КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue
DOI 10.28925/2663-4023.2025.30.973
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

Спасітєлєва Світлана Олексіївна
кандидат фізико-математичних наук, доцент,
доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський столичний університет імені Бориса Грінченка, Київ, Україна
ORCID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua

МОДЕЛЬ ФОРМУВАННЯ КОГНІТИВНИХ НАВИЧОК СПЕЦІАЛІСТІВ З КІБЕРБЕЗПЕКИ

Анотація. Дана стаття присвячена розробці та теоретичному обґрунтуванні методики формування когнітивних навичок у спеціалістів з інформаційної та кібернетичної безпеки, впровадження якої дозволить удосконалити професійну підготовку спеціалістів та сприятиме підвищенню мотивації у навчальному процесі. Актуальність проблеми підготовки висококваліфікованих спеціалістів з кібербезпеки зумовлено стрімким зростання кіберзагроз, що вимагає не лише технічних знань людини, але й розвинених когнітивних навичок (критичного мислення, здатності до швидкого прийняття рішень, розпізнавання патернів та стійкості до стресу). Шляхом аналізу психологічної та методичної літератури деталізовано суть та структуру поняття «когнітивні навички», які є критичними для спеціалістів з інформаційної та кібербезпеки. На основі проблемно-діяльнісного та особистісно орієнтованого підходів розроблено модель формування когнітивних навичок спеціалістів з кібербезпеки, основними етапами якої є діагностичний, формувальний та контрольно-коригуючий. Спираючись на принципи системності та професійної спрямованості визначено формувальний блок, що містить змістову та діяльнісну складову. Змістова частина методики охоплює науково-методичне забезпечення дисциплін спеціальності F5, програмне забезпечення для навчальних активностей та спеціалізовані тести з психології. Діяльнісна частина моделі забезпечується тренінгами, симуляційними вправами такими як імітація кібератак в середовищі кіберполігону, ігровими методами (зловмисник – спеціалістів з безпеки) та когнітивними тренажерами спрямованими на розвиток уваги, пам’яті, швидкості обробки інформації. Окреслено педагогічні умови для ефективної реалізації даної методики, зокрема, готовність та кваліфікація викладачів і технічне забезпечення. Результати дослідження можуть бути використані закладами вищої освіти та навчальними центрами для модернізації навчальних програм та підвищення якості підготовки фахівців у сфері інформаційної безпеки.

Ключові слова: інформаційна безпека; кібербезпека; когнітивні навички; захист інформації; модель формування когнітивних навичок.

ВСТУП

Постановка проблеми. Кіберпростір науковці розглядають як складну адаптивну соціально-технічну систему, функціональна архітектура якої формується динамічно через взаємодію трьох ключових складників: людей, технологій та процесів. Нелінійна природа цих взаємодій породжує високий рівень невизначеності та ризиків. Ефективне розуміння, моделювання та управління кіберпростором вимагає міждисциплінарного підходу та інтеграцію знань не лише технічних наук для розробки засобів захисту інформації, а й соціальних наук для аналізу людського фактора, мотивації зловмисників та формування політик безпеки [1].

Сучасний ландшафт кібербезпеки характеризується ескалацією атак, які використовують генеративний штучний інтелект для створення правдоподібних глибоких фейків (*deepfakes*) та іншого синтетичного медіаконтенту. Це призводить до формування нового, критичного вектора когнітивної атаки, спрямованого на експлуатацію фундаментальних обмежень людських когнітивних функцій, зокрема: сприйняття (здатність відрізняти реальне від синтетичного); уваги (перевантаження сенсорною інформацією); критичного мислення та прийняття рішень (обхід евристичних фільтрів) [2].

З огляду на непередбачувану природу поведінки та рішень суб’єктів, людина є вирішальним чинником, який встановлює або обмежує рівень інформаційної та кібербезпеки. Такі фактори, як когнітивні упередження, методи соціальної інженерії та індивідуальні процеси прийняття рішень, суттєво впливають на безпековий стан системи [3].

Таким чином, дослідження нейрокогнітивних основ кіберстійкості та розробка ефективних когнітивних контрзаходів (наприклад, спеціалізованих тренінгів та ергономічних інтерфейсів) стають імперативом для мінімізації вразливості «людського актора» в умовах зростаючої гіперреалістичної соціальної інженерії.

Аналіз останніх досліджень і публікацій. Потреба у висококваліфікованих експертах з питань безпеки зростає експоненціально разом з неперервним потоком нових, складніших та поширеніших кіберзагроз. Цим фахівцям необхідно не просто відповідати актуальним викликам, а постійно їх випереджати та прогнозувати. Оволодіння передовими навичками є основою захисту інформаційного та кіберпростору.

Про важливу роль формування та розвиток когнітивних навичок спеціалістів з кібербезпеки підкреслено в роботах [1–13].

