Медіафорум : аналітика, прогнози, інформаційний менеджмент.
Том 17. 205-226

Mediaforum: Analytics, Forecasts, Information Management.
Volume 17. 205-226

https://doi.org/10.31861/mediaforum.2025.17.205-226
УДК: 327 (342.1)

© *Наталія Ротар*[1]

КІБЕРБЕЗПЕКА ТА СТІЙКІСТЬ В СТРУКТУРІ ЦИФРОВОЇ ПОЛІТИКИ КРАЇН ВИШЕГРАДСЬКОЇ ГРУПИ

У статті здійснений порівняльний аналіз кібербезпеки та стійкості в структурі цифрової політики країн Вишеградської групи (Польщі, Чехії, Словаччини та Угорщини). Доведено, що Спільним для національних моделей кібербезпеки та цифрової стійкості країн Вишеграду є прагнення інтегрувати власні політики у стратегічні рамки «Цифрового десятиліття» ЄС, де кіберзахист розглядається як ключовий чинник легітимності цифрової демократії. Усі країни визнають кібербезпеку стратегічним пріоритетом, поєднуючи інституційні реформи, правову гармонізацію та освітні програми для громадян і бізнесу. Вони поступово вибудовують інституційну координацію, створюють спеціалізовані центри та механізми реагування на інциденти, а також інвестують у розвиток цифрових навичок, що формує культуру відповідальності та довіри до цифрових інституцій. Обґрунтовано, що специфіка кожної національної (польської, чеської, словацької, угорської) моделі кібербезпеки та цифрової стійкості полягає у різних акцентах і політичних контекстах, які визначають їхню роль у структурі цифрової політики. Польська модель вирізняється системністю та багаторівневістю, вона поєднує законодавчі реформи, інституційну координацію та масштабні освітні програми, що створює цілісну архітектуру цифрової стійкості. Чеська модель має особливість у високій суспільній обізнаності та активній участі бізнесу, що формує підґрунтя для демократичної участі громадян у цифровому середовищі. Угорська модель відрізняється подвійним характером: з одного боку, вона демонструє прогрес у впровадженні європейських стандартів і технологічних рішень, а з іншого, функціонує в умовах авторитарного режиму, де кібербезпека

[1] Доктор політичних наук, професор, професор кафедри політології та державного управління Чернівецького національного університету імені Юрія Федьковича, n.rotar@chnu.edu.ua; https://orcid.org/0000-0002-6430-3460.

використовується не лише як інструмент захисту, але й як механізм контролю над суспільством. Специфіка словацької моделі кібербезпеки та цифрової стійкості полягає у поєднанні відносно низького рівня інцидентів у корпоративному секторі з високим рівнем суспільного запиту на посилення захисту цифрових послуг.

Ключові слова: *цифрова політика, цифрова трансформація, цифрова демократія, кібербезпека, стійкість, Вишеградська група, Європейський Союз, Польща, Словаччина, Угорщина, Чехія.*

Cybersecurity and Resilience in the Structure of Digital Policy of the Visegrad Group Countries

The article provides a comparative analysis of cybersecurity and resilience in the digital policy framework of the Visegrad Group countries (Poland, the Czech Republic, Slovakia and Hungary). It is proven that the national models of cybersecurity and digital resilience of the Visegrad countries share a common desire to integrate their own policies into the strategic framework of the EU's "Digital Decade", where cyber security is considered a key factor in the legitimacy of digital democracy. All countries recognize cybersecurity as a strategic priority, combining institutional reforms, legal harmonization and educational programs for citizens and businesses. They are gradually building institutional coordination, creating specialized centers and incident response mechanisms, and investing in the development of digital skills, which forms a culture of responsibility and trust in digital institutions. It is substantiated that the specificity of each national (Polish, Czech, Slovak, Hungarian) model of cybersecurity and digital resilience lies in different emphases and political contexts that determine their role in the structure of digital policy. The Polish model is distinguished by its systematicity and multi-levelness, it combines legislative reforms, institutional coordination and large-scale educational programs, which creates a holistic architecture of digital resilience. The Czech model is characterized by high public awareness and active participation of business, which forms the basis for the democratic participation of citizens in the digital environment. The Hungarian model is distinguished by a dual character: on the one hand, it demonstrates progress in the implementation of European standards and technological solutions, and on the other, it functions in the conditions of an authoritarian regime, where cybersecurity is used not only as a tool of protection, but also as a mechanism of control over society. The specificity of the Slovak model of cybersecurity and digital resilience lies in the combination of a relatively low level of incidents in the

corporate sector with a high level of public demand for increased protection of digital services.

Keywords: *digital policy, digital democracy, digital transformation, cybersecurity, resilience, Visegrad Group, European Union, Poland, Slovakia, Hungary, Czech Republic.*

Постановка наукової проблеми та її значення. Актуальність політологічного вивчення кібербезпеки та цифрової стійкості в структурі цифрової політики країн Вишеградської групи визначається тим, що саме ці держави перебувають на перетині кількох стратегічних процесів: інтеграції у європейський цифровий простір, протидії зростаючим загрозам у сфері інформаційної безпеки та пошуку балансу між демократичними цінностями і політичними практиками, які не завжди відповідають стандартам відкритості. Польща, Чехія, Словаччина та Угорщина демонструють різні моделі реагування на виклики цифрової доби, але всі вони стикаються з необхідністю узгодження національних стратегій із рамками «Цифрового десятиліття» ЄС, де кіберзахист і стійкість інституцій розглядаються як фундамент цифрової демократії. Саме регіональний вимір є важливим для розуміння того, як національні моделі можуть взаємодіяти між собою та з європейськими структурами, створюючи умови для колективної стійкості у межах ЄС.

Аналіз останніх досліджень та методологія дослідження. Структура наукових досліджень кібербезпеки та цифрової стійкості в межах цифрової політики країн Вишеградської групи формується як складний аналітичний простір. У центрі уваги перебуває питання гармонізації національних стратегій із європейськими рамками «Цифрового десятиліття» (Harangozó, Fakó 2024), де кіберзахист і стійкість інфраструктури розглядаються як ключові умови легітимності цифрової демократії (Belas, Kliestik, Dvorsky, Streimikiene 2025). Структура досліджень унаочнює поєднання аналізу нормативних рамок (Procházka 2025), оцінки інституційної ефективності (Zawicki 2024), вивчення технологічних інновацій (Oramus 2024) та дослідження суспільних настроїв, що дозволяє комплексно осмислити кібербезпеку як політичний ресурс і водночас як основу стійкості цифрової демократії.

