DOI 10.31891/2307-5732-2024-339-4-44
УДК 004.7.056.5:004.94

ГУПАЛЕНКО ВОЛОДИМИР
Черкаський державно технологічний університет
e-mail: vovan4363@gmail.com
ТАЗЕТДІНОВ ВАЛЕРІЙ
Черкаський державно технологічний університет
https://orcid.org/0000-0002-1091-9075
e-mail: valeriy.tazetdinov@gmail.com

АНАЛІЗ ТА ДОСЛІДЖЕННЯ СИСТЕМ ЗАХИСТУ НА ОСНОВІ КОГНІТИВНОГО МОДЕЛЮВАННЯ ПРИ ПРОГНОЗУВАННІ ПОВЕДІНКИ ЗЛОВМИСНИКІВ

У статті обговорюється підхід до розробки широкомасштабних когнітивних кіберфізичних систем, що характеризуються високим рівнем структурної, функціональної та архітектурної динаміки. Основна ідея запропонованого підходу полягає у використанні декількох сучасних парадигм побудови кіберфізичних систем, таких як безперервна архітектура, гнучка архітектура, цифрові двійники та цифрові потоки. Запропоновано трирівневу модель когнітивної кіберфізичної системи.

Ключові слова: когнітивність, кіберфізичність, динамічні моделі, неперервна архітектура, цифровізація.

HUPALENKO VOLODYMYR, TAZETDINOV VALERIY
Cherkassy State Technological University

ANALYSIS AND RESEARCH OF SECURITY SYSTEMS BASED ON COGNITIVE MODELLING IN PREDICTING THE BEHAVIOUR OF INTRUDERS

Attention is drawn to the scientific interpretation of the terms "cognitive modeling", "cyberspace and cyber security" by both domestic and foreign researchers. The main threats and ways to solve the challenges we face when working with corporate and state networks in the field of practical cyber protection of Ukraine are considered. At the center of the question are scientific terms, possibilities and methods of protection of the latest technologies, which take into account various risks and possibilities of bypassing protection in cyberspace. Taking into account the dynamic events and challenges associated with the attack of the Russian Federation, it is necessary to look for new methods of protecting the sphere in cyberspace and digital systems of Ukraine to ensure the stable operation of the systems of state bodies and new companies of Ukraine even before the events take place in reality. The approach to the development of large-scale cognitive cyber-physical systems characterized by a high level of structural, functional and architectural dynamics is considered. The main idea of the proposed approach is to use several modern paradigms of building cyber-physical systems, such as continuous architecture, flexible architecture, digital twins and digital streams. A three-level model of the cognitive cyber-physical system is proposed. In order to ensure the necessary level of flexibility of the system, this possibility should be laid at earlier stages of the life cycle, that is, at the stage of development. At the upper level, the system is described in terms of a continuous architecture, at the middle level, the system is presented as a system with a flexible architecture, which is described as a multi-level relatively finite automaton, and at the lower level , structural-functional models are used to illustrate the system in operation. The article provides examples of the use of the proposed approach.

Keywords: cognition, cyberphysicality, dynamic models, continuous architecture, digitalization.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Однією з відмінних рис сучасного етапу розвитку суспільства є дуже швидкі зміни в житті людей і способах виробництва. Сучасні компанії та організації адаптують свою стратегію, бізнес-моделі, продукти та послуги, а також бізнес-процеси та інформаційні системи щоб підвищити рівень їх цифровізації за допомогою інтелектуальних сервісів та продуктів з цифровим вдосконаленням. Потенціал інтернету та пов'язаних з ним цифрових технологій, таких як розумні речі, штучний інтелект (ChatGPT та інші аналоги), аналіз даних, хмарні обчислення, мобільні системи та кіберфізичні системи, включає стратегічні фактори, що сприяють розвитку цифрових платформ з екосистемами інтелектуальних послуг для цифрових продуктів що швидко розвиваються. В даний час парадигма що широко використовується для побудови реальних систем. Можна визначити кіберфізичні системи як системи засновані на інтеграції сутностей різної фізичної природи, коли окремі підсистеми різної фізичної природи функціонують як єдине ціле.