У статті [4] представлена когнітивна модель безпеки, призначена для прискорення та підвищення ефективності кібероперацій. Вона досягає цього, поєднуючи технології Big Data, ML, системи підтримки рішень з мисленням аналітика. Таке поєднання дозволяє швидше генерувати знання та реагувати на загрози, автоматизуючи рутинні когнітивні процеси. Однак, використовуючи механізми MAPE-K, OODA та "Human in the Loop", модель зберігає аналітика як головного відповідального за перевірку та прийняття ключових рішень. Основна мета розробників — комплексно підтримувати ситуаційну обізнаність у сфері кібербезпеки за допомогою інтеграції когнітивних теорій.

Розробники у дослідженні [5] створили когнітивну структуру, що покращує сприйняття та розуміння результатів моделей аналізу уразливостей на основі штучного інтелекту. Їх методика працює в три етапи: спочатку система збирає та категоризує різнорідні дані у локальну базу; надалі за допомогою штучного інтелекту система автоматично генерує шаблони загроз, уразливостей та атак, а також проводить первинну оцінку ризику; на третьому етапі експерти з безпеки оцінюють та верифікують

результати, а їхній зворотний зв'язок потім використовується для офлайн-навчання моделі, що дозволяє постійно підвищувати її точність.

Нам імпонує дослідження [6], в якому підкреслюється, що кібероператорам потрібен різноманітний набір компетенцій, які виходять за рамки технічних навичок. Їх експеримент у навчальному середовищі щодо взаємозв'язку саморегуляції людини та продуктивності в кібероперацiях доводить необхідність зосередитися на розвитку м'яких навичок спеціалістів з кібербезпеки.

Беручи до уваги той факт, що навчання та адаптація спеціалістів з кіберзахисту стають критично важливими і їх перепідготовка має бути протягом усієї кар'єри, дослідники [7] запропонували когнітивну модель у вигляді адаптивного програмного забезпечення для навчання з метою посилити навички, необхідні для таких спеціалістів.

Науковці вивчають та експериментують з різними технологіями та засобами для ефективного формування та розвитку когнітивних навичок людини. Сучасність характеризується широким впровадженням у систему освіти методів штучного інтелекту. У зв'язку з цим вченими [8] було проведено дослідження щодо впливу генеративного штучного інтелекту на формування трьох ключових когнітивних навичок для прийняття рішень, а саме: аналітичного, творчого та системного мислення. У результаті було доведено, що штучний інтелект підсилює здібності людини у сфері структурування та логіки, але водночас може послаблювати креативність, критичність та здатність до широкої міждисциплінарної інтеграції.

Таким чином, аналіз наукової літератури засвідчує, що проблему розвитку когнітивних навичок спеціалістів інформаційної та кібербезпеки досліджено науковцями на різних рівнях, тому наше дослідження певною мірою доповнює й розширює попередні наукові розвідки.

Мета статті. Метою статті є розробка та наукове обґрунтування методики формування ключових когнітивних навичок спеціалістів з інформаційної та кібербезпеки, необхідних для ефективного виявлення, аналізу та реагування на інциденти кібербезпеки.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Когнітивні навички – це розумові здібності людини для обробки інформації. До когнітивних здібностей належать: увага, уява, пам'ять, виконавчі функції, аналітичне та творче мислення, здатність до прийняття рішень та саморегуляція [14-15]. Формування навичок залежить від низки емпіричних факторів, які можна поділити на три основні групи [16]:

1. Процесуальні чинники: мотивація, попередня навченість, прогрес засвоєння, вправа, підкріплення та метод навчання (цілісне чи по частинах).
2. Фактори усвідомлення змісту: визначають, як суб'єкт розуміє суть дії (операції).
3. Чинники оволодіння: контролюють якість засвоєння дії, включаючи повноту її з'ясування та поетапний перехід до вищих рівнів автоматизованості, інтеріоризованості та швидкості.

Комбінація цих факторів створює унікальну траєкторію формування навички, яка може мати різну динаміку: швидке навчання на старті з подальшим уповільненням, зворотний сценарій або їхні змішані форми.

Виділяють когнітивні та метакогнітивні навички [17].

Когнітивні навички функціонують не ізольовано, вони тісно переплітаються із спеціальними та емоційними навичками [18-19].

Слід відмітити, що когнітивні здібності людини дано від природи, тому їх розвиток підтримувати доцільно протягом життя [20]. Студентський вік є найкращим для активного і ефективного їх удосконалення при умові створення спеціального навчання.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Пошук інформації та аналіз зарубіжних і українських вчених свідчать про те, що когнітивні аспекти у сфері інформаційної та кібернетичної безпеки становлять великий інтерес серед науковців та практиків-фахівців, представлено у дослідженнях [21-23]. Робота спеціаліста з кібербезпеки є дуже напруженою, оскільки вимагає швидкого прийняття численних критичних рішень на основі складних та високошвидкісних інформаційних потоків, що потребує високого рівня когнітивних навичок. Індивідуальні когнітивні відмінності суттєво впливають на успіх у кіберзахисті [9], існує нагальна потреба з'ясувати, які саме когнітивні функції є найбільш визначальними для високої продуктивності в цій галузі.

