуги відображають силу впливу одного концепта на інший [19]. Ця математична модель ідеально підходить для комп'ютерного моделювання. Її структура дозволяє легко трансформувати її в програмний код, що дає змогу створити ефективну програму для проведення статичного та динамічного аналізу складної системи.

Область застосування когнітивного моделювання досить широка – бізнес, управління, кібернетика, соціологія, психологія, військова сфера, інформаційна безпека конфліктологія, тощо. Когнітивне моделювання використовується для створення систем

штучного інтелекту, що імітують людське мислення та вирішення проблем. Наприклад, моделі ACT-R або SOAR допомагають покращити обробку природної мови, дозволяючи комп'ютерам краще розуміти та генерувати людську мову. У психології когнітивне моделювання застосовується для перевірки теорій про роботу мозку. Наприклад, моделі відновлення пам'яті дозволяють вивчати, як люди запам'ятовують інформацію, що може допомогти у лікуванні таких розладів, як хвороба Альцгеймера. В освіті моделі когнітивних процесів використовуються для розробки адаптивних навчальних програм, що підлаштовуються під особливості засвоєння інформації кожним курсантом.

На сучасному етапі міждисциплінарний феномен когнітивної науки дозволив швидко інтегрувати дані знання у всілякі галузі нашого суспільства, а розроблені методи адаптувати до досліджень у різні сфери діяльності, зокрема у системи інформаційної та кібербезпеки.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Когнітивні аспекти у сфері інформаційної та кібернетичної безпеки становлять великий інтерес серед науковців та практиків-фахівців. Більшість видів діяльності у складній динамічній системі тісно пов’язані з ризиком, що обумовлений невизначеністю умов та можливими помилковими рішеннями керуючих осіб. Когнітивне моделювання допомагає експерту проаналізувати ситуацію і розробити найбільш ефективну стратегію управління, спираючись не стільки на власну інтуїцію, скільки на впорядковане, структуроване і верифіковане знання про складну систему.

Аналіз наукових джерел дозволив виділити наступні когнітивні моделі, які застосовуються у системах безпеки: символічне моделювання (моделювання на основі правил); мережеве моделювання (моделювання з використанням нейронних мереж); баєсівські моделі (ймовірнісне моделювання); моделювання на основі агентів.

3.1 Символічне моделювання (моделювання на основі правил)

Цей метод передбачає прийняття рішень системою згідно з чітко сформульованими умовами типу "якщо-то", які відображають експертну логіку. У сфері кібербезпеки його застосовують для побудови систем виявлення вторгнень (IDS), що аналізують мережевий трафік на предмет відомих атак. Наприклад, правило "якщо IP-адреса надсилає понад 1000 запитів на один порт щосекунди — це DDoS-атака" є типовим. Такі системи добре справляються з виявленням уже відомих загроз, але не здатні розпізнавати нові або приховані атаки.

Це підтверджується у роботі [20]. Досліджуючи експертну систему на основі правил RBES, науковці здійснили порівняльний аналіз традиційних та гібридних методів виявлення загроз. RBES історично пропонували чіткі, керовані правилами методи для виявлення відомих загроз, але їхня статична природа ледве встигає за сучасним швидкозмінним кіберландшафтом, особливо проти експлойтів нульового дня та передових стійких загроз (APT). Щоб вирішити ці проблеми, дослідники все частіше звертаються до гібридних систем штучного інтелекту, які поєднують символічне мислення з машинним навчанням та глибоким навчанням. Це було підтверджено емпіричними даними.

3.2 Мережеве моделювання (моделювання з використанням нейронних мереж)

Цей підхід базується на принципах роботи людського мозку, де штучні "нейрони" формують мережу, здатну навчатися та розпізнавати складні закономірності. У

кібербезпеці нейронні мережі лежать в основі систем виявлення аномалій, які аналізують типову поведінку мережі (наприклад, обсяг трафіку, час активності) та фіксують відхилення, що можуть свідчити про нові, невідомі загрози. Це робить їх особливо корисними для виявлення атак нульового дня. Актуальність даної проблеми підтверджується великою кількістю наробок у цій сфері.