Сьогодні ще однією цікавою темою для IT-розробників є когнітивні системи. В IT-індустрію поняття "когнітивність" прийшло з когнітивної психології, яка вивчає процеси, що відбуваються в мозку людини під час обробки інформації. Пізніше це поняття лягло в основу одного з напрямків штучного інтелекту, який займається розробкою штучних когнітивних систем з урахуванням досягнень нейрофізіології та когнітивної психології. Найпростішою когнітивною системою можна вважати систему, яка може мати певні знання про себе і зовнішній світ функціонування якої реалізується у вигляді досягнення цілей. Можна сказати, що когнітивна система повинна мати як мінімум модель себе і моделі зовнішнього світу, представлені у вигляді знань застосованих на практиці. Можна проаналізувати та застосувати підхід до когнітивних систем, які здатні сприймати інформацію про стан зовнішнього світу і власний стан, працюючи з моделлю себе і моделлю зовнішнього світу, а також системи, які не використовують ці моделі можна визначити як інтелектуальні системи.

Однією з головних відмінних рис сучасних систем підтримки прийняття рішень (СППР) є варіативність їх структури та поведінки. Таким чином можна сказати, що сучасні системи можуть мати

здатність до еволюції тобто їх можна розглядати як системи, що розвиваються і яким притаманні такі характерні риси як і спонтанна зміна стану системи та протидія на вплив середовища що призводить до зміни його початкового стану і перманентні зміни в структурі та поведінці системи. Якщо система, що розвивається та еволюціонує за рахунок власних ресурсів, то такі системи називаються саморозвиваючими.

Практично всі когнітивні СППР, що саморозвиваються є інтенсивні програмні системи (Software Intensive Systems, скорочено SWIS), які використовують механізми роботи з інтелектуальними базами.

Аналіз досліджень та публікацій

Концептуальна модель когнітивних кіберфізичних систем складається з п'яти рівнів: фізичного, мережевого, зберігання, обробки та аналітики даних прикладного рівня. Масштабні кіберфізичних системи найчастіше реалізуються на платформах або системах хмарних та периферійних обчислень.

Основна тенденція еволюції кіберфізичних систем пов'язана з постійним ускладненням реалізованого функціоналу і на сьогоднішній день багато сучасних кіберфізичних моделей можна розглядати як системи аналізу навколишнього середовища. Значну частину сучасних СППР можна віднести і до когнітивних систем.

Стосовно IT-сфери термін "когнітивність" найчастіше асоціюється з похідними поняттями когнітивного моделювання, когнітивних систем та когнітивних архітектур, а також систем, що реалізують когнітивну поведінку.

Когнітивне моделювання можна визначити як процес підтримки прийняття рішень з урахуванням взаємного впливу різних подій і взаємозв'язку між ними. Когнітивний аналіз, використовуючи апарат когнітивних моделей і технологій дозволяє оперативно вирішувати такі завдання, як побудова моделі ситуації, оцінка впливу зовнішніх і внутрішніх факторів на можливі сценарії розвитку ситуації та виявлення тенденцій розвитку ситуацій. Технологія когнітивного моделювання зазвичай використовується для вирішення управлінських завдань в умовах непередбачуваних обставин.

Класичні системи з когнітивною архітектурою використовують евристичні алгоритми, натхненні людиною, які знаходять психологи та біологи, що часто входять до складу команди розробників. Історія створення такого роду когнітивних систем налічує щонайменше 40 років. Здебільшого це експериментальні системи. При їх побудові найчастіше використовуються такі поняття, як патерни ситуацій та ф'южн. Здебільшого це також системи підтримки прийняття рішень. Як приклад використання цього підходу можна розглянути концепцію когнітивних інтернет речей (Cognitive Internet of Things).

Основна ідея цієї парадигми полягає в тому, що сучасні інтернет речі – це просто сукупність найрізноманітніших пристроїв, оснащених датчиками стану та виконавчими механізмами. Для управління та підтримки такої складної інфраструктури в належному стані необхідно наділити її інтелектом, тобто здатністю сприймати інформацію про власний стан і при необхідності видавати керуючі дії з метою реконфігурації структури. Когнітивною системою тут виступає система управління інтернет речами за допомогою хмарних обчислень, яка може бути побудована як розподілена інтелектуальна система. В рамках цієї парадигми не дається ніяких конкретних рішень визначається лише те що потрібно робити, але не те як повинні бути реалізовані механізми пізнання та аналізу.

