оцінку 4.3/5 за точність порівняно з 2.8/5 для традиційних підходів. У сфері архітектурних рішень агентні системи на 54% частіше рекомендують рішення, що відповідають довгостроковим вимогам проєкту.

Результати дослідження переконливо доводять, що адаптивні RAG-системи з агентним управлінням знаннями є потужним інструментом для прискорення еволюції програмних продуктів. Поєднуючи можливості LLM, механізми пошуку та агентне управління, ці системи ефективно вирішують складні задачі розробки, оптимізації та підтримки програмного забезпечення. Проаналізовані експериментальні дані демонструють значне покращення ефективності порівняно з традиційними підходами, що робить адаптивні RAG-системи перспективним напрямком для подальших досліджень та практичного застосування в індустрії програмного забезпечення.

Література:

1. Singh A., Ehtesham A., Kumar S., Talaei Khoei T. Agentic Retrieval-Augmented Generation: A Survey on Agentic RAG. arXiv Computer Science, 2025. URL: https://arxiv.org/html/2501.09136v1 (дата звернення: 02.03.2025).

2. Wang L., Ma C., Feng X., Zhang Z. A Survey on Large Language Model Based Autonomous Agents. Frontiers of Computer Science, 2024. Vol. 18(6). URL: https://arxiv.org/abs/2308.11432 (дата звернення: 01.03.2025).

3. Jeong S., Baek J., Cho S., Hwang S.J., Park J.C. Adaptive-RAG: Learning to Adapt Retrieval-Augmented Large Language Models through Question Complexity. arXiv Computer Science, 2024. URL: https://arxiv.org/html/2403.14403v1 (дата звернення: 09.03.2025).

4. Yan S-Q., Gu J-C., Zhu Y., Ling Z-H. Corrective Retrieval Augmented Generation. arXiv Computer Science, 2024. URL: https://arxiv.org/html/2401.15884v1 (дата звернення: 04.03.2025).

DOI https://doi.org/10.36059/978-966-397-491-0-33

КІБЕРБЕЗПЕКА ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Прядка С. А.
магістр
Міжнародний гуманітарний університет
м. Одеса, Україна

Кібербезпека є ключовим елементом національної безпеки України. У 2015 році було ухвалено Стратегію національної безпеки, яка визначає

захист критичної інфраструктури як один із пріоритетів державної політики, а у 2016 році – Стратегію кібербезпеки. Їхнє ухвалення зумовлене безпрецедентними подіями, зокрема численними кібератаками: у 2014 році зафіксовано 1240 зовнішніх втручань у критичну інфраструктуру, у 2015 році – 865, у 2016 році – понад 200. У першому кварталі 2019 року кількість кіберінцидентів в Україні зросла до 1 582 054.

Критична інфраструктура є основою функціонування будь-якої країни, охоплюючи оборону, промисловість, енергетику, охорону здоров'я, виробництво стратегічних товарів, водопостачання та транспорт. В Україні триває формування власної системи кіберзахисту в умовах протистояння російській агресії, з урахуванням передового досвіду НАТО, ЄС та міжнародних практик.

Розробка нових методів боротьби з кіберзагрозами українськими фахівцями має значення не лише для України, а й для міжнародних партнерів. Кіберзлочинність все частіше використовується не лише для фінансового вимагання, а й як інструмент дестабілізації та геополітичного впливу, що вимагає спільних зусиль у сфері кібербезпеки на глобальному рівні [1, с. 494-495].

Кіберзахист включає систему організаційних, правових та технічних заходів, спрямованих на запобігання кіберзагрозам та ліквідацію їх наслідків. Деякі дослідники вважають, що ми вступили в фазу кібервійн, оскільки кількість небезпечних дій в кіберпросторі зростає. Кіберінтервенція – це комплекс суспільно небезпечних дій, які завдають шкоди важливим сферам держави та суспільства.

В Україні кількість кібератак значно зросла з 2014 року. Кожен третій комп'ютер в Україні заражений шкідливими програмами. Тому одним із важливих завдань держави є встановлення рівнів захисту інформації, таких як запобігання, виявлення, обмеження та відновлення.

Створення безпечного кіберпростору передбачає впровадження системи заходів на декількох рівнях: політичному, юридичному, міжнародному, освітньому та науково-технічному. З кожним роком органи публічного управління все більше залежать від технологій, що потребує якісної взаємодії з громадянами та цифрової грамотності.

Україна має орієнтуватись на кращі зарубіжні практики зі створення ефективної системи кіберзахисту та розширювати міжнародну співпрацю. В 2005 році була ратифікована Конвенція Ради Європи про кіберзлочинність, яка передбачає настання відповідальності за правопорушення проти конфіденційності та цілісності комп'ютерних даних та систем.

Нормативно-правову базу кібербезпеки в Україні складають Конституція, Стратегія кібербезпеки, закони «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про

захист персональних даних» та інші. Однак дослідники вказують на наявність багатьох проблем, таких як застаріла нормативна база, відсутність чіткого правового механізму залучення громадянського суспільства та недостатня обізнаність громадян.