Дослідниками [21] було проаналізовано 80 статей щодо використання алгоритмів глибокого навчання для застосувань кібербезпеки, зокрема, згорткова нейронна мережа (CNN), автокодувальник (AE), глибока мережа довіри (DBN), рекурентна нейронна мережа (RNN), генеративно-змагальна мережа (GAN) та глибоке навчання з підкріпленням (DIL). Експериментальний аналіз довів, що дані моделі покращили точність, масштабованість, надійність програм кібербезпеки при застосуванні в режимі реального часу.

У статті [22] представлено і експериментально перевірено інноваційний алгоритм глибокого навчання, розроблений для ефективного виявлення потенційних загроз безпеці у великомасштабному мережевому трафіку. Алгоритм автоматизує навчання ознак через багаторівневу стратегію екстракції, поєднуючи базові, статистичні та поведінкові характеристики для ідентифікації коротко- та довготривалих закономірностей. Завдяки динамічному коригуванню ваги та інтеграції автокодерів і генеративно-змагальної мережі (GAN), він адаптується до мережевого середовища, виявляючи як відомі, так і невідомі загрози. Механізм уваги покращує інтерпретованість моделі, дозволяючи експертам розуміти її рішення.

3.3 Баєсівські моделі (ймовірнісне моделювання)

Цей метод використовує статистичні підходи для оцінки ймовірності виникнення певних подій. У контексті кібербезпеки він допомагає прогнозувати ризики та ймовірність успішного здійснення атаки на конкретну систему. Наприклад, модель може визначити, наскільки ймовірно, що фішинг-лист буде ефективним, враховуючи його тему, час надсилання та характеристики користувача.

Впровадження даного методу представлено у роботі [23]. Автори проаналізували баєсівські підходи, що використовуються для виявлення аномалій обсягу трафіку, мережевих аномалій та шкідливого програмного забезпечення, а також типові типи даних, що використовуються в кожному з них. Баєсівські моделі в кібербезпеці ефективно вирішують проблеми виявлення аномалій завдяки трьом ключовим причинам: вони успішно працюють з великими латентними змінними для виявлення прихованих структур у даних, забезпечують чітке ймовірнісне представлення невизначеності, що робить прогнози стабільнішими, та дозволяють інтегрувати різнорідну інформацію в єдину логічну структуру, зокрема через баєсівські мережі, для подолання дефіциту даних.

3.4 Моделювання на основі агентів

Цей підхід передбачає створення цифрових "агентів", які моделюють поведінку різних учасників — хакерів, користувачів, систем захисту. У кібербезпеці він використовується для симуляції кібератак і перевірки стійкості систем. Такі моделювання дозволяють дослідникам аналізувати взаємодію між атакуючими та захисниками, виявляючи потенційні уразливості ще до того, як ними скористаються реальні зловмисники.

Автори проєкту «Освоєння кіберпотужності: когнітивні науки та людський фактор у цивільній та військовій кібербезпеці» стверджують, що створення симуляцій та

експериментів на основі моделей когнітивних процесів дозволяє досліджувати сценарії кібератак та оцінювати ефективність захисних стратегій, підвищуючи рівень безпеки інформаційних систем [24, 25].

Когнітивний підхід є перспективним психологічним напрямом дослідження особливостей когнітивних процесів оператора кібербезпеки. На це вказують автори роботи [26], обґрунтувавши вимоги до професіоналізму та рівня інтелектуальної, когнітивної і наукової підготовки персоналу для різних рівнів ієрархії виробництва й управління та ступеня повноважень у прийнятті рішень. Для оперативного управління командою в АСУ-ТП, де кожен член є інтелектуальним агентом, інформація для прийняття рішень агрегується з мультимедійних щитів. Для кожного ієрархічного рівня інфраструктури розроблені методи оцінки ситуації для виявлення збоїв та атак, що дозволяє формувати адекватні способи протидії відповідно до типу загроз.