Формулювання цілей статті

Значна частина сучасних когнітивних СППР, що саморозвиваються є великими та складними розподіленими системами з високим рівнем не тільки структурної та функціональної, але й архітектурної варіативності. Однією з ключових проблем пов'язаних з побудовою когнітивних СППР що саморозвиваються, є проблема забезпечення їх керованості на всіх рівнях. Вирішення цієї проблеми в свою чергу вимагає наявності достатньої інформації про поточний стан системи, яка зазвичай представляється у вигляді набору моделей.

Проектування когнітивних СППР що саморозвиваються також є досить складною проблемою. Дуже часто використання традиційних підходів до проектування СППР не дає бажаних результатів. Тож потрібна розробка нових підходів до проектування когнітивних СППР що саморозвиваються.

Виклад основного матеріалу

Основна ідея запропонованого підходу полягає в тому, що пропонується використовувати декілька сучасних парадигм для побудови когнітивних моделей на основі кіберфізичних систем, таких як безперервна архітектура, гнучка архітектура, цифрові двійники та цифрові потоки. Запропонований підхід можна розглядати як адаптацію парадигми цифрових потоків до когнітивних моделей.

Реалізація передбачається на основі модельного підходу і передбачає використання трирівневої моделі життєвого циклу кіберфізичних систем.

Трирівнева модель когнітивної моделі що може саморозвиватись. Для того щоб забезпечити необхідний рівень таких можливостей когнітивних моделей як гнучкість, ця можливість повинна бути закладена на більш ранніх етапах когнітивних систем, а саме на етапі розробки. Ця модель може бути використана як основа точки зору на розробку або інкапсульована в окрему архітектурну точку бачення.

Запропонована модель описує безперервну гнучку архітектуру на всіх п'яти стадіях когнітивних моделей на трьох рівнях. Структура моделі показана на рисунку 1.

Рис. 1. Трирівнева модель

На верхньому рівні когнітивних моделей (Continuous agile architecture) описуються в термінах безперервної архітектури.

На середньому рівні (Agile architecture) система представлена у вигляді гнучкої архітектури та описує як багаторівневу відносно скінченну автоматичну систему.

На нижньому рівні (Runtime agile architecture) використовуються структурно-функціональні моделі, що описують систему в процесі функціонування.

Ці моделі описують кіберфізичні системи на різних етапах життєвого циклу. Верхній рівень описує всі етапи. Середній рівень стосується переважно етапів експлуатації та модернізації. Нижній рівень стосується переважно етапу експлуатації.

На наступному рівні описується процес трансформації архітектурних можливостей когнітивних систем під час переходу між окремими стадіями життєвого циклу (рисунок 2).

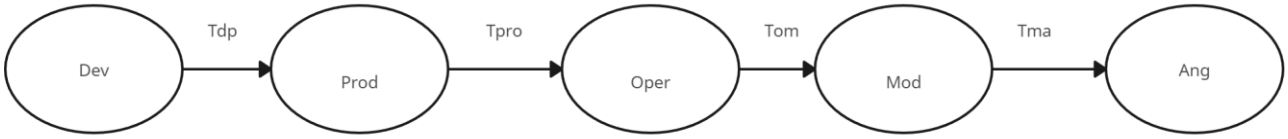

Рис. 2. Трансформація артефактів

Загалом можна виділити п'ять фаз життєвого циклу: Розробка (Dev), Виробництво (Prod), Експлуатація (Oper), Модернізація (Mod) та Знищення (Ang). Ланцюжок перетворень можна представити так:

Art Dev--> Tdp_--> Art Prod--> Tpo--> Art Oper--> Tmo--> Art Mod--> Tma-->--> Tmo--> Art Ang.

На кожній фазі життєвого циклу формується певний набір артефактів (Art). Артефакти можуть належати до наступних класів:

Класи Артів: = <Модель|Код|Фізичний об'єкт>. Кожна з фаз використовує свій власний набір артефактів.