Когнітивні навички спеціалістів з кібербезпеки

Когнітивним вважається пізнавальний процес, під час якого відбувається обробка свідомістю інформації, що надходить, її уявним перетворенням у знання, зберігання й використання накопиченого досвіду в повсякденному житті [18]. Когнітивні здібності є сильними предикатом відбору та продуктивності роботи співробітників кіберзахисту [10]. Це підтверджується науковцями [11], які провели аналіз повідомлень про роботу, і на основі цього визначили найбільш затребувані навички та зв’язок між ними та кіберролями. Продовження досліджень у цьому руслі було здійснено вченими [12]. Вони запропонували когнітивний фреймворк для класифікації вакансій у сфері кібербезпеки (наприклад, операторів та аналітиків) саме на основі їх елементарних вимог з метою оптимального підбору кандидатів. Результати ретельного опрацювання наукових та аналітичних джерел дозволив виділити основні когнітивні навички спеціалістів безпеки, що є критичними для даної професії (таблиця 1).

Таблиця 1

Когнітивні навички спеціалістів з кібербезпеки

№ з/п	Когнітивні чинники	Значення для спеціаліста з ІКБ
1	Когнітивні уявлення про ризик (обов’язково) [24]	Формують сприймання та оцінювання ризикової ситуації
2	Стійка увага (обов’язково) [9, 25]	Дозволяє відрізнити «нормальну» активність від шкідливого вторгнення та адекватно відреагувати на загрозу; забезпечує моніторинг та швидке перемикання; допомагає підтримувати ситуаційну обізнаність та впливає на ефективність рішення
3	Пам'ять (обов’язково) [9]	Робоча пам'ять дозволяє утримувати контент та дії, порівнювати та зіставляти. Довготривала пам'ять є основою для накопичення знань: семантична пам'ять слугує для зберігання фактів, концепцій та правил, а процедурна – для зберігання автоматизованих навичок.
4	Виконавчі функції (обов’язково) [9, 26, 27]	Необхідні для ефективного вирішення проблем та реагування на інциденти, є механізмом, який керує, контролює та координує інші когнітивні процеси:

№ з/п	Когнітивні чинники	Значення для спеціаліста з ІКБ
		- когнітивна гнучкість (перемикання завдань) дозволяє оператору переходити за шаблоном: моніторинг, розслідування, реагування; - інгібіторний контроль (гальмування, пригнічення) допомагає уникати передчасних рішень та ігнорувати фальшиві спрацьовування; - робоча пам'ять.
5	Когнітивно-рефлексивний стиль, саморегуляція (обов'язково) [6, 24]	Впливає на стратегію сприйняття ситуації ризику та контроль за поведінкою; характеризується більш виваженим реагуванням, що забезпечує кращий контроль у ситуації ризику. Імпульсивність є значущим чинником ризику. Когнітивна саморегуляція прогнозує ефективність кібероператорів.
6	Креативність у поєднанні з толерантністю до невизначеності (бажано)	Дозволяє швидко реагувати, ефективно долати труднощі та знаходити конструктивні рішення в умовах ризику
7	Виконавчі функції вищого порядку: аналітичне та творче мислення (обов'язково) [26]	Аналітичне та творче мислення виконують взаємодоповнюючі та критично важливі ролі для оператора з кібербезпеки: - за допомогою аналітичного мислення проблема розкладається на частини, виявляються причинно-наслідкові зв'язки та здійснюються логічні висновки; - за допомогою творчого мислення генеруються нові нестандартні ідеї та рішення.

Варто зауважити, що фахівці кібербезпеки мають володіти навичками емоційного інтелекту для покращення співпраці та стійкості команди [13].

Моделювання процесу формування когнітивних навичок спеціалістів з кібербезпеки

Дана модель побудована згідно теорії педагогічних систем, що містить три взаємопов'язаних структурних блоків.

1. Дидактико-цілепокладальний блок визначає мету, завдання та принципи формування когнітивних навичок спеціалістів з кібербезпеки.

Метою даної технології є удосконалення професійної підготовки фахівців з інформаційної та кібербезпеки на основі застосування когнітивного підходу, спрямованого на розвиток ключових когнітивних навичок, критично важливих для ефективного виявлення, аналізу та реагування на кіберзагрози.

Для досягнення даної мети потрібно реалізувати наступні завдання: сформувати систему наукових знань в галузі інформаційної та кібербезпеки, визначити та систематизувати когнітивні навички, критичні для спеціалістів з кібербезпеки, сформувати та розвинути дані когнітивні навички.

Теоретико-методологічною основою слугує проблемно-діяльнісний та особистісно-орієнтований підходи, характеристики та зміст яких сприяють завданням даної технології.

Дана технологія ґрунтується на принципах системності, практико-орієнтованості та індивідуалізації.

2. Формувальний блок містить змістову та діяльнісну складову.

Змістовий блок охоплює науково-методичне забезпечення дисциплін спеціальності F5, спеціалізовані тести щодо когнітивних здібностей людини та програмне забезпечення для навчальних активностей, які дозволяють формувати та розвивати когнітивні навички фахівців кібербезпеки.

Діяльнісний блок – це тренінги, симуляційні вправи, ігрові методи, когнітивні тренажери.

3. Діагностико-коригувальний блок містить інформацію про стан сформованості відповідної когнітивної навички.

Схема моделі формування когнітивних навичок спеціалістів з кібербезпеки представлена на рис.1.