Агентно-орієнтовану модель системного моделювання для виявлення як явної, так і прихованої структури складних корпоративних систем та людської взаємодії з метою ідентифікації уразливостей описано у праці [27]. Модель фіксує емерджентну поведінку численних мережевих агентів, використовуючи ризик-орієнтований підхід для прогнозування атак, тоді як нейронна мережа класифікує типи атак на основі мережевого трафіку. Правила взаємодії самоорганізованої поведінки призначають захисні механізми, а ефективність оцінюється за діаграмами стану/часу та вартістю інцидентів, що інформує про необхідність удосконалення рішень безпеки.

Здійснено всебічний огляд засобів моделювання поведінки агентів в інформаційно-комунікаційних системах у роботі [28].

Автори дослідницького проєкту [29] продемонстрували агентно-орієнтовані моделі та сценарії для моделювання впливу довіри користувачів, витонченості зловмисників, навчання користувачів та системного захисту на кібербезпеку. Ці незалежні симуляції використовують програмні агенти, які припускають певні заздалегідь визначені атрибути для емуляції своїх фізичних аналогів у середовищі, що представляє кіберпростір.

У статті [30] представлена агентно-орієнтована структура моделювання, яка вирішує складність імітації людської сприйнятливості до фішингу, інтегруючи динамічні людські фактори, такі як риси особистості та історія навчання, для оцінки їхнього впливу на уразливість.

Слід відмітити, що сучасні когнітивні моделі носять гібридний характер, об’єднуючи різні методи когнітивізму для ефективної стратегії захисту.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Когнітивне моделювання розглядається як один із перспективних підходів у сфері кіберзахисту. Завдяки цьому методу можна створити глибоку модель безпекової системи, яка демонструє взаємозв’язки між її компонентами, їхній вплив один на одного та потенційні наслідки різних подій. Така модель дозволяє прогнозувати розвиток ситуацій і формувати дієві стратегії для запобігання загрозам та вирішення можливих проблем.

Когнітивна модель виступає як розумний асистент для фахівця, допомагаючи йому орієнтуватися в складному потоці інформації, встановлювати причинно-наслідкові зв’язки та приймати обґрунтовані рішення навіть за умов обмежених ресурсів і часу.

Разом з цим впровадження когнітивного моделювання у сферу безпеки має свої проблеми, пов’язані з потребою великих обсягів якісних даних про поведінку зловмисників, складність моделювання людської поведінки, етичні питання. Тому перспективним надалі є дослідження, які присвячені впровадженню гібридних моделей когнітивного напряму з інтеграцією штучного