Вирішення цих проблем потребує комплексного підходу, включаючи вдосконалення законодавства, розширення міжнародної співпраці, просвітницькі кампанії та активні дії з боку держави. Важливим кроком є створення єдиної інтелектуальної системи кібербезпеки та розвиток освіти в цій сфері.

З жовтня 2020 року реалізується спільний проєкт CRDF Global із МНТУ та ДІТМ МНТУ. Першим етапом співпраці стало проведення безкоштовного онлайн-курсу «Базові правила безпеки у цифровому середовищі», у якому взяли участь 300 студентів. Курс, присвячений основам кібергігієни, здобув популярність серед українських студентів і поширився в інших країнах. У доступній формі він пояснює особливості кіберпростору, діяльність хакерів, їхні цілі, а також надає рекомендації щодо захисту особистих даних і безпечного використання інформаційних ресурсів.

Студенти різних спеціальностей, які пройшли курс, успішно склали підсумкове тестування та отримали сертифікати. Після завершення першого етапу було проведено опитування, яке показало високу оцінку користі курсу. Учасники залишили позитивні відгуки про таку практику підвищення обізнаності у сфері кібербезпеки [2, с. 89-91].

Місцеві органи влади в Україні традиційно мають слабший рівень кіберзахисту порівняно з центральними, які користуються підтримкою ключових кібербезпекових структур. Важливо приділити увагу зміцненню кібербезпеки на місцевому рівні, зокрема шляхом розробки базових рекомендацій для таких організацій. Досвід США та Великої Британії свідчить, що хакери дедалі частіше атакують саме ці об’єкти, включно з підприємствами водного сектору, щоб завдати шкоди на локальному рівні [3, с. 30].

Для місцевих організацій варто створити більше інструментів самооцінки кібербезпеки, наприклад, на основі рекомендацій CISA Cybersecurity Performance Goals. Це дасть змогу впроваджувати найкращі практики та самостійно оцінювати рівень захисту.

Україна практично не володіє точною інформацією про стан кібербезпеки місцевих органів влади, їхні потреби та можливості. Необхідно ініціювати оцінку цих потреб для формування ефективної державної політики в цій сфері.

Підготовка нового покоління кіберфахівців є пріоритетом для багатьох країн. У процесі розробки проєкту Стратегії кібербезпеки на період після 2025 року Україні варто визначити власний підхід до цього питання. Це

можна оформити як окремий розділ у новій Стратегії кібербезпеки або створити спеціальний документ, наприклад, Стратегію розвитку кадрів у сфері кібербезпеки.

Як і більшість країн, Україна стикається з нестачею кваліфікованих фахівців, особливо в державному секторі, і має шукати ефективні шляхи вирішення цієї проблеми. Корисним може бути досвід США, де розширюють навчальні програми, залучаючи нові цільові групи, зокрема жінок, військовослужбовців та державних службовців, що проходять перекваліфікацію. Крім того, у США спрощують вимоги до посад у сфері кібербезпеки, що сприяє залученню ширшого кола спеціалістів [3, с. 31-32].

Міжнародна співпраця у сфері кібербезпеки потребує подальшої систематизації. У 2022–2023 роках Україна налагодила партнерство з ENISA (ЄС) та CISA (США). ENISA має глибоку експертизу в аналітиці та дослідженнях, а CISA спеціалізується на розширенні кіберсервісів для різних стейкхолдерів. Для ефективного використання цих напрацювань Україні варто розробити чіткі плани співпраці з конкретними цілями.

Україна неминуче зіткнеться з питанням захисту виборчого процесу, пов'язаного з активним використанням ІТ. Вже зараз слід активізувати взаємодію з CISA, переймаючи їхній досвід кіберзахисту виборів і, водночас, надаючи експертну підтримку через обмін інформацією про кіберзагрози.

Євроінтеграція залишається ключовим зовнішньополітичним пріоритетом України, проте в частині кібербезпеки цей процес потребує більшої прозорості та систематизації. Необхідно чітко визначити європейські нормативні акти, що підлягають імплементації в Україні, та оцінити стан їх виконання. Це також передбачає постійний моніторинг змін у законодавстві ЄС і визначення оптимальних термінів для їх впровадження в українське законодавство [3, с. 32].

Література:

1. Кібербезпека як складова національної безпеки та кіберзахист критичної інфраструктури України. URL: https://www.researchgate.net/publication/337725857_KIBERBEZPEKA_AK_SKLADOVA_NACIONALNOI_BEZPEKI_TA_KIBERZAHIST_KRITICNOI_INFRASTRUKTURI_UKRAINI

2. Шляхи удосконалення системи кібербезпеки в Україні. URL: https://www.researchgate.net/publication/358597497_Slahi_udoskonalenna_sistemi_kiberbezpeki_v_Ukraini

3. Річний аналітичний огляд: ключові події, тенденції та виклики у сфері кібербезпеки у 2024 році. URL: https://www.rnbo.gov.ua/files/2024/NATIONAL_CYBER_SCC/20250109/Year%20in%20review_UKR_upd.pdf