https://doi.org/10.15407/sofs2026.02.139
УДК 004.056.55(477)(091)

П.О. МАКАРЕНКО, аспірант
Національний технічний університет
«Харківський політехнічний інститут»
вул. Кирпичова, 2, Харків, 61002, Україна
e-mail: Pavlo.Makarenko@sgt.khpi.edu.ua
https://orcid.org/0009-0002-9728-2456

ЕТАПИ СТАНОВЛЕННЯ НАЦІОНАЛЬНОЇ КРИПТОГРАФІЧНОЇ СИСТЕМИ В УКРАЇНІ (1991—2022)

Стаття присвячена становленню та розвитку національної криптографічної системи в період незалежності України (1991—2022), від створення нормативно-правової бази криптографічного захисту, заснування відповідних навчальних підрозділів у провідних українських університетах до розроблення власних стандартів шифрування та активної участі українських фахівців у провідних світових блокчейн-проєктах. Джерельну базу дослідження склали законодавчі та нормативно-правові акти України у сфері криптографії та кібербезпеки, національні стандарти ДСТУ, технічні специфікації та наукові публікації українських криптографів, інформація з офіційних сайтів функціональних підрозділів НТУУ «КПІ імені Ігоря Сікорського» та НТУ «Харківський політехнічний інститут», офіційна документація та матеріали спеціалізованих видань. Визначено три основні етапи інституційного становлення національної криптографічної системи: перехідний період (1992—2006) — використання пострадянських стандартів і створення Державної технічної комісії при Службі безпеки України (СБУ) і Державної служби спеціального зв'язку та захисту інформації при СБУ; період формування національної системи (2006—2014) — створення Державної служби спеціального зв'язку та захисту інформації України і проведення національного криптографічного

Цитування: Макаренко П.О. Етапи становлення національної криптографічної системи в Україні (1991—2022). *Наука та наукознавство*. 2026. № 2 (132). С. 139—150. https://doi.org/10.15407/sofs2026.02.139

конкурсу; період консолідації та міжнародного визнання (2014—2022) — ухвалення національних стандартів криптографічного захисту та їх подання до ISO/IEC. Особливу увагу приділено участі українських фахівців у світових блокчейн-проєктах (Bitfury, Solana, NEAR Protocol, zkSync, Trust Wallet, WhiteBIT, Hacken), що свідчить про міжнародне визнання вітчизняної криптографічної системи та здатність представників України створювати інноваційні технологічні рішення світового рівня. Встановлено, що українська криптографічна система пройшла шлях від використання пострадянських державних стандартів до створення оригінальних національних алгоритмів та інноваційних рішень світового рівня.

Ключові слова: *національна криптографічна система, захист інформації, криптовалюта, кібербезпека, національна безпека, державні стандарти України, блокчейн, цифрові технології.*

Вступ. Національна криптографічна система України демонструє високий рівень теоретичних і прикладних досліджень. Успіхи українських криптографів у створенні провідних світових блокчейн-платформ свідчать про її високий науковий потенціал. Протягом 1991—2022 рр. українська наукова школа криптографії посіла провідне місце у світовому науковому просторі завдяки створенню національної інституційної системи криптографічної діяльності та розробленню криптографічних стандартів, що уможливило активну участь українських фахівців у світових криптографічних та блокчейн-проєктах. В умовах гібридної війни та постійних кіберзагроз питання криптографічного захисту інформації набуло стратегічного значення для національної безпеки України. Дослідження розвитку національної криптографічної системи дає змогу відтворити етапи її формування і досвід створення національних криптографічних стандартів.

Аналіз досліджень і публікацій. Хоча історія української криптографії привертає увагу вітчизняних істориків науки та інших фахівців, ця тема є відносно новою для науково-історичного аналізу, що зумовлює обмеженість спеціалізованих джерел.

Прикладом комплексного дослідження згаданої теми є колективна монографія [1], де систематизовано значний фактаж щодо розвитку криптографічної діяльності від античності до сучасного етапу. Особливу увагу автори приділили порівняльному аналізу радянської та американської криптографічних систем, що дає змогу зрозуміти стартові умови, в яких формувалася українська система після 1991 р. Але монографія охоплює надзвичайно широкий хронологічний діапазон і містить лише побіжний аналіз важливих аспектів пострадянського етапу розвитку української криптографії, зокрема інституційного будівництва, нормативно-правового регулювання.