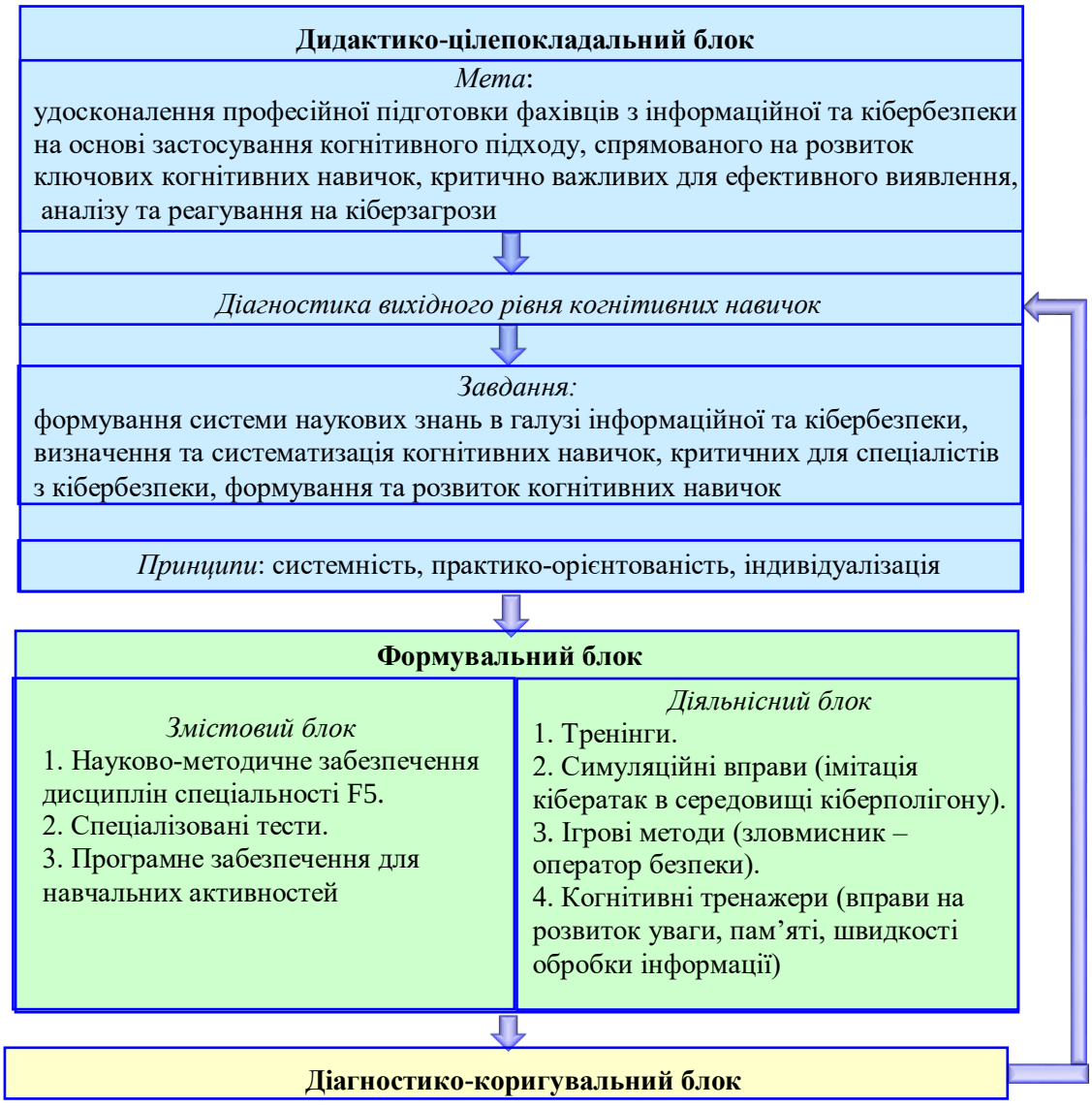

Рис.1. Модель формування когнітивних навичок спеціалістів з кібербезпеки

Логіка функціонування даного процесу ґрунтується на ітераціях взаємодії структурних блоків та їх складників. Спочатку діагностується поточний рівень когнітивних навичок спеціаліста, що слугує вхідним параметром в системі. Далі відбувається цілеспрямована організація змісту, методів та засобів, що орієнтує на досягнення наступного рівня. Цей досягнутий рівень автоматично стає вихідним параметром для переходу до подальшого навчального циклу. Кількість таких циклів, що охоплюють діагностику, корекцію змістового та діяльнісного блоку, визначається індивідуальною траєкторією та успішним формуванням когнітивних навичок за встановленими критеріями.

Ефективному впровадженню даної технології сприяє комплекс педагогічних умов, зокрема, готовність та кваліфікація викладача і відповідне технічне забезпечення.

Точкові експерименти щодо реалізації даної технології описано в дослідженнях [21-23, 28-37].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

На теоретичному етапі дослідження обґрунтовано та представлено модель формування когнітивних навичок спеціалістів з кібербезпеки. Деталізація методичного забезпечення, опис етапів її практичної реалізації включно з експериментальною перевіркою її ефективності планується висвітлити у серії подальших наукових розвідках.