Методологія дослідження ґрунтується на міждисциплінарному підході, який поєднує інституційний аналіз, порівняльний метод,

нормативно-правову оцінку та методи вторинного аналізу соціологічних досліджень. Вона передбачає використання якісних і кількісних методів, що дозволяють дослідити як формальні рамки цифрової політики, так і практичні механізми її реалізації. Інституційний аналіз дає змогу оцінити ефективність державних органів, спеціалізованих центрів та механізмів координації, які відповідають за кібербезпеку. Порівняльний підхід дозволив виявити відмінності між польською, чеською, словацькою та угорською національними моделями кібербезпеки та цифрової стійкості в структурі цифрової політики національних держав. Нормативно-правовий аналіз спрямований на оцінку імплементації європейських директив та відповідності національних стратегій цінностям «Цифрового десятиліття» ЄС. В дослідженні також був використаний Індекс DESI, що виступає комплексним інструментом для оцінювання та відстеження рівня цифрової трансформації держав-членів ЄС.

Метою статті є здійснення комплексного політологічного дослідження кібербезпеки та цифрової стійкості в структурі цифрової політики країн Вишеградської групи. Для досягнення мети нами були визначені такі дослідницькі завдання: по-перше, охарактеризувати польську модель кібербезпеки та стійкості в структурі національної цифрової політики; по-друге, визначити матрицю чеської моделі кібербезпеки та стійкості ; по-третє, дослідити структуру угорської моделі кібербезпеки та стійкості як елементу національної цифрової політики; по-четверте, проаналізувати основні маркери словацької модель кібербезпеки та цифрової стійкості.

Виклад результатів дослідження. Сьогодні кібербезпека є одним з інструментів забезпечення легітимності державної влади, адже від здатності захистити дані та цифрові сервіси залежить рівень довіри громадян до політичних інститутів. Країни Вишеградської групи мають спільні історичні та політичні риси, але водночас демонструють відмінності у підходах до цифрової політики: від системної інституційної координації Польщі до високої суспільної обізнаності в Чехії, від корпоративної активності у Словаччині до подвійного характеру угорської моделі, де кіберзахист використовується також як інструмент політичного контролю.

Польська модель кібербезпеки та стійкості в структурі національної цифрової політики

Польща дедалі більше усвідомлює, що кібербезпека перетворю-

ється на один із ключових вимірів ефективності цифрової демократії. Зростання глобальної нестабільності та поширення онлайн-злочинності створюють нові ризики для державних інституцій, бізнесу та громадян, що змушує владу шукати системні рішення для захисту критичних інформаційних інфраструктур. Центральне геополітичне положення країни на східному фланзі НАТО робить її особливо вразливою до кібератак, а отже, потреба у цифровій стійкості стає не лише технічним завданням, а й стратегічним чинником безпеки та легітимності держави. Саме тому кіберзахист визначено одним із головних пріоритетів польського головування в Раді ЄС у першій половині 2025 року, а також інтегровано до проєкту Державної стратегії цифровізації, де він розглядається як наскрізна категорія, що впливає на всі інші напрями цифрової трансформації (Rada Ministrów 2024a). У цьому дискурсі кібербезпека постає як інструмент протидії загрозам та фундаментальний елемент європейської цифрової демократії, який забезпечує баланс між свободою комунікації, захистом прав громадян та інституційною спроможністю держави діяти в умовах нових ризиків.

Серед ключових викликів цифрової трансформації Польщі особливо виразною залишається проблема недостатнього рівня навичок цифрової безпеки серед населення. У контексті російсько-української війни ця слабкість набуває стратегічного значення, адже саме компетентність громадян у сфері захисту персональних даних визначає якість їхньої участі у цифровому суспільстві та довіру до інституцій. Дані 2023 р. засвідчили, що лише трохи більше половини поляків (54,06%) здійснили хоча б одну дію, спрямовану на захист власної інформації в інтернеті, тоді як середній показник по ЄС значно вищий (69,55%). (European Commission 2025). Ще більш проблематичною є ситуація з поглибленими навичками: менше третини населення (30,55%) продемонстрували здатність застосовувати комплексні практики цифрової безпеки, що свідчить про обмеженість суспільної готовності до викликів кіберпростору. Найчастіше громадяни обмежували доступ до даних про своє місцеперебування (34,03%), тоді як перевірка надійності вебресурсів залишалася найменш поширеною практикою (18,02%) (European Commission 2025). Така асиметрія у поведінкових моделях демонструє нерівномірність цифрової грамотності, а відтак потребу у системній політиці з підвищення компетентностей, що має стати складовою національної стра-

тегії цифровізації Польщі та наближуватися, таким чином, до загальноєвропейського дискурсу європейської моделі цифрової демократії.

Згідно з результатами опитування Eurobarometer у 2025 р., більшість громадян Польщі визнали, що підвищення рівня кіберзахисту, ефективніший контроль за персональними даними та гарантії безпечного функціонування цифрових технологій є важливими умовами для їхнього повсякденного використання. Водночас показник довіри до цих аспектів у польському суспільстві становить 74%, що помітно нижче за середній рівень по ЄС, який сягає 81% (European Commission 2025d). Крім того, у порівнянні з попереднім роком фіксується його зниження на 3%, що свідчить про певне послаблення суспільних очікувань та зростання критичності у ставленні до цифрової безпеки.