інтелекту. Це дозволить перетворити кібербезпеку з реактивної оборони на інтелектуальну стратегічну гру.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
2. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
3. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N.V., & Skladannyi, P. M. (2023). Enterprise information and cyber security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
4. Bone, J. (2016). Cognitive Risk Framework for Cybersecurity: Bounded Rationality: Executive Summary: Part I. EDPACS, 54(5), 1–11. https://doi.org/10.1080/07366981.2016.1247564
5. Shevchenko S., Zhdanova Y., Shevchenko H., Nehodenko O., and Spasiteleva S. (2023) Information Security Risk Management using Cognitive Modeling Cybersecurity Providing in Information and Telecommunication Systems, V. 3550. c. 297-305. ISSN 1613-0073
6. Shevchenko S., Zhdanova Y., Kryvytska, O. Shevchenko, H. and Spasiteleva S. (2024) Fuzzy cognitive mapping as a scenario approach for information security risk analysis Cybersecurity Providing in Information and Telecommunication Systems II 2024, 3826. c. 356-362. ISSN 1613-0073
7. Шевченко, С., Жданова, Ю., Складанний, П., & Петренко, Т. (2024). Нечіткі когнітивні карти як інструмент візуалізації сценаріїв реагування на інциденти в системах безпеки. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2(26), 417–429. https://doi.org/10.28925/2663-4023.2024.26.707
8. Bone, James. (2016). Cognitive Risk Framework for Cybersecurity, Part II https://www.corporatecomplianceinsights.com/cognitive-risk-framework-cybersecurity-part-2/
9. Bone, James. (2024). Cognition in Cybersecurity Situational Awareness. Cognitive risk institute, 1(1) 10.13140/RG.2.2.23490.59842. https://www.researchgate.net/publication/379076804_Cognition_in_Cybersecurity_Situational_Awareness
10. Roberto, O Andrade, Sang Guun Yoo. (2019) Cognitive security: A comprehensive study of cognitive science in cybersecurity. Journal of Information Security and Applications 48. https://doi.org/10.1016/j.jisa.2019.06.008
11. Yuning Jiang, Yacine Atif, (2021) A selective ensemble model for cognitive cybersecurity analysis, Journal of Network and Computer Applications, Volume 193, 2021, https://doi.org/10.1016/j.jnca.2021.103210.
12. Онопрієнко, М.В. (2011) Феномен когнітивної науки і технології. Вісник Національного авіаційного університету. Філософія. Культурологія. 1, 68-72. http://nbuv.gov.ua/UJRN/Vnau_f_2011_1_18
13. Dictionary of Education Terms. https://minicoursegenerator.com/dictionary-of-education-terms/en/letter/a
14. Sun, R. The Cambridge Handbook of Computational Psychology. New York: Cambridge University Press, 2008. – 753 p
15. Мілявський, Ю. Л. Ідентифікація та керування складними системами на основі моделей імпульсних процесів когнітивних карт : дис. … д-ра техн. наук. : 01.05.04 Системний аналіз і теорія оптимальних рішень / Мілявський Юрій Леонідович. – Київ, 2019. – 297 с.
16. Sun, R., (2020). Cognitive Modeling, In P. Atkinson, S. Delamont, A. Cernat, J.W. Sakshaug, & R.A. Williams (Eds.), *SAGE Research Methods Foundations.* https://doi.org/10.4135/9781526421036869642
17. Frischkorn, G. T., & Schubert, A. L. (2018). Cognitive Models in Intelligence Research: Advantages and Recommendations for Their Application. *Journal of Intelligence*, *6*(3), 34. https://doi.org/10.3390/jintelligence6030034
18. Farrell, S., & Lewandowsky, S. (2018). *Computational modeling of cognition and behavior*. Cambridge University Press. https://doi.org/10.1017/CBO9781316272503
19. Kosko Bart. (1986) Fuzzy Cognitive Maps. International Journal of Man-Machine Studies. 24, 65–75. http://katedrawiss.uwm.edu.pl/sites/default/files/download/202006/kosko_fcm_fuzzy_cognitive_maps.pdf
20. Quffa, Abdallah & Abu-Naser, Samy. (2025). A Rule-Based Expert System for Cybersecurity Threat Detection: Evolution, Applications, and the Hybrid AI Paradigm. 10.13140/RG.2.2.21026.49606