Є очевидним, що ефективний захист можливий лише у збалансованому поєднанні найсучасніших технічних засобів з психологічними та поведінковими знаннями про людську діяльність в системах безпеки.

ПОДЯКА

Дослідження проведено в рамках реалізації науково-дослідної теми «Методи та моделі забезпечення кібербезпеки інформаційних систем переробки інформації та функціональної безпеки програмно-технічних комплексів управління критичної інфраструктури (реєстраційний номер 0122U200483 від 06.07.2022)».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R. *et al.* (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecur* **3**, 10 https://doi.org/10.1186/s42400-020-00050-w
2. Bone, James. (2024). Cognition in Cybersecurity Situational Awareness. 10.13140/RG.2.2.23490.59842.
3. Eden, S., Kasowaki, L., The Human Element in Cybersecurity: Understanding and Mitigating Risks. EasyChair print no. 11642, 2023
4. 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
5. 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
6. Jøsok Ø, Lugo R, Knox BJ, Sütterlin S and Helkala K (2019) Self-Regulation and Cognitive Agility in Cyber Operations. *Front. Psychol.* 10:875. doi: 10.3389/fpsyg.2019.00875
7. Yvan Burguin, Philippe Rauffet, David Espes, Christine Chauvin, Philippe Le Parc. (2022) RESCAPE Project: Tool for cyberdefense adaptive training based on the classification of operator cognitive state.. 13th AHFE Conference (Applied Human Factors and Ergonomics), New York, United States.
8. Musazade, N., Mezei, J., & Wang, X. (2025). Exploring the Impact of AI Tools on Cognitive Skills: A Comparative Analysis. *Algorithms*, *18*(10), 631. https://doi.org/10.3390/a18100631

9. Cole, K. A., Francis, A. L., Rogers, M. K., & Balazs, J. (2025). Can individual differences in cognitive capacity predict cybersecurity performance? Computers & Security, 155, 104497. https://doi.org/10.1016/j.cose.2025.104497
10. Lugo, R.G., Firth-Clark, A., Knox, B.J., Jøsok, Ø., Helkala, K., Sütterlin, S. (2019). Cognitive Profiles and Education of Female Cyber Defence Operators. In: Schmorrow, D., Fidopiastis, C. (eds) Augmented Cognition. HCII 2019. Lecture Notes in Computer Science, vol 11580. Springer, Cham. https://doi.org/10.1007/978-3-030-22419-6_40
11. Ullah, Faheem & Ye, Xiaohan & Fatima, Uswa & Akhtar, Zahid & Wu, Yuxi & Ahmad, Hussain. (2025). What Skills Do Cyber Security Professionals Need?. https://doi.org/10.48550/arXiv.2502.13658
12. Susan G. Campbell, Lelyn D. Saner, and Michael F. Bunting. (2016) Characterizing cybersecurity jobs: applying the cyber aptitude and talent assessment framework. In Proceedings of the Symposium and Bootcamp on the Science of Security (HotSos '16). Association for Computing Machinery, New York, NY, USA, 25–27. https://doi.org/10.1145/2898375.2898394
13. Khadka, K., Ullah, A.B. (2025). Human factors in cybersecurity: an interdisciplinary review and framework proposal. Int. J. Inf. Secur. 24, 119 https://doi.org/10.1007/s10207-025-01032-0
14. Максименко С., Деркач Л., Кіричевська Е., Касинець М. Психологія когнітивних процесів: науковий посібник / Національна академія педагогічних наук України, Інститут психології імені Г.С. Костюка. Київ: «Видавництво Людмила», 2022. – 420 с.
15. Максименко С.Д., Ірхін Ю.Б., Деркач Л.М., Марусинець М.М., Касинець М.М. Психологічна організація модульного формування когнітивних здібностей: генетико-креативний підхід: навчальний посібник. Том 2. – Київ: «Видавництво Людмила», 2023. – 356 с.
16. Шапар В. Б. Сучасний тлумачний психологічний словник. — Х.: Прапор, 2007.— 640 с. ISBN 966-7880-85-0.
17. Мукан, Н., Чубінська, Н., & Стасишин, Р. (2023). Роль і значення когнітивних та метакогнітивних навичок у професійній діяльності правника. *Академічні візії*, (22). https://academy-vision.org/index.php/av/article/view/477
18. Носенко, Е. Л., Коврига, Н. В. (2003). Емоційний інтелект: концептуалиізація феномену, основні функції. К.: Вища школа., 2023, 159 с.
19. Tang, K. S. (2020). The use of epistemic tools to facilitate epistemic cognition & metacognition in developing scientific explanation. Cognition and Instruction, 38(4), 474 502.
20. Eric A. Hanushek et al. (2025) Age and cognitive skills: Use it or lose it.Sci. Adv.11,eads1560. https://www.science.org/doi/10.1126/sciadv.ads1560
21. 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. с. 297-305. https://ceur-ws.org/Vol-3550/short15.pdf
22. 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. с. 356-362. https://ceur-ws.org/Vol-3826/short28.pdf
23. 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
24. Вдовіченко, Оксана. (2020). Концептуальні основи ризику особистості: циклічна структурно-процесуальна модель. *Вісник ХНПУ імені Г.С Сковороди Психологія*. 18-36. https://doi.org/10.34142/23129387.2020.62.01
25. McIntire, L.K., et al. (2013), Detection of vigilance performance using eye blinks, *Applied Ergonomics*. http://dx.doi.org/10.1016/j.apergo.2013.04.020
26. Diamond A. (2013) Executive functions. Annu Rev Psychol.; 64:135-68. doi:10.1146/annurev-psych-113011-143750. Epub 2012 Sep 27. PMID: 23020641; PMCID: PMC4084861
27. David A.O. Njoga, Samuel Liyala, Silvance Abeka. (2022) Influence Of Cognitive Agility Of Cyber Operators On SituationalAware Cyberspace Protection. International Journal of Innovative Research and Advanced Studies (IJIRAS) Volume 9.
28. Шевченко С.М. (2007) Педагогічні умови формування аналітичного мислення студентів вищих технічних навчальних закладів. *Педагогіка, психологія та медико-біологічні проблеми фізичного виховання і спорту.* 2007. № 3. С. 151–154.
29. Шевченко С.М. (2013) Розвиток аналітичного мислення студентів вищих технічних навчальних закладів у процесі вивчення математичних дисциплін: автореф. дис. на здобуття наук. ступеня канд.