У 2024 р. польські державні інституції активізували діяльність, спрямовану на формування суспільної обізнаності щодо цифрових загроз та розвиток навичок кібербезпеки серед широких верств населення. Ці ініціативи були зорієнтовані насамперед на дітей та молодь, але водночас охоплювали й інші соціальні групи, що відповідає стратегічним пріоритетам «Цифрового десятиліття» ЄС та концепції цифрової демократії, де безпека і довіра громадян до цифрового середовища є ключовими умовами їхньої участі у суспільному житті. Національний науково-дослідний інститут NASK-PIB реалізував масштабну програму освітніх і профілактичних заходів, включаючи тренінги, майстер-класи, уроки та вебінари (NASK 2024a). У цих активностях взяли участь понад 36,333 тис. IT-фахівців та представників державної адміністрації, майже 287 тис. учнів, 18507 педагогів і спеціалістів, які працюють із дітьми та молоддю, 2060 батьків та 525 офіцерів, відповідальних за соціальну профілактику. Програма також включала конференції та виступи у медіа, що сприяло поширенню знань про цифрову безпеку на суспільному рівні (NASK 2024a). Офіс електронних комунікацій (Urząd Komunikacji Elektronicznej) провів кампанію #KeepCTRL («Klikam z głową»), яка охопила понад шість тисяч учнів через внутрішньошкільні уроки та понад шістдесят тисяч дітей початкових шкіл через онлайн-вебінари (Urząd Komunikacji Elektronicznej 2025). Основними темами були відповідальне користування цифровими пристроями та додатками, захист персональних даних і протидія кібербулінгу, що безпосередньо пов'язано з формуванням культури цифрової демократії серед

молодого покоління. Окремо варто відзначити Європейський місяць кібербезпеки, координований NASK-PIB, який був спрямований на дорослих користувачів. Кампанія охопила питання шахрайств у романтичних стосунках, фальшивих інвестицій, використання штучного інтелекту та поширення дипфейків. Вона забезпечила доступ до широкого спектра освітніх матеріалів, статей та інфографіки, вебінарів і практичних посібників, і охопила близько 1,4 мільйона осіб (Komisja Europejska 2025). Ці ініціативи у сфері кібербезпеки демонструють прагнення інтегрувати національні освітні та профілактичні практики у ширший європейський контекст «Цифрового десятиліття», де розвиток цифрових навичок і довіра до технологій розглядаються як основа демократичної участі та інституційної стійкості.

У 2024 р. для польського бізнес середовища був характерним відносно нижчий рівень кіберінцидентів, порівняно із середнім показником по ЄС, хоча тенденція до зростання загроз була очевидною. Частка підприємств, які зіткнулися з атаками, що призвели до тимчасової недоступності цифрових послуг, зокрема через програми-вимагачі чи атаки відмови в обслуговуванні, зросла з 2,93% у 2022 р. до 3,02% у 2024 р., залишаючись нижчою за середній рівень по ЄС (3,43%) (European Commission 2025). Ця динаміка підтверджується регулярними аналітичними оглядами, зокрема Барометром кібербезпеки KPMG Poland та щорічним «Звітом про кібербезпеку польських компаній» від VECTO. За їхніми даними, у 2024 р. кількість підприємств, що повідомили про щонайменше один кіберінцидент, зросла до 83% (на 16 пунктів більше, ніж роком раніше) за даними Барометра кібербезпеки (Barometr cyberbezpieczeństwa 2024), та до 73,9% (на 4 пункти більше) згідно зі Звітом Vecto (VECTO 2024).

Серед найбільш резонансних випадків варто відзначити масштабну розподілену атаку відмови в обслуговуванні проти компаній Autostrada Wielkopolska та Gdańsk Transport Company, які управляють ділянками автомагістралей A2 та A1. Відповідальність за атаку взяла проросійська група, що раніше здійснювала подібні дії проти транспортних компаній у Чехії та державних порталів у Франції. Іншим прикладом стала атака програм-вимагачів на польську IT-компанію Atende SA, яка призвела до несанкціонованого доступу до персональних даних працівників, клієнтів і партнерів. Також мережа аптек Super-Pharm зазнала витоку даних клієнтів унаслідок цілеспрямованої кібератаки. Ці інциденти демонструють, що навіть за

відносно нижчого рівня загроз порівняно з середнім по ЄС, польські підприємства залишаються вразливими до складних і координованих атак та підкреслюють необхідність системної інтеграції кіберзахисту у стратегії цифровізації, адже безпека даних в умовах російсько-української війни набула особливого значення.

Разом з тим, у 2024 р. польські компанії продемонстрували відносно високий рівень застосування базових заходів ІКТ-безпеки, перевищуючи середній показник по ЄС (92,76%), хоча рвень усвідомлення працівниками власних обов'язків у сфері кіберзахисту залишався нижчим за європейський середній рівень, що вказує на певну асиметрію між інституційними практиками та культурою цифрової відповідальності. За статистикою, 94,11% підприємств упровадили ті чи інші заходи безпеки, тоді як лише 56,84 % повідомили персонал про конкретні вимоги у сфері ІКТ-безпеки. Така ситуація демонструє, що формальні стандарти безпеки інтегруються швидше, ніж внутрішня корпоративна комунікація та розвиток цифрової компетентності працівників.

Найбільшим викликом для польського бізнесу у 2024 р. залишалася кадрова проблема, тобто складність залучення та утримання кваліфікованих спеціалістів у сфері кіберзахисту. Хоча 34% респондентів «Барометра кібербезпеки» згадали цю проблему, її значущість знизилася порівняно з попереднім роком, що може свідчити про поступове вдосконалення управлінських практик. Другою за поширеністю проблемою була обмеженість фінансування, яку відзначили 33 % опитаних, але й вона поступово втрачає гостроту завдяки зростанню пріоритетності кібербезпеки у корпоративних бюджетах. Натомість більшою мірою актуалізувалася інша загроза, така як недостатня підтримка з боку топ-менеджменту, яка зросла з 17% у 2023 р. до 26% у 2024 р. (Barometr cyberbezpieczeństwa 2024). Це свідчить про те, що стратегічне бачення цифрової безпеки ще не стало невід'ємною частиною управлінської культури багатьох польських компаній.

Важливим чинником зміцнення корпоративної кіберстійкості стали заходи, передбачені національною дорожньою картою цифровізації. Програма «Основи бізнес-кібербезпеки» (NASK 2024), реалізована у співпраці Міністерства економічного розвитку та технологій із NASK-PIB і профінансована з ресурсів політики згуртованості, спрямована на підтримку малих і середніх підприємств у діагностиці та вдосконаленні їхньої кібербезпеки. У 2024 р. вона перебувала на

другому етапі пілотного впровадження. Паралельно розвивається «Ścieżka SMART» (Rada Ministrów 2024), що фінансується за пріоритетом 1 програми FENG, який дозволяє компаніям, що реалізують проєкти у сфері досліджень та інновацій, отримувати додаткову підтримку для посилення кіберзахисту (Fundusze Europejskie na Rozwój Cyfrowy 2024). Реалізація таких кроків політикик цифрових трансформацій дозволяє стверджувати: по-перше, що польський бізнес демонструє поступову інтеграцію кібербезпеки у власні стратегії розвитку що відповідає загальноєвропейським орієнтирам «Цифрового десятиліття»; по-друге, свідчить про формування нового балансу між технологічними інноваціями, корпоративною відповідальністю та демократичними цінностями цифрової епохи в польському соціокультурному полі.