Можна виділити чотири основні типи цифрових перетворень:

M--> M-1, M--> Code, M--> PhE, M1--> M2, де M - моделі, а PhE - фізичні об'єкти.

Загалом на кожному етапі життєвого циклу систем використовується свій набір властивостей, які пов'язані між собою механізмами трансформації.

На верхньому рівні можна говорити про одну модель. На середньому рівні кожна фаза використовує власні артефакти. Кожна фаза використовує власні гнучкі архітектури (AA). Кожній з архітектур AA відповідає набір архітектур часу виконання (RTAA).

Кожна фаза використовує власні системи артефактів, але також можна виділити деякі спільні риси.

Артефакти класифікація яких показана на рисунку 3, можна розділити на три групи: сутності, моделі та метрики.

Сутності можуть бути фізичними або віртуальними. Фізичні сутності можуть бути як фізичними елементами так і їх фізичними моделями. Віртуальними ж можуть бути як елементи кіберфізичних систем, так і їх моделі. Віртуальна сутність може виступати як код або як аналітичний процес.

Ця модель може бути використана як на етапі експлуатації так і на етапі модернізації.

У першому випадку мова йде про підтримку механізмів маневреності в режимі виконання, а в другому про підтримку цих механізмів в процесі модернізації.

Низький рівень. На низькому рівні підтримуються механізми структурно-функціонального майнінгу, тобто відстеження поточного структурно-функціонального стану спостережуваної когнітивної моделі.

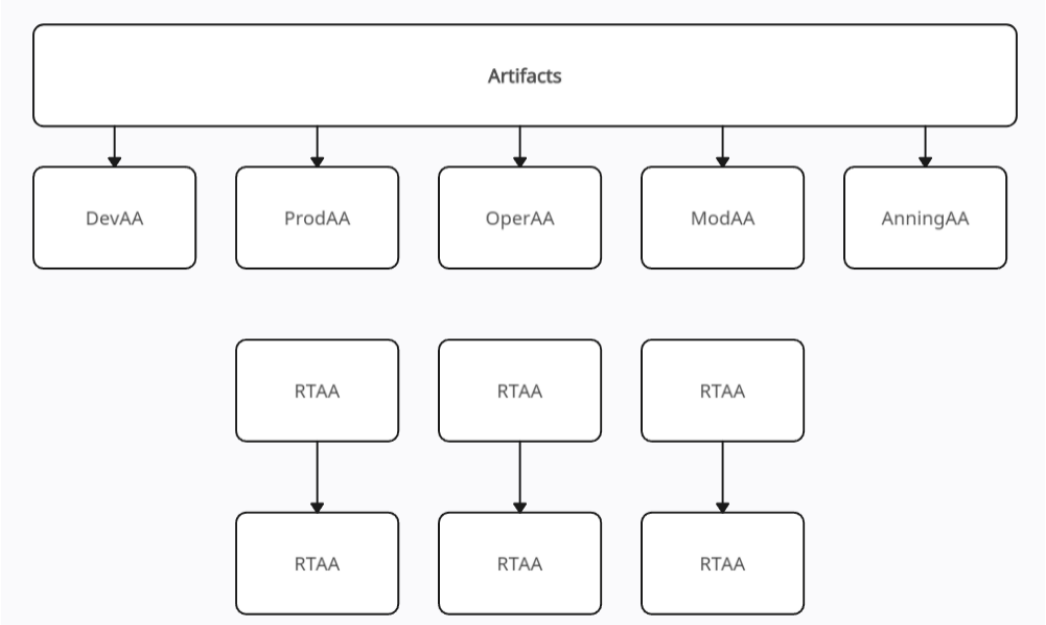

Рис. 3. Структура системи артефактів

Архітектурний стан спостережуваної когнітивної моделі може бути описаний за допомогою різних моделей в залежності від поставлених цілей.