21. Priyanka Dixit, Sanjay Silakari. Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review, *Computer Science Review*, Volume 39, 2021, https://doi.org/10.1016/j.cosrev.2020.100317
22. Chao, J., & Xie, T. (2024). Deep Learning-Based Network Security Threat Detection and Defense. *International Journal of Advanced Computer Science and Applications*
23. José A. Perusquía & Jim E. Griffin & Cristiano Villa. (2022) Bayesian Models Applied to Cyber Security Anomaly Detection Problems," International Statistical Review, International Statistical Institute, vol. 90(1), pages 78-99
24. Veksler, V. D., Buchler N., Hoffman B. E., Cassenti D. N., Sample C. & Sugrim S. (2018). Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users. Frontiers in Psychology 9. 10.3389/fpsyg.2018.00691
25. Veksler V. D., Buchler N., LaFleur C. G., Yu Michael S., Lebiere C., Gonzalez C. (2020) Cognitive Models in Cybersecurity: Learning From Expert Analysts and Predicting Attacker Behavior. *Frontiers in Psychology* Vol 11. URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2020.01049/full#B34
26. Sikora, L. S., Lysa, N. K., Pavluk, O. M., Sabat, V. I., & Fedevych, O. Yu. (2023). Information and logical-cognitive approaches to the formation of cybersecurity of ecotechnogenic infrastructures of the region taking into account the level of risks. Scientific Bulletin of UNFU, 33(1), 71–81. https://doi.org/10.36930/40330110
27. L. Ashiku and C. Dagli, "Agent Based Cybersecurity Model for Business Entity Risk Assessment," *2020 IEEE International Symposium on Systems Engineering (ISSE)*, Vienna, Austria, 2020, pp. 1-6, doi: 10.1109/ISSE49799.2020.9272234
28. 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. Збірник наукових праць.* 6. 63-70. 10.26906/SUNZ.2019.6.063
29. Francia III, G.A., Francia, X.P., Bridges, C. (2021). Agent-Based Modeling of Entity Behavior in Cybersecurity. In: Daimi, K., Peoples, C. (eds) Advances in Cybersecurity Management. Springer, Cham. https://doi.org/10.1007/978-3-030-71381-2_1
30. Jeongkeun Shin, Kathleen M. Carley, and L. Richard Carley. (2023). Integrating Human Factors into Agent-Based Simulation for Dynamic Phishing Susceptibility. In Social, Cultural, and Behavioral Modeling: 16th International Conference, SBP-BRiMS 2023, Pittsburgh, PA, USA, September 20–22, 2023, Proceedings. Springer-Verlag, Berlin, Heidelberg, 169–178. https://doi.org/10.1007/978-3-031-43129-6_17

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 1 (29), 2025
ISSN 2663 - 4023

Svitlana M. Shevchenko
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

Yuliia D. Zhdanova
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0002-9277-4972
y.zhdanova@kubg.edu.ua

Arina M. Harkushenko
Student of the Faculty of Information Technologies and Mathematics
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0009-0003-7568-7900
amharkushenko.fitm24m@kubg.edu.ua

COGNITIVE APPROACH IN INFORMATION AND CYBER SECURITY

Abstract. In the field of information and cybersecurity, one of the most important and critical challenges is the human factor, because no software or technical tool can fully compensate for the lack of awareness of information and cyber risks, appropriate behavior and a responsible attitude to information protection. The introduction of cognitive science theories into the field of cyber security will increase the level of effectiveness of protection strategies. Cognitive modeling contributes to the creation of mathematical models that simulate the processes of human thinking, decision-making and behavior, which brings the transition from reactive protection to a proactive approach. This article is devoted to the study of the implementation of the cognitive approach in security systems. Based on the analysis of scientific literature, the main definitions of cognitive science are highlighted, in particular, the concepts of cognitive modeling, cognitive analysis and synthesis, types of cognitive models, fuzzy cognitive map. The advantages of cognitive theories in various sectors of society are outlined. It has been proven that cognitive modeling can be applied in the field of cybersecurity to understand and predict the behavior of both attackers and protective systems. The following cognitive models in cyber systems are described: symbolic modeling (rule-based modeling) is used to build intrusion detection systems (IDS) that analyze network traffic for known attacks; network modeling (modeling using neural networks) includes anomaly detection systems that analyze typical network behavior; Bayesian models (probabilistic modeling) help predict risks and the probability of a successful attack on a specific system; agent-based modeling is used to simulate cyberattacks and test the resilience of systems. It was determined that the use of hybrid models that combine the above is effective. The challenges of implementing cognitive modeling in the security field are highlighted. These are the difficulties associated with the need for large volumes of qualitative data on the behavior of attackers, the complexity of modeling human behavior, and ethical issues. The results of the study can be used as educational material for students of the specialty F5 Cybersecurity and Information Protection.