Аналіз місця кібербезпеки та стійкості в структурі цифрової політики Польщі вказує на те, що фіксується відставання від загальноєвропейських тенденцій у впровадженні сучасних стандартів інтернет-безпеки, зокрема протоколу IPv6, що має стратегічне значення для розвитку цифрової демократії та реалізації цілей «Цифрового десятиліття» ЄС. Низький рівень використання цього протоколу серед польських користувачів (близько 15% проти середнього показника по ЄС у 36%) та на серверному рівні (3% проти 17% у ЄС) створює ризики для майбутнього економічного зростання, інноваційної динаміки та стійкості цифрової інфраструктури (European Commission 2025). В умовах вичерпання адресного простору IPv4 перехід на IPv6 стає політичним пріоритетом, адже він забезпечує масштабованість, стабільність і підвищений рівень безпеки інтернету, що є фундаментом посилення довіри громадян до цифрових інституцій.

Важливим елементом європейської цифрової стратегії також виступає розширення застосування DNSSEC, який вводить механізми автентифікації та захисту в систему доменних імен. У Польщі рівень валідації DNSSEC у третьому кварталі 2024 р. становив 46%, що майже відповідає середньому показнику по ЄС (47%) (European Commission 2025), що свідчить про поступове наближення країни до європейських стандартів, одночасно підкреслюючи потребу у більш системному підході до впровадження критичних цифрових протоколів.

Кібербезпека залишається одним із найвразливіших напрямів функціонування державної адміністрації Польщі, що чітко окрес-

лено у проєкті «Стратегії цифровізації держави» (Rada Ministrów 2024a). Основними слабкими місцями визначено низький рівень усвідомлення ризиків та недостатність практичних навичок у сфері цифрової безпеки серед посадових осіб та працівників ключових політичних інституцій. У 2024 р. NASK-PIB реалізував низку масштабних програм, спрямованих на формування компетентностей та розвиток культури кіберзахисту в органах влади. Серед найважливіших ініціатив варто відзначити проєкт SecureV, орієнтований на підготовку стратегічних груп польського політикум (парламентарів та членів уряду), представників місцевого самоврядування, медичних закладів первинної допомоги та Національного виборчого офісу. Окремо було організовано навчання для керівників державних підприємств, що мало на меті інтеграцію принципів цифрової безпеки у корпоративне управління. Проєкт EDU-EXE охопив близько 27,5 тис. осіб, серед яких поліцейські, педагоги, працівники судових установ та органів місцевої влади, забезпечуючи поширення практичних знань у різних секторах публічного управління. Додатково понад 33 тис. учасників, залучених до національної системи кібербезпеки, пройшли спеціалізовані тренінги з реагування на кризові ситуації.

У 2024 р. Польща започаткувала масштабну ініціативу «Cyberbezpieczny Samorząd» (Rada Ministrów 2023), спрямовану на підвищення рівня інформаційної безпеки у територіальних громадах. Майже дев'ять із десяти самоврядних одиниць отримали фінансову підтримку для вдосконалення технічних рішень, організаційних процесів та розвитку компетентностей у сфері кіберзахисту. Цей проєкт став важливим кроком у формуванні цифрової стійкості на місцевому рівні, що відповідає стратегічним орієнтирам «Цифрового десятиліття» ЄС. Паралельно було започатковано створення Центру кібербезпеки NASK (NASK 2024a), який має об'єднати низку спеціалізованих підрозділів, офісів та лабораторій. Його завдання полягає у зміцненні національної системи кіберзахисту та підвищенні здатності держави ефективно реагувати на сучасні й майбутні загрози у цифровому середовищі. У 2025 році відбувся запуск нових програм, серед яких проєкт «Cyberbezpieczny Rząd» (Rada Ministrów 2025), орієнтований на посилення кібербезпеки центральних органів влади, міністерств та воєводських адміністрацій. Водночас планується реалізація ініціативи «Lokalne Centrum Cyberbezpieczeństwa»

(Horbaczewski 2025), що передбачає створення або розвиток регіональних структур кіберзахисту для підтримки місцевих органів самоврядування.

У польському дискурсі цифрової трансформації дедалі більше уваги приділяється питанням інституційної координації у сфері кібербезпеки. У проєкті «Стратегії цифровізації держави» передбачено створення центрального органу, який би відповідав за узгодження дій різних суб'єктів національної системи кіберзахисту та забезпечував цілісність політики у цій сфері. Хоча документ ще не набув чинності й не містить детальних положень щодо майбутньої структури, сама ідея відображає прагнення Польщі до формування цифрової стійкості держави та її інституцій. Паралельно Міністерство цифрових справ працює над розробкою Національної стратегії кібербезпеки на 2025–2029 роки, публікація якої очікується у середині 2025 року, ймовірно синхронно з ухваленням «Стратегії цифровізації держави». Важливим елементом цього процесу стане прийняття законодавчого акту, що імплементує положення Директиви NIS2 у польську правову систему (Rada Ministrów 2024a). Це означає не лише формальне наближення до європейських стандартів, а й посилення інституційної спроможності держави протидіяти кіберзагрозам, оскільки Польща поступово формує багаторівневу систему кібербезпеки, яка поєднує місцевий, національний та європейський рівні, що стверджують її суб'єктність у європейському дискурсі цифрової демократії.

Матриця чеської моделі кібербезпеки та стійкості в структурі національної цифрової політики

У чеському суспільстві питання цифрової безпеки набуває дедалі більшої ваги, що підтверджується високим рівнем практичної активності громадян у захисті власних персональних даних. У 2023 р. 81,98% населення країни здійснили хоча б одну дію для посилення своєї цифрової безпеки, що значно перевищує середній показник по ЄС (69,55%). Більш ніж половина громадян застосовували комплексні заходи, виконуючи три й більше дій, що свідчить про формування у Чехії культури цифрової грамотності, яка є фундаментом для розвитку цифрової демократії. Найпоширенішою практикою стало блокування використання персональних даних у рекламних цілях (58,19%), тоді як ознайомлення з політиками конфіденційності залишалося менш поширеним, (35,75%), що демонструє вибірковість у поведінкових моделях користувачів (European Commission 2025a).