Реалізація когнітивних СППР що самоорганізуються та розвиваються на платформах хмарних та периферійних обчислень пов'язана з вирішенням низки проблем, центральними з яких є те що когнітивні СППР мають бути орієнтовані на роботу зі знаннями, однак робота з антологіями та графами знань потребує достатньо потужних обчислювальних ресурсів які не завжди доступні навіть на хманному рівні, а тому дійсно повномасштабна підтримка механізмів роботи зі знаннями може бути організована лише на ньому.

Функції пов'язані з управлінням повільними аналітичними процесами, такі як управління самоорганізацією, можуть бути реалізовані в переважно в хмарному середовищі, нейронних мережах і алгоритмах когнітивного навчання які можуть бути використані для реалізації функцій з більш високими вимогами до продуктивності.

Практичне застосування

Запропонований підхід може бути використаний при побудові низки реальних систем. Слід зазначити, що для вирішення реальних задач не було би необхідності використовувати його в повному обсязі.

Нижче наведено короткий опис можливих реальних проектів в яких можна буде використати запропонований підхід.

Приклад 1. Метою розробки була модернізація виробничої системи з мобільними об'єктами на інтелектуальному рівні побудованій на платформі розумних речей. У цьому проекті є дві ключові підзадачі: збір даних на аналітичному рівні в умовах дуже високого рівня електромагнітних завад і завдання побудови корпоративного графіку. Ця система орієнтована в основному на роботу в режимі виконання і використовує структурні та функціональні моделі, що працюють на низькому рівні. Використання моделей верхнього рівня дозволяє підвищити гнучкість і спростити процес інтеграції в корпоративну інформаційну систему. Наявність динамічної моделі, що ілюструє виробничу систему відкриває можливості для побудови когнітивних виробничих систем. Цей приклад можна розглядати як використання запропонованого підходу для побудови динамічних цифрових двійників.

Приклад 2. У третьому випадку модельний підхід було використано для розв'язання задачі побудови навчального плану освітньої траєкторії початкового рівня в **IT**-домені. Це задача синтезу на основі моделі бізнес-процесів. Ця задача цікава ще й тим, що освітні системи можна розглядати як один з різновидів соціально-кібернетичних систем де потрібно працювати з моделями компетенцій. Це вказує на можливість, з певними можливостями, пов'язаними з адаптацією моделі використання даного підходу для вирішення задач.

Приклад 3. Математичний розрахунок для захисту систем на основі когнітивного моделювання за допомогою математичної моделі Байєса. Для забезпечення захисту інформаційних систем за допомогою когнітивного моделювання важливо застосовувати математичні методи для аналізу поведінки користувачів і виявлення аномалій. У цьому прикладі буде представлено математичну модель, що використовує байєсове оцінювання для виявлення аномальних дій.

Модель байєсового оцінювання

Байєсова теорема дозволяє оновлювати ймовірність гіпотези на основі нових даних. Для виявлення аномалій в поведінці користувачів ми будемо використовувати наступні позначення:

- H - гіпотеза, що користувач здійснює аномальну дію.
- E - спостережувані дані (дії користувача).
- P(H) - апостеріорна ймовірність гіпотези H.
- P(E|H) - ймовірність отримати дані E, якщо гіпотеза H істинна.
- P(E|¬H) - ймовірність отримати дані E, якщо гіпотеза H хибна.
- P(¬H) - ймовірність того, що гіпотеза H хибна.

Згідно з теоремою Байєса:

$$P(H \mid E) = \frac{P(\text{EH}) \cdot P(H)}{P(E)}$$

де $P(E) = P(E \mid H) \cdot P(H) + P(E \mid \neg H) \cdot P(\neg H)$.

Приклад застосування моделі

Розглянемо систему, в якій ми аналізуємо поведінку користувача для виявлення аномалій на основі логів доступу до системи. Нехай імовірність аномальної дії P(H)=0.01, ймовірність отримати дані E при наявності аномальної дії P(E|H)=0.8, і ймовірність отримати дані E при відсутності аномальної дії P(E|¬H)=0.1.