пед. наук: спец. 13.00.02 – теорія та методика навчання (математика) / С.М. Шевченко. – К.: НПУ ім. М.П. Драгоманова, 2013. – 20 с.

30. Бурячок, В. Л. та Шевченко, С. М. та Складанний, П. М. (2018) Віртуальна лабораторія для моделювання процесів в інформаційній та кібербезпеці як засіб формування практичних навичок студентів. *Кібербезпека: освіта, наука, техніка* (2). с. 98-104. ISSN 2663-4023
31. Жданова, Ю. Д. та Спасітєлєва, С. О. та Шевченко, С. М. (2019) Застосування бібліотеки класів Security.Cryptography для практичної підготовки спеціалістів з кібербезпеки. *Кібербезпека: освіта, наука, техніка*, 4 (4). с. 44-53. ISSN 2663-4023
32. Жданова, Ю Д. та Спасітєлєва, С.О. та Шевченко, С М. (2019) Формування у студентів ІТ-спеціальностей компетентностей в області захисту інформації з використанням криптографічних служб .NET FRAMEWORK *Фізико-математична освіта: науковий журнал* (1(19)). с. 48-54. ISSN 2413-158X
33. Жданова, Ю.Д. та Шевченко, С.М. та Спасітєлєва, С.О. та Кравчук К. В. (2020). Прикладні та методичні аспекти застосування хеш-функцій в інформаційній безпеці. *Кібербезпека: освіта, наука, техніка*, 4 (8). с. 85-96. ISSN 2663-4023
34. Шевченко, Світлана Миколаївна та Жданова, Юлія Дмитрівна та Спасітєлєва, Світлана Олексіївна та Складанний, Павло Миколайович (2020) Проведення SWOT-аналізу оцінювання інформаційних ризиків як засіб формування практичних навичок студентів спеціальності 125 Кібербезпека *Кібербезпека: освіта, наука, техніка*, 2 (10). с. 158-168. ISSN 2663-4023
35. Бурячок, В.Л. та Коршун, Н. В. та Шевченко, С.М. та Складанний, П. М. (2020) Застосування середовища NI Multisim при формуванні практичних навичок студентів спеціальності 125 «Кібербезпека» *Кібербезпека: освіта, наука, техніка*, 9 (1). с. 159-196. ISSN 2663-4023
36. Бурячок, В.Л. та Шевченко, С.М та Жданова, Ю. Д. та Складанний, П. М. (2021) Міждисциплінарний підхід до формування навичок управління ризиками ІБ на засадах теорії прийняття рішень. *Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка"*, 3 (11). с. 155-165. ISSN 2663-4023
37. Шевченко, С.М. та Жданова, Ю. Д. та Кравчук, К.В. (2021) Модель захисту інформації на основі оцінки ризиків інформаційної безпеки для малого та середнього бізнесу *Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка",* 2 (14). с. 158-175. ISSN 2663-4023

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (30), 2025
Спеціальний випуск ISSN 2663 – 4023
Special issue

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

Svitlana O. Spasiteleva
PhD, Associate Professor,
Associate Professor of the Department of Information and Cyber Security
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine
ORCID: 0000-0003-4993-6355
s.spasitielieva@kubg.edu.ua