На рівні корпоративного сектору Чехія стикається з більшою кількістю інцидентів, пов'язаних із порушенням ІКТ-безпеки, ніж середній показник по ЄС. У 2024 р. 4,49% підприємств повідомили про атаки, що призвели до недоступності цифрових сервісів, зокрема через програми-вимагачі чи атаки відмови в обслуговуванні. Відтак, чеські компанії формують та демонструють високий рівень готовності: 92,08 % впроваджують заходи кіберзахисту, а 77,47% активно навчають працівників їхнім обов'язкам у сфері ІКТ-безпеки, що значно перевищує середній показник по ЄС (59,97%) (European Commission 2025a).

Важливим свідченням стратегічного поступу є прогрес у впровадженні критично важливих інтернет-стандартів. Розгортання IPv6 у Чехії досягло 22% серед кінцевих користувачів і 37% на серверному рівні, що демонструє прагнення країни забезпечити масштабовану та безпечну інтернет-інфраструктуру. У контексті «Цифрового десятиліття» ЄС ці кроки підтверджують, що Чехія розглядає кібербезпеку як технічний виклик, політика подолання якого має формуватися на принципах цифрової демократії.

Чеська Республіка перебуває на етапі завершення імплементації положень Директиви NIS2, що є ключовим інструментом ЄС для гармонізації стандартів кіберзахисту. Незважаючи на те, що процес ще триває, держава послідовно наголошує на кібербезпеці як на стратегічному пріоритеті, особливо в умовах загострення геополітичних ризиків, спричинених війною Росії проти України. Сучасна рамка політики кіберзахисту визначається Національною стратегією кібербезпеки (NUKIB 2021) та відповідним Планом дій, які охоплюють державне управління, бізнес-сектор і критичні галузі, включно з охороною здоров'я та інфраструктурою. Усвідомлюючи трансформацію ландшафту загроз, чеська влада у 2023 р. розпочала процес оновлення Національної стратегії кібербезпеки, залучивши до консультацій як приватних, так і державних стейкхолдерів. Новий документ перебуває на стадії підготовки, а його ухвалення очікується до кінця 2025 р. разом із деталізованим Планом дій, що визначатиме конкретні кроки та часові рамки їх реалізації (NUKIB 2025).

Паралельно Чехія активно інтегрує положення «Арсеналу кібербезпеки ЄС 5G» (European Commission 2020), який визначено як критично важливий для захисту цифрової інфраструктури. Ці заходи спрямовані на посилення стійкості комунікаційних мереж та міні-

мізацію ризиків, пов'язаних із новими технологіями та зростаючими загрозами. У ширшому контексті «Цифрового десятиліття» ЄС такі кроки підтверджують прагнення Чехії поглибити інтеграцію національної політики кіберзахисти у європейську систему цифрової демократії та спільну європейську політику цифрових трансформацій.

За результатами вимірювань Євробарометру у 2025 р., більшість громадян Чехії визнають важливість кібербезпеки для щоденного використання цифрових технологій, проте рівень підтримки цього твердження (71%) залишається нижчим за середній показник по Європейському Союзу (81%) (European Commission 2025d). Така різниця відображає специфіку національного контексту та потребу у більш системному підході до формування довіри громадян до національної політики цифрових трансформацій. Одним з політичних інструментів чеського політикуму може стати оновлена дорожня карта цифрової політики Чехії, яка враховує зростаючі ризики у сфері кіберзахисту, особливо в охороні здоров'я та критичній інфраструктурі, де загрози мають прямий вплив на безпеку громадян і легітимність державних інституцій. Не менш важливим є збільшення бюджетних асигнувань, що засвідчуватимуть усвідомлення масштабності проблеми.

Структура угорської моделі кібербезпеки та стійкості як елементу національної цифрової політики

Угорська модель цифрової кібербезпеки як елемент національної цифрової політики демонструє відносно високий рівень базових навичок серед населення, що свідчить про поступове формування культури цифрової демократії у контексті «Цифрового десятиліття» ЄС. У 2023 р. 74,81% громадян Угорщини здійснили хоча б одну дію для захисту своїх персональних даних в інтернеті, що перевищує середній показник по ЄС (69,55%). Водночас 46,43% населення продемонстрували більш комплексні практики, застосовуючи три й більше заходів безпеки, що дозволяє розглядати їх як носіїв розширених компетентностей у сфері цифрової стійкості. Найбільш поширеною формою захисту стала відмова від використання персональних даних у рекламних цілях (48,71%), що відображає прагнення громадян контролювати власну інформацію та обмежувати комерційні ризики. Натомість перевірка надійності вебресурсів, які запитують персональні дані, залишалася найменш поширеною практикою (31,98%), що свідчить про нерівномірність у розподілі цифрових навичок

та потребу у більш системному підході до їх розвитку (European Commission 2025b). Таким чином, угорський досвід демонструє, що навіть за умов відносно високої базової обізнаності населення, існує потреба у подальшому зміцненні цифрової грамотності та поширенні комплексних практик кіберзахисту.

Угорська модель корпоративної кібербезпеки демонструє певну парадоксальність: з одного боку, підприємства стикаються з меншою кількістю інцидентів, ніж у середньому по ЄС, з іншого – рівень усвідомлення працівниками власних обов'язків у сфері ІКТ-безпеки залишається помітно нижчим. У 2024 р. лише 2,45% угорських компаній повідомили про інциденти, що призвели до недоступності цифрових послуг через атаки програм-вимагачів чи відмову в обслуговуванні, тоді як середній показник по ЄС становив 3,43%. Аналогічно, частка підприємств, які зазнали проблем із апаратними чи програмними збоями, була майже удвічі нижчою, ніж у європейських конкурентів. Попри це, рівень інституційної інтеграції заходів безпеки залишається недостатнім: близько 85% компаній упровадили певні механізми захисту, що нижче за середній показник ЄС, а менше половини повідомили своїх працівників про конкретні зобов'язання у сфері кіберзахисту (European Commission 2025b). Така ситуація свідчить про розрив між формальним упровадженням технічних рішень та розвитком культури цифрової відповідальності, яка є ключовою умовою функціонування цифрової демократії. Показовим є інцидент листопада 2024 р., коли Угорське агентство з оборонних закупівель стало мішенню іноземних хакерів (Reuters 2024). Цей випадок підтверджує, що навіть за відносно низького рівня загальних інцидентів держава та її стратегічні інституції залишаються у фокусі міжнародних груп, які спеціалізуються на отриманні чутливої інформації. На нашу думку, попри авторитарні політичні практики із захисту державних інтересів, угорська модель кібербезпеки потребує посилення технічних стандартів, інституційної структури та освітньої складової.