Тоді апостеріорна ймовірність P(H|E) обчислюється наступним чином:

1. Обчислимо P(E):

$$P(E) = P(E \mid H) \cdot P(H) + P(E \mid \neg H) \cdot P(\neg H)$$
$$P(E) = 0.8 \cdot 0.01 + 0.1 \cdot 0.99$$
$$P(E) = 0.008 + 0.099$$
$$P(E) = 0.107$$

2. Обчислимо апостеріорну ймовірність P(H|E):

$$P(H \mid E) = \frac{P(EH) \cdot P(H)}{P(E)}$$
$$P(H \mid E) = \frac{0.8 \cdot 0.01}{0.107}$$
$$P(H \mid E) \approx \frac{0.008}{0.107}$$
$$P(H \mid E) \approx 0.0748$$

Таким чином, апостеріорна ймовірність того, що користувач здійснює аномальну дію становить приблизно 7.48%.

Інтерпретація результатів

Отримане значення P(H|E)≈0.0748 означає, що при спостереженні даних E ймовірність того, що користувач здійснює аномальну дію, становить приблизно 7.48%. Це значення вище початкової ймовірності 1%, що вказує на підвищену загрозу, яку необхідно досліджувати детальніше.

Використання байєсового оцінювання дозволяє ефективно аналізувати дані про поведінку користувачів та виявляти аномалії. Цей підхід є важливим елементом когнітивного моделювання, що сприяє підвищенню рівня кібербезпеки інформаційних систем. Для досягнення більш високої точності необхідно використовувати додаткові дані та удосконалювати моделі, враховуючи специфіку конкретних інформаційних систем і загроз.

Цей математичний розрахунок демонструє застосування теореми **Байєса** для аналізу поведінки користувачів у контексті кібербезпеки, що дозволяє виявляти потенційні загрози і оперативно реагувати на них.

Висновки з даного дослідження
і перспективи подальших розвідок у даному напрямі

Описаний вище підхід можна розглядати перш за все, як підхід до розробки великомасштабних когнітивних гетерогенних СППР з високим рівнем структурної функціональної та архітектурної динаміки побудованих на платформах хмарних обчислень. Ключова ідея розробленого підходу полягає у використанні систем динамічних моделей СППР яка може підтримуватись в актуальному стані протягом усього життєвого циклу системи.

Реалізація запропонованого підходу дозволяє вирішити ряд важливих завдань, таких як підвищення рівня інтелектуальності СППР та підвищення рівня доступності сервісів і вийти на новий рівень складності створюваної СППР. Наявність модельних знань про минулі стани системи дозволяє визначати першопричини подій та прогнозувати майбутні стани системи для реалізації про активного управління. Крім того, наявність знань про минулі стани дозволяє використовувати механізми навчання.

Наразі робота над подальшим розвитком запропонованого підходу ведеться у трьох напрямках: створення нових моделей, розширення сфери застосування підходу зокрема для аналізу соціальних мереж, та розробка нових алгоритмів синтезу моделей та перетворень існуючих моделей.

Література

1. В. Мохор, В. Цуркан, and О. Крук, “Функціональне моделювання системи керування ризиком безпеки інформації,” Захист інформації, vol. 18, no. 1, pp. 74–80, 2016.

2. Л. О. Нікіфорова, А. А. Шиян, and Ю. Яремчук, “Моделювання вибору оптимального методу протидії загрозам інформаційній безпеці,” Реєстрація, зберігання і обробка даних, vol. 16, no. 4, pp. 28–33, 2014.

3. В. Хорошко and М. Прокофьєв, “Проблеми захисту інформації в Україні,” Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, vol. 2, no. 30, pp. 9–14, 2015.

4. В. Ю. Степанов, “Інформаційна безпека як складова державної інформаційної політики,” Державне будівництво, no. 2, pp. 1–9, 2016.

5. О. М. Хошаба, “Частина 13. Захист інформації в системах електронного урядування,” in Електронне урядування та електронна демократія: навч. посібник, К: ФОП Москаленко О.М., 2017, p. 72.

6. О. М. Маковецький, “Підходи до удосконалення методики оцінки ефективності комплексної системи захисту інформації,” Сучасні інформаційні технології у сфері безпеки та оборони, vol. 2, no. 26, pp. 54– 58, 2016.

7. Ю. М. Щебланін and А. О. Гресько, “Загальний, комплексний опис проблем інформаційної безпеки в ‘Інтернеті речей,’” Сучасний захист інформації, no. 1, pp. 69–73, 2016.