Keywords: information security; cybersecurity; cognitive modeling; cognitive analysis; cognitive synthesis; fuzzy cognitive map; cognitive skills; information protection.

REFERENCES

1. Kostiuk, Yu. V., Skladannyi, P. M., Bebeshko, B. T., Khorolska, K. V., Rzaieva, S. L., & Vorokhob, M. V. (2025). Information and communication systems security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
2. Kostiuk, Yu. V., Skladannyi, P. M., Hulak, H. M., Bebeshko, B. T., Khorolska, K. V., & Rzaieva, S. L. (2025). Information security systems. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
3. Hulak, H. M., Zhyltsov, O. B., Kyrychok, R. V., Korshun, N.V., & Skladannyi, P. M. (2023). Enterprise information and cyber security. [Textbook] Kyiv: Borys Grinchenko Kyiv Metropolitan University.
4. Bone, J. (2016). Cognitive Risk Framework for Cybersecurity: Bounded Rationality: Executive Summary: Part I. EDPACS, 54(5), 1–11. https://doi.org/10.1080/07366981.2016.1247564
5. Shevchenko S., Zhdanova Y., Shevchenko H., Nehodenko O., and Spasiteleva S. (2023) Information Security Risk Management using Cognitive Modeling *Cybersecurity Providing in Information and Telecommunication Systems*, V. 3550. c. 297-305. ISSN 1613-0073
6. Shevchenko S., Zhdanova Y., Kryvytska, O. Shevchenko, H. and Spasiteleva S. (2024) Fuzzy cognitive mapping as a scenario approach for information security risk analysis *Cybersecurity Providing in Information and Telecommunication Systems II 2024*, 3826. c. 356-362. ISSN 1613-0073
7. Shevchenko S., Zhdanova Y., Skladannyi, P., & Petrenko, T. (2024). Fuzzy cognitive maps as a tool for visualizingincident response scenarios in security systems. *Cybersecurity: Education, Science, Technique*, 2(26), 417–429. https://doi.org/10.28925/2663-4023.2024.26.707
8. Bone, James. (2016). Cognitive Risk Framework for Cybersecurity, Part II https://www.corporatecomplianceinsights.com/cognitive-risk-framework-cybersecurity-part-2/
9. Bone, James. (2024). Cognition in Cybersecurity Situational Awareness. Cognitive risk institute, 1(1) 10.13140/RG.2.2.23490.59842. https://www.researchgate.net/publication/379076804_Cognition_in_Cybersecurity_Situational_Awareness
10. Roberto, O Andrade, Sang Guun Yoo. (2019) Cognitive security: A comprehensive study of cognitive science in cybersecurity. *Journal of Information Security and Applications* 48. https://doi.org/10.1016/j.jisa.2019.06.008
11. Yuning Jiang, Yacine Atif, (2021) A selective ensemble model for cognitive cybersecurity analysis, *Journal of Network and Computer Applications*, Volume 193. https://doi.org/10.1016/j.jnca.2021.103210.
12. Onopriyenko, M. (2011) The phenomenon of cognitive science and technology. *Proceedings of the State University "Kyiv Aviation Institute". Vol.: Philosophy. Cultural Studies: collection of scientific papers*. 1, 68-72. http://nbuv.gov.ua/UJRN/Vnau_f_2011_1_18
13. Dictionary of Education Terms. https://minicoursegenerator.com/dictionary-of-education-terms/en/letter/a
14. Sun, R. The Cambridge Handbook of Computational Psychology. New York: Cambridge University Press, 2008. – 753 p
15. Milyavsky, Yu. L. Identification and control of complex systems based on models of impulse processes of cognitive maps: dissertation … Dr. Tech. Sci.: 01.05.04 System analysis and theory of optimal solutions / Milyavsky Yuri Leonidovich. – Kyiv, 2019. – 297 p.
16. Sun, R., (2020). Cognitive Modeling, In P. Atkinson, S. Delamont, A. Cernat, J.W. Sakshaug, & R.A. Williams (Eds.), *SAGE Research Methods Foundations.* https://doi.org/10.4135/9781526421036869642
17. Frischkorn, G. T., & Schubert, A. L. (2018). Cognitive Models in Intelligence Research: Advantages and Recommendations for Their Application. *Journal of Intelligence*, *6*(3), 34. https://doi.org/10.3390/jintelligence6030034
18. Farrell, S., & Lewandowsky, S. (2018). *Computational modeling of cognition and behavior*. Cambridge University Press. https://doi.org/10.1017/CBO9781316272503
19. Kosko Bart. (1986) Fuzzy Cognitive Maps. International Journal of Man-Machine Studies. 24, 65–75. http://katedrawiss.uwm.edu.pl/sites/default/files/download/202006/kosko_fcm_fuzzy_cognitive_maps.pdf
20. Quffa, Abdallah & Abu-Naser, Samy. (2025). A Rule-Based Expert System for Cybersecurity Threat Detection: Evolution, Applications, and the Hybrid AI Paradigm. 10.13140/RG.2.2.21026.49606
21. Priyanka Dixit, Sanjay Silakari. Deep Learning Algorithms for Cybersecurity Applications: A Technological and Status Review, Computer Science Review, Volume 39, 2021, https://doi.org/10.1016/j.cosrev.2020.100317
22. Chao, J., & Xie, T. (2024). Deep Learning-Based Network Security Threat Detection and Defense. *International Journal of Advanced Computer Science and Applications*