В частині національної цифрової політики Угорщина демонструє помітний поступ у впровадженні сучасних стандартів інтернет-безпеки, що є важливим елементом реалізації стратегічних орієнтирів «Цифрового десятиліття» ЄС. Найбільш відчутні результати досягнуто у розгортанні протоколу IPv6 для кінцевих користувачів: рівень його застосування становить 47%, що перевищує середній показник по ЄС. Водночас на серверному рівні країна відстає від європейських

стандартів, досягаючи лише 7% проти середнього показника у 17% (European Commission 2025b). Це свідчить про нерівномірність розвитку цифрової інфраструктури, яка потребує подальшого вдосконалення для забезпечення масштабованості, стабільності та безпеки інтернету в умовах вичерпання адресного простору IPv4. Важливим викликом залишається низький рівень впровадження DNSSEC, який у третьому кварталі 2024 р. становив лише 11%, тоді як середній показник по ЄС сягає 47% (European Commission 2025c). Це означає, що механізми автентифікації та захисту в системі доменних імен ще не інтегровані належним чином, що створює додаткові ризики для цифрової стійкості країни.

На законодавчому рівні Угорщина зробила важливий крок, імплементувавши положення Директиви NIS2 у Закон LXIX 2024 р. та відповідні підзаконні акти (National Assembly 2025). Це забезпечує гармонізацію національної правової системи з європейськими стандартами та закладає основу для подальшого розвитку цифрової стійкості. Суспільні настрої демонструють високу підтримку посилення кіберзахисту: 80% х громадян Угорщини переконані, що вдосконалення безпеки цифрових технологій та захисту персональних даних полегшить їхнє щоденне використання цифрових сервісів (European Commission 2025d).

Словацька модель кібербезпеки та цифрової стійкості: лідерство, стратегування та компетентність

У Словаччині рівень цифрової грамотності населення у сфері безпеки даних демонструє поступове зростання, хоча й залишається дещо нижчим за середні показники Європейського Союзу. У 2023 році 63,91% громадян здійснили принаймні одну дію для захисту своїх персональних даних в інтернеті, що свідчить про базове усвідомлення ризиків цифрового середовища. Водночас 69,55% населення застосувала комплексніші практики, виконуючи три й більше заходів, що дозволяє віднести їх до групи з розширеними навичками цифрової безпеки. Найчастіше громадяни обирали відмову від використання персональних даних у рекламних цілях (38,54%), що відображає прагнення контролювати власну інформацію та обмежувати комерційні ризики. Натомість перевірка надійності вебресурсів, де надаються персональні дані, залишалася найменш поширеною практикою (16,97%), що вказує на нерівномірність у розвитку цифрових компетентностей (European Commission 2025c).

Словацький корпоративний сектор у сфері кібербезпеки демонструє відносно стійкі результати, що свідчить про поступове формування культури цифрової відповідальності та узгодження з європейськими орієнтирами «Цифрового десятиліття». У 2024 р. частка підприємств, які зазнали зовнішніх атак, що призвели до недоступності ІКТ-послуг (зокрема програм-вимагачів чи атак відмови в обслуговуванні), становила 2,02%, що хоч і зросло порівняно з 2022 р., проте залишалося нижчим за середній показник по ЄС (European Commission 2025c). Це свідчить про відносну стійкість цифрової інфраструктури країни та ефективність базових механізмів захисту. Більшість словацьких компаній інтегрували заходи кіберзахисту у свою діяльність: понад 87% підприємств застосовують певні інструменти безпеки, що лише трохи поступається середньому рівню ЄС (59,97%) (European Commission 2025c). Особливо важливим є те, що понад 61% компаній інформують своїх працівників про їхні обов'язки у сфері ІКТ-безпеки, перевищуючи середній показник по ЄС. Це свідчить про усвідомлення ролі людського фактора у забезпеченні цифрової стійкості та формування корпоративної культури, де безпека даних стає спільною відповідальністю. Таким чином, словацька модель корпоративної кібербезпеки поєднує відносно низький рівень інцидентів із високою увагою до освітньої та комунікаційної складової.

Наприкінці 2024 р. Словаччина продемонструвала суперечливу динаміку у впровадженні ключових інтернет-стандартів, що мають стратегічне значення для цифрової демократії та реалізації цілей «Цифрового десятиліття» ЄС. З одного боку, країна стала лідером у розгортанні протоколу IPv6 на серверному рівні: понад половина інтернет-сервісів функціонувала через нову версію протоколу, що значно перевищує середній показник по ЄС, що свідчить про високий рівень готовності інституційної та корпоративної інфраструктури до масштабованого та безпечного цифрового середовища. З іншого боку, впровадження IPv6 серед кінцевих користувачів залишалося критично низьким – лише 8 % населення мали доступ до інтернету через цей протокол, що суттєво відстає від середнього рівня ЄС (36%). Така асиметрія між серверною та користувацькою сторонами створює ризики для повноцінної інтеграції країни у європейський цифровий простір, адже саме масове використання IPv6 є передумовою для стійкості та довіри громадян до цифрових сервісів. Ще

одним викликом для Словаччини залишається низький рівень впровадження DNSSEC, лише 24% валідації проти майже половини у середньому по ЄС (European Commission 2025c). Це означає, що механізми автентифікації та захисту в системі доменних імен ще не стали достатньо поширеними, що обмежує можливості країни у забезпеченні цілісності та безпеки глобального кіберпростору. На нашу думку, словацька модель цифрової стійкості демонструє сильні позиції у сфері інституційної та корпоративної інфраструктури, але водночас відставання у користувацькому сегменті та стандартах DNSSEC.