8. К. М. Носенко, Т. А. Ліхоузова, and О. І. Півторак, “Огляд систем виявлення атак в мережевому трафіку,” Міжвідомчий науково-технічний збірник “Адаптивні системи автоматичного управління,” vol. 1, no. 24, pp. 67–75, 2014.

9. Кібербербезпека і національна безпека / за ред. Франкліна Д. Крамера, Стюарта Х. Старра, Ларрі Венца. Cyberpower and National Security / ed.by Franklin D.Kramer, Stuart H.Starr, Larry Wentz. Washington, D.C.: Potomac Books,2009..

10. Information systems defence and security: France's strategy. French Network and Information Security Agency. 2011.

11. Національна військова стратегія операцій у кіберпросторі. National Military Strategy for Cyberspace Operations. http://www.dod.gov/pubs/foi/ ojcs/07-F-2105doc1 .paf

12. Баранов О. Про тлумачення та визначення поняття «кібербезпека». Інформація і право.

13. 2014. С. 54-62.

14. Національна бібліотека України імені В. І. Вернадського. www.nbuv.gov.ua.

15. «Когнітивне моделювання для оцінки безпеки мережі: Огляд» (2018). https://www.researchgate.net/publication/325160821.

16. Захист та безпека інформаційних систем: Стратегія Франції. Французьке агентство мережевої та інформаційної безпеки агентство мережевої та інформаційної безпеки Франції. 2011. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/France_2011_2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf

References

1. V. Mokhor, V. Tsurkan and O. Kruk Functional modeling of the information security risk management system. Protection of information. 18, issue 1, p. 74–80, 2016.

2. L. O. Nikiforova, A. A. Shiyan, Yu. Yaremchuk Modeling the choice of the optimal method of countering threats to information security. Registration, storage and processing of data. 16, issue 2014. No. 4. P. 28–33.

3. V. Khoroshko and M. Prokofiev, "Problems of information protection in Ukraine", Legal, regulatory and metrological support of the information protection system in Ukraine, Vol. 2, No. 30, pp. 9–14, 2015.

4. V. Yu. Stepanov Information security as a component of state information policy. State construction. 2016. No. 2. P. 1–9.

5. O. M. Khoshaba Part 13. Information protection in electronic government systems. Electronic government and electronic democracy: training. manual, K: FOP Moskalenko O.M., 2017, p. 72.

6. O. M. Makovetskyi, P. Approaches to improving the methodology for evaluating the effectiveness of a complex information protection system. Modern information technologies in the sphere of security and defense. 2, No. 26, pp. 54–58, 2016.

7. Yu. M. Shcheblanin and A. O. Gresko, "General, comprehensive description of information security problems in the 'Internet of Things'", Modern information protection, No. 1, pp. 69–73, 2016.

8. K. M. Nosenko, T. A. Likhouzova, and O. I. Pivtorak, "Overview of a systemic attack in network traffic", Interagency Scientific and Technical Collection "Adaptive Automatic Control Systems", vol. 1, No. 24, p. 67–75, 2014.

9. Cyber power and national security / edited by Franklin D. Kramer, Stuart H. Starr, Larry Wentz. – Cyberpower and National Security / ed. by Franklin D. Kramer, Stuart H. Starr, Larry Wentz. Washington, D.C.: Potomac Books, 2009.

10. Protection and security of information systems: France's strategy. French network and information security Agency. 2011.

11. National military strategy for operations in cyberspace. National Military Strategy for Cyberspace Operations. http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.paf

12. Baranov O. On the interpretation and definition of the concept of "cyber security". Information and law. 2014. P. 54-62.

13. National Library of Ukraine named after V. I. Vernadskyi. www.nbuv.gov.ua.

14. Cognitive Modeling for Network Security Assessment: An Overview (2018). https://www.researchgate.net/publication/325160821.

15. Protection and security of information systems: A French strategy. French Agency for Network and Information Security Agency for Network and Information Security of France. 2011. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/France_2011_2011-02-15_Information_system_defence_and_security_-_France_s_strategy.pdf.