23. José A. Perusquía & Jim E. Griffin & Cristiano Villa. (2022) Bayesian Models Applied to Cyber Security Anomaly Detection Problems, International Statistical Review, International Statistical Institute, vol. 90(1), pages 78-99
24. Veksler, V. D., Buchler N., Hoffman B. E., Cassenti D. N., Sample C. & Sugrim S. (2018). Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users. *Frontiers in Psychology* 9. 10.3389/fpsyg.2018.00691
25. Veksler V. D., Buchler N., LaFleur C. G., Yu Michael S., Lebiere C., Gonzalez C. (2020) Cognitive Models in Cybersecurity: Learning From Expert Analysts and Predicting Attacker Behavior. *Frontiers in Psychology* VOL 11. URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2020.01049/full#B34
26. Sikora, L. S., Lysa, N. K., Pavluk, O. M., Sabat, V. I., & Fedevych, O. Yu. (2023). Information and logical-cognitive approaches to the formation of cybersecurity of ecotechnogenic infrastructures of the region taking into account the level of risks. *Scientific Bulletin of UNFU*, 33(1), 71–81. https://doi.org/10.36930/40330110
27. L. Ashiku and C. Dagli, "Agent Based Cybersecurity Model for Business Entity Risk Assessment," *2020 IEEE International Symposium on Systems Engineering (ISSE)*, Vienna, Austria, 2020, pp. 1-6, doi: 10.1109/ISSE49799.2020.9272234
28. Milov, O. & Kostyak, M. & Milevskyi, Stanislav & Pogasiy, S. (2019). Tools for modeling agents' behavior in information and communication systems. *Control, navigation and communication systems. Collection of scientific papers*. 6. 63-70. 10.26906/SUNZ.2019.6.063
29. Francia III, G.A., Francia, X.P., Bridges, C. (2021). Agent-Based Modeling of Entity Behavior in Cybersecurity. In: Daimi, K., Peoples, C. (eds) Advances in Cybersecurity Management. Springer, Cham. https://doi.org/10.1007/978-3-030-71381-2_1
30. Jeongkeun Shin, Kathleen M. Carley, and L. Richard Carley. (2023). Integrating Human Factors into Agent-Based Simulation for Dynamic Phishing Susceptibility. In Social, Cultural, and Behavioral Modeling: 16th International Conference, SBP-BRiMS 2023, Pittsburgh, PA, USA, September 20–22, 2023, Proceedings. Springer-Verlag, Berlin, Heidelberg, 169–178. https://doi.org/10.1007/978-3-031-43129-6_17