Кібербезпека сьогодні посідає центральне місце у політичному порядку денному Словаччини, що відображає підвищення суспільної чутливості до цифрових ризиків. Зростання масштабів атак, серед яких переважна більшість становлять фішингові кампанії, поєднується з активнішим повідомленням про інциденти, що свідчить про підвищення рівня обізнаності громадян та інституцій. Символічним стало порушення роботи інформаційної системи Управління геодезії, картографії та кадастру у січні 2025 р., що є найбільшим кіберінцидентом у сучасній історії країни, який поставив під сумнів надійність цифрових державних послуг та актуалізував питання їхньої стійкості (Maundrill 2025). Результати опитувань підтверджують суспільний запит на посилення цифрової безпеки: 90% громадян Словаччини переконані, що вдосконалення кіберзахисту та захисту персональних даних значно полегшить їхнє щоденне використання цифрових технологій. Цей показник не лише перевищує середній рівень по ЄС, але й демонструє приріст у 5% порівняно з попередніми роками. Відтак, словацький досвід свідчить про формування нового суспільно-політичного консенсусу довкола позиціонування кібербезпеки як чинника легітимності цифрової демократії.

У межах чинної Стратегії кібербезпеки Словаччини на 2021–2025 рр. (Národný bezpečnostný úrad 2021) реалізується комплекс заходів, спрямованих на підвищення цифрової стійкості держави. До них належать реагування та обробка інцидентів, систематичний моніторинг безпеки й оцінка вразливостей у державному секторі, а також освітні програми для бізнесу, державних службовців і шкіл, які здійснює Національний центр компетенцій. Водночас обмежені повноваження Міністерства інвестицій, регіонального розвитку та інформатизації (MIRRI) у сфері усунення виявлених загроз знижують ефективність політики: міністерство може лише надавати рекомен-

дації, які не завжди виконуються відповідними суб'єктами. Це створює розрив між стратегічними намірами та практичною реалізацією, що є критично важливим у контексті цифрової демократії, де безпека інституцій визначає рівень довіри громадян.

З 2026 р. планується ухвалення нової Стратегії кібербезпеки на 2026–2030 рр., яка розвиватиме попередні напрацювання, але водночас інтегруватиме нові пріоритети та посилюватиме критичні напрями. Вона буде узгоджена з положеннями Директиви NIS2, імплементованої через Закон про кібербезпеку, що набув чинності 1 січня 2025 р. Серед ключових дій передбачено перегляд чинного законодавства для забезпечення відповідності європейським стандартам, розширення функцій урядового Центру операцій з безпеки, який надаватиме послуги ширшому колу організацій, а також реалізацію проєкту «Ахіллес», що здійснюватиме регулярні оцінки вразливостей у державному секторі.

MIRRI також планує створення Служби розвідки про загрози для обміну знаннями та аналітикою між міністерствами, що сприятиме формуванню спільної культури кіберстійкості. Особливий акцент робитиметься на проактивних заходах, зокрема на тестуванні проникнення, яке через обмежені ресурси спершу буде спрямоване на охорону здоров'я та критичну інфраструктуру. Освітня складова залишатиметься пріоритетною: технічний персонал і керівники проходитимуть спеціалізовані навчальні модулі, що забезпечить розвиток компетенцій у сфері цифрової безпеки. Фінансування з європейського Фонду відновлення та стійкості (RRF) дозволить стандартизувати технічні та процедурні рішення, посилити навчання державних службовців і створити систему раннього реагування.

Висновки. Здійснений порівняльний аналіз кібербезпеки та стійкості в структурі цифрової політики країн Вишеградської групи (Польщі, Чеїії, Словаччини та Угорщини) дозволив визначити низку спільних та відмінних рис відповідних національних моделей. Спільним для національних моделей кібербезпеки та цифрової стійкості країн Вишеграду є прагнення інтегрувати власні політики у стратегічні рамки «Цифрового десятиліття» ЄС, де кіберзахист розглядається як ключовий чинник легітимності цифрової демократії. Усі країни визнають кібербезпеку стратегічним пріоритетом, поєднуючи інституційні реформи, правову гармонізацію та освітні програми для громадян і бізнесу. Вони поступово вибудовують інституційну

координацію, створюють спеціалізовані центри та механізми реагування на інциденти, а також інвестують у розвиток цифрових навичок, що формує культуру відповідальності та довіри до цифрових інституцій.

Специфіка кожної національної (польської, чеської, словацької, угорської) моделі кібербезпеки та цифрової стійкості полягає у різних акцентах і політичних контекстах, які визначають їхню роль у структурі цифрової політики. Польська модель вирізняється системністю та багаторівневістю: вона поєднує законодавчі реформи, інституційну координацію та масштабні освітні програми, що створює цілісну архітектуру цифрової стійкості. Її специфіка полягає у значних фінансових інвестиціях у цифрову трансформацію та розбудові спеціалізованих центрів кіберзахисту, які забезпечують узгодженість дій між державою, бізнесом і місцевим самоврядуванням. Чеська модель має особливість у високій суспільній обізнаності та активній участі бізнесу, що формує підґрунтя для демократичної участі громадян у цифровому середовищі. Її специфіка полягає у поєднанні сильної корпоративної культури безпеки з викликами інституційної інтеграції, що полягають у необхідності завершення імплементації Директиви NIS2 та забезпеченням прозорого фінансування та посиленням захисту критичної інфраструктури. Угорська модель відрізняється подвійним характером: з одного боку, вона демонструє прогрес у впровадженні європейських стандартів і технологічних рішень, а з іншого, функціонує в умовах авторитарного режиму, де кібербезпека використовується не лише як інструмент захисту, але й як механізм контролю над суспільством. Її специфіка полягає у поєднанні європейської інтеграції з політичними практиками, що обмежують прозорість та демократичну участь. Специфіка словацької моделі кібербезпеки та цифрової стійкості полягає у поєднанні відносно низького рівня інцидентів у корпоративному секторі з високим рівнем суспільного запиту на посилення захисту цифрових послуг. Словаччина є лідером у впровадженні IPv6 на серверному рівні, але значно відстає у його застосуванні серед кінцевих користувачів, а також демонструє низький рівень валідації DNSSEC порівняно з середнім показником по ЄС. Це створює асиметрію між технічною інфраструктурою та практичними навичками громадян.

References:

1. Barometr cyberbezpieczeństwa (2024). Najważniejsze spostrzeżenia z raportu. https://kpmg.com/pl/pl/home/insights/2024/02/barometr-cyberbezpieczenstwa-2024.html

2. Belas, J., Kliestik, T., Dvorsky, J., Streimikiene, D. (2025). "Exploring gender-based disparities in the digital transformation and sustainable development of SMEs in V4 countries". Journal of Innovation & Knowledge. 10(2):100681.