A MODEL FOR FORMATION COGNITIVE SKILLS FOR CYBERSECURITY SPECIALISTS

Abstract. This article is devoted to the development and theoretical substantiation of a methodology for the formation of cognitive skills in information and cyber security specialists, the implementation of which will allow improving the professional training of specialists and will contribute to increasing motivation in the educational process. The relevance of the problem of training highly qualified cybersecurity specialists is due to the rapid growth of cyber threats, which requires not only technical knowledge of a person, but also developed cognitive skills (critical thinking, the ability to make quick decisions, pattern recognition and stress resistance). By analyzing psychological and methodological literature, the essence and structure of the concept of "cognitive skills", which are critical for information and cybersecurity specialists, are detailed. Based on the problem-activity and personality-oriented approaches, a model of the formation of cognitive skills of cybersecurity specialists has been developed, the main stages of which are diagnostic, formative and control-corrective. Based on the principles of systematicity and professional orientation, a formative block has been defined, which contains a content and activity component. The content part of the methodology covers the scientific and methodological support of disciplines of the specialty F5, software for educational activities and specialized tests in psychology. The activity part of the model is provided by trainings, simulation exercises such as imitation of cyberattacks in the cyber polygon environment, game methods (attacker - security specialists) and cognitive simulators aimed at developing attention, memory, speed of information processing. Pedagogical conditions for the effective implementation of this methodology are outlined, in particular, the readiness and qualification of teachers and technical support. The results of the study can be used by higher education institutions and training centers to modernize curricula and improve the quality of training specialists in the field of information security.

Keywords: information security; cybersecurity; cognitive skills; information security; model of forming cognitive skills.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Maalem Lahcen, R. A., Caulkins, B., Mohapatra, R., et al. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity, 3*(10). https://doi.org/10.1186/s42400-020-00050-w
2. Bone, J. (2024). *Cognition in cybersecurity situational awareness.* https://doi.org/10.13140/RG.2.2.23490.59842
3. Eden, S., & Kasowaki, L. (2023). *The human element in cybersecurity: Understanding and mitigating risks. EasyChair Preprint,* 11642.
4. Andrade, R. O., & Yoo, S. G. (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
5. Jiang, Y., & Atif, Y. (2021). A selective ensemble model for cognitive cybersecurity analysis. *Journal of Network and Computer Applications, 193,* 103210. https://doi.org/10.1016/j.jnca.2021.103210
6. Jøsok, Ø., Lugo, R., Knox, B. J., Sütterlin, S., & Helkala, K. (2019). Self-regulation and cognitive agility in cyber operations. *Frontiers in Psychology, 10,* 875. https://doi.org/10.3389/fpsyg.2019.00875
7. Burguin, Y., Rauffet, P., Espes, D., Chauvin, C., & Le Parc, P. (2022). *RESCAPE Project: Tool for cyberdefense adaptive training based on the classification of operator cognitive state. 13th AHFE Conference (Applied Human Factors and Ergonomics),* New York, United States.
8. Musazade, N., Mezei, J., & Wang, X. (2025). Exploring the impact of AI tools on cognitive skills: A comparative analysis. *Algorithms, 18*(10), 631. https://doi.org/10.3390/a18100631
9. Cole, K. A., Francis, A. L., Rogers, M. K., & Balazs, J. (2025). Can individual differences in cognitive capacity predict cybersecurity performance? *Computers & Security, 155,* 104497. https://doi.org/10.1016/j.cose.2025.104497
10. Lugo, R. G., Firth-Clark, A., Knox, B. J., Jøsok, Ø., Helkala, K., & Sütterlin, S. (2019). Cognitive profiles and education of female cyber defence operators. In D. Schmorrow & C. Fidopiastis (Eds.), *Augmented cognition. HCII 2019. Lecture Notes in Computer Science* (Vol. 11580). Springer. https://doi.org/10.1007/978-3-030-22419-6_40
11. Ullah, F., Ye, X., Fatima, U., Akhtar, Z., Wu, Y., & Ahmad, H. (2025). *What skills do cyber security professionals need?* https://doi.org/10.48550/arXiv.2502.13658
12. Campbell, S. G., Saner, L. D., & Bunting, M. F. (2016). Characterizing cybersecurity jobs: Applying the cyber aptitude and talent assessment framework. In *Proceedings of the Symposium and Bootcamp on the Science of Security (HotSos '16)* (pp. 25–27). ACM. https://doi.org/10.1145/2898375.2898394
13. Khadka, K., & Ullah, A. B. (2025). Human factors in cybersecurity: An interdisciplinary review and framework proposal. *International Journal of Information Security, 24,* 119. https://doi.org/10.1007/s10207-025-01032-0
14. Maksymenko, S., Derkach, L., Kirichevska, E., & Kasynets, M. (2022). *Psychology of cognitive processes: A scientific manual.* Kyiv: Lyudmila Publishing House.
15. Maksymenko, S. D., Irkhin, Yu. B., Derkach, L. M., Marusynets, M. M., & Kasynets, M. M. (2023). *Psychological organization of modular formation of cognitive abilities: Genetic-creative approach* (Vol. 2). Kyiv: Lyudmila Publishing House.
16. Shapar, V. B. (2007). *Modern explanatory psychological dictionary.* Kharkiv: Prapor. ISBN 966-7880-85-0.
17. Mukan, N., Chubinska, N., & Stasyshyn, R. (2023). The role and significance of cognitive and metacognitive skills in the professional activity of a lawyer. *Academic Visions, (22).* https://academy-vision.org/index.php/av/article/view/477
18. Nosenko, E. L. (2003). *Emotional intelligence: Conceptualization of the phenomenon, basic functions.* Kyiv: Higher School.
19. Tang, K. S. (2020). The use of epistemic tools to facilitate epistemic cognition and metacognition in developing scientific explanation. *Cognition and Instruction, 38*(4), 474–502.
20. Hanushek, E. A., et al. (2025). Age and cognitive skills: Use it or lose it. *Science Advances, 11,* eads1560. https://doi.org/10.1126/sciadv.ads1560
21. Shevchenko, S., Zhdanova, Y., Shevchenko, H., Nehodenko, O., & Spasiteleva, S. (2023). Information security risk management using cognitive modeling. *Cybersecurity Providing in Information and Telecommunication Systems, 3550,* 297–305. https://ceur-ws.org/Vol-3550/short15.pdf
22. Shevchenko, S., Zhdanova, Y., Kryvytska, O., Shevchenko, H., & Spasiteleva, S. (2024). Fuzzy cognitive mapping as a scenario approach for information security risk analysis. *Cybersecurity Providing in Information and Telecommunication Systems II, 3826,* 356–362. https://ceur-ws.org/Vol-3826/short28.pdf

23. Shevchenko, S., Zhdanova, Y., Skladannyi, P., & Petrenko, T. (2024). Fuzzy cognitive maps as a tool for visualizing incident response scenarios in security systems. *Cybersecurity: Education, Science, Technique, 2*(26), 417–429. https://doi.org/10.28925/2663-4023.2024.26.707
24. Vdovichenko, O. (2020). Conceptual foundations of personality risk: A cyclical structural-process model. *Bulletin of the KhNPU named after G.S. Skovoroda. Psychology*, 18–36.
25. McIntire, L. K., et al. (2013). Detection of vigilance performance using eye blinks. *Applied Ergonomics.* https://doi.org/10.1016/j.apergo.2013.04.020
26. Diamond, A. (2013). Executive functions. *Annual Review of Psychology, 64,* 135–168. https://doi.org/10.1146/annurev-psych-113011-143750
27. Njoga, D. A. O., Liyala, S., & Abeka, S. (2022). Influence of cognitive agility of cyber operators on situationally aware cyberspace protection. *International Journal of Innovative Research and Advanced Studies (IJIRAS), 9.*
28. Shevchenko, S. M. (2007). Pedagogical conditions for the formation of analytical thinking of students of higher technical educational institutions. *Pedagogy, Psychology and Medical-Biological Problems of Physical Education and Sports, (3),* 151–154.
29. Shevchenko, S. M. (2013). *Development of analytical thinking of students of higher technical educational institutions in the process of studying mathematical disciplines* (Doctoral dissertation). National Pedagogical University named after M. P. Drahomanov, Kyiv.
30. Buriachok, V. L., Shevchenko, S. M., & Skladannyi, P. M. (2018). Virtual laboratory for process modeling in information and cybersecurity as a means of forming students' practical skills. *Cybersecurity: Education, Science, Technique, 2*(2), 98–104. https://doi.org/10.28925/2663-4023.2018.2.98104
31. Zhdanova, Y., Spasiteleva, S., & Shevchenko, S. (2019). Application of the Security.Cryptography class library for practical training of cybersecurity specialists. *Cybersecurity: Education, Science, Technique, 4*(4), 44–53. https://doi.org/10.28925/2663-4023.2019.4.4453
32. Zhdanova, Y., Spasiteleva, S., & Shevchenko, S. (2019). Formation of IT students' competencies in information protection using cryptographic services .NET Framework. *Physics and Mathematics Education, 1*(19), 48–54.
33. Zhdanova, Y., Spasiteleva, S., Shevchenko, S., & Kravchuk, K. (2020). Applied and methodical aspects of using hash functions for information security. *Cybersecurity: Education, Science, Technique, 4*(8), 85–96. https://doi.org/10.28925/2663-4023.2020.8.8596
34. Shevchenko, S., Zhdanova, Y., Spasiteleva, S., & Skladannyi, P. (2020). Conducting a SWOT-analysis of information risk assessment as a means of forming practical skills of Students Specialty 125 Cyber Security. *Cybersecurity: Education, Science, Technique, 2*(10), 158–168. https://doi.org/10.28925/2663-4023.2020.10.158168
35. Buriachok, V., Korshun, N., Shevchenko, S., & Skladannyi, P. (2020). Application of NI Multisim environment in the practical skills building for students of 125 "Cybersecurity" specialty. *Cybersecurity: Education, Science, Technique, 9*(1), 159–196. https://doi.org/10.28925/2663-4023.2020.9.159169
36. Buriachok, V., Shevchenko, S., Zhdanova, Y., & Skladannyi, P. (2021). Interdisciplinary approach to the development of information security risk management skills on the basis of decision-making theory. *Cybersecurity: Education, Science, Technique, 3*(11), 155–165. https://doi.org/10.28925/2663-4023.2021.11.155165
37. Shevchenko, S., Zhdanova, Y., & Kravchuk, K. (2021). Information protection model based on information security risk assessment for small and medium-sized businesses. *Cybersecurity: Education, Science, Technique, 2*(14), 158–175. https://doi.org/10.28925/2663-4023.2021.14.158175