3. European Commission (2020). The EU toolbox for 5G security. URL: https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security.

4. European Commission (2025). Digital Decade 2025 country reports. Poland. Accompanying the document Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future/ Brussels, 16.6.2025 SWD(2025) 294 final PART 21/27. {COM(2025) 290 final} {SWD(2025) 290 final} {SWD(2025) 291 final} {SWD(2025) 292 final} {SWD(2025) 293 final} {SWD(2025) 295 final}. URL: https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-country-reports.

5. European Commission (2025a). Digital Decade 2025 country reports. Czech Republic. Accompanying the document Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future/ Brussels, 16.6.2025 SWD(2025) 294 final PART 6/27. {COM(2025) 290 final} {SWD(2025) 290 final} {SWD(2025) 291 final} {SWD(2025) 292 final} {SWD(2025) 293 final} {SWD(2025) 295 final}. URL: https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-country-reports.

6. European Commission (2025b). Digital Decade 2025 country reports. Hungary. Accompanying the document Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future/ Brussels, 16.6.2025 SWD(2025) 294 final PART 13/27. {COM(2025) 290 final} {SWD(2025) 290 final} {SWD(2025) 291 final} {SWD(2025) 292

final} {SWD(2025) 293 final} {SWD(2025) 295 final}. URL: https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-country-reports.

7. European Commission (2025c). Digital Decade 2025 country reports. Slovakia. Accompanying the document Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee and the Committee of the Regions State of the Digital Decade 2025: Keep building the EU's sovereignty and digital future {COM(2025) 290 final} {SWD(2025) 290 final} {SWD(2025) 291 final} {SWD(2025) 292 final} {SWD(2025) 293 final} {SWD(2025) 295 final}. URL: https://digital-strategy.ec.europa.eu/en/library/digital-decade-2025-country-reports.

8. European Commission (2025d). Special Eurobarometer 566 on 'the Digital Decade' 2025. URL: https://digital-strategy.ec.europa.eu/en/news-redirect/883227.

9. Fundusze Europejskie na Rozwój Cyfrowy (2024). Cele Programu. URL: https://www.rozwojcyfrowy.gov.pl/strony/dowiedz-sie-wiecej-o-programie/o-programie/

10. Harangozó, G., Fakó, P. (2024). "Relationship between the DESI and the SDG index in the European Union with a special focus on the Visegrad Group countries". Regional Statistics. 14(6): 1187-1221.

11. Horbaczewski, R. (2025). Lokalne Centrum Cyberbezpieczeństwa. URL: https://www.prawo.pl/samorzad/lokalne-centra-cyberbezpieczenstwa-cybercuw,533362.html

12. Komisja Europejska (2025). Europejski Miesiąc Cyberbezpieczeństwa 2025 rozpoczyna się z naciskiem na zagrożenia phishingowe. URL: https://digital-strategy.ec.europa.eu/pl/news/european-cybersecurity-month-2025-kicks-focus-phishing-threats.

13. Maundrill, B (2025). Slovakia Hit by Historic Cyber-Attack on Land Registry. URL: https://www.infosecurity-magazine.com/news/slovakia-hit-by-large-scale/

14. Národný bezpečnostný úrad (2021). Národná stratégia a akčný plán kybernetickej bezpečnosti na roky 2021 až 2025 schválila vláda Slovenskej republiky 7. januára 2021 uznesením č. 5/2021. URL: https://www.nbu.gov.sk/data/att/396.pdf.

15. NASK (2024). Program Firma Bezpieczna Cyfrowo. URL: https://firmabezpiecznacyfrowo.pl/o_programie/

16. NASK (2024a). What Makes Us different? URL: https://www.nask.pl/en/institute/for-science/thinkstat.

17. National Assembly (2025). Act LXIX of 2024 on the cybersecurity of Hungary (as in force on 31 May 2025). URL: https://njt.hu/jogszabaly/en/2024-69-00-00.

18. NUKIB (2021). National Cyber Security Strategy of the Czech Republic 2021-2025. URL: https://nukib.gov.cz/download/publications_en/strategy_action_plan/NSCS_2021_2025_ENG.pdf.

19. NUKIB (2025). Národní strategie kybernetické bezpečnosti. 2026. URL: https://nukib.gov.cz/cs/infoservis/dokumenty-a-publikace/strategie-akcni-plan/

20. Oramus, M. (2024). "Open Data Policy as a Response of the V4 Countries to the Technological Shift". Honour Consciousness, Religion and Gender: Brazilian and Pakistani Lived Experiences in Australia. 60:164.

21. Procházka, G. (2025). Artificial Intelligence and Sustainable Development: Policy Approaches from Visegrad Group Countries. URL: https://www.scilit.com/publications/068f738cd087ea4c017eec98271a91e6.

22. Rada Ministrów (2023). Cyberbezpieczny Samorząd. URL: https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad.

23. Rada Ministrów (2024). Program FENG – Ścieżka SMART. URL: https://www.biznes.gov.pl/pl/portal/004295#1.

24. Rada Ministrów (2024a). Strategia Cyfryzacji Polski do 2035 roku. URL: https://www.gov.pl/web/cyfryzacja/strategia-cyfryzacji-polski-do-2035-roku.

25. Rada Ministrów (2025). Cyberbezpieczny Rząd. URL: https://www.gov.pl/web/cppc/cyberbezpieczny-rzad.

26. Reuters (2024). Hungary's defence procurement agency hacked, government says. November 14. URL: https://www.reuters.com/technology/cybersecurity/hungarys-defence-procurement-agency-hacked-government-says-2024-11-14/

27. Urząd Komunikacji Elektronicznej (2025). Klikam z głową. URL: https://cik.uke.gov.pl/edukacjatop/klikam-z-glowa/

28. VECTO (2024). Cyberbezpieczeństwo w polskich firmach. URL: https://vecto.pl/aktualnosci/artykul?id=263.

29. Zawicki, M. (2024). "The Visegrád Group at the Threshold of the Fourth Industrial Revolution". Honour Consciousness, Religion and Gender: Brazilian and Pakistani Lived Experiences in Australia. 60:1.

Надійшла до редакції / Received: 18.11.2025 *Схвалено до друку / Accepted: 08.12.2025*