Участь українських фахівців у світових блокчейн-проєктах задокументована переважно в медійних, а не наукових джерелах. Видання *Forbes Ukraine* у 2021 р. опублікувало матеріал про *Solana* як блокчейн українського походження[1], де розглянуто біографію засновника Анатолія Яковенка, технічні особливості платформи та її механізм консенсусу *Proof of History*; у 2022 р. — аналітичний огляд українських засновників найбільших блокчейн-проєктів світу[2], де систематизовано інформацію про платформи — *Trust Wallet* (засновник — Віктор Радченко), *Bitfury* (Валерій Вавілов), *Solana* (Анатолій Яковенко), *NEAR Protocol* (Ілля Полосухін), *WhiteBIT* (Володимир Носов), *Hacken* (Дмитро Будорін) та ін., наведено дані про обсяги залучених інвестицій (понад 1 млрд дол. для понад 80 українських *Web3*-стартапів станом на 2022 р.). Видання AIN.UA у 2021 р. опублікувало матеріал про Віктора Радченка — засновника платформи *Trust Wallet*[3]. Але ці матеріали мали переважно інформаційно-популяризаторський характер і не включали історичного аналізу становлення української криптографічної системи як чинника, що забезпечив успіхи українських фахівців у міжнародних технологічних проєктах.

Мета статті — висвітлити результати комплексного історичного аналізу становлення національної криптографічної системи в Україні в період 1991—2022 рр.

Хронологічні межі дослідження (1991—2022) обумовлені специфікою предмета. Нижня межа пов'язана з проголошенням незалежності України та початком формування національної криптографічної системи. Верхня межа визначається початком повномасштабної російської агресії, що кардинально змінило вимоги до національної системи кібербезпеки та криптографічного захисту інформації.

Наукова новизна дослідження полягає у комплексному історичному аналізі становлення української криптографічної системи в період 1991—

---

[1] Антонюк Д. Українець Анатолій Яковенко створює найшвидший у світі блокчейн. Як інвестори заробили на його стартапі Solana понад $1 млрд. *Forbes Ukraine*. 14 грудня 2021. URL: https://forbes.ua/innovations/ukrainets-anatoliy-yakovenko-stvoryue-nayshvidshiy-u-sviti-blokcheyn-yak-investori-zarobili-na-startapi-1-mlrd-14122021-2973 (дата звернення: 15.01.2025).

[2] Мельник Т. Тягне на дно. FTX встигла проінвестувати в засновані українцями Solana, NEAR Protocol і Subsocial. Як їх зачепив крах біржі. *Forbes Ukraine*. 21 листопада 2022. URL: https://forbes.ua/innovations/tyagne-na-dno-birzha-ftx-vstigla-proinvestuvati-v-sotni-startapiv-sered-yakikh-zasnovani-ukraintsyami-solana-near-protocol-i-subsocial-yak-ikh-zachepila-tsya-khvilya-21112022-9914 (дата звернення: 15.01.2025).

[3] «В первую ночь в Долине я спал в машине на холме с сильным туманом». Интервью с украинцем, который продал свой продукт Binance. AIN.UA. 29 марта 2021. URL: https://ain.ua/ru/2021/03/29/kak-ukrainec-prodal-prilozhenie-binance/ (дата звернення: 15.01.2025).

2022 рр., що охоплює три взаємопов'язані напрями: формування нормативно-правової бази та інституційної структури криптографічної діяльності, розроблення національних криптографічних стандартів, інтеграцію українських фахівців у світову блокчейн-індустрію. Вперше проаналізовано комплекс чинників, що забезпечили трансформацію української криптографії від залежності пострадянських систем до міжнародно визнаної системи, здатної створювати інноваційні технологічні рішення світового рівня. Систематизовано внесок українських криптографів у розвиток світових блокчейн-платформ і показано зв'язок між розвитком національної криптографічної системи та успіхами українських фахівців у міжнародних технологічних проєктах.

Методи дослідження. Загальнонаукові: історизму, об'єктивності та всебічності; спеціально-історичні: історико-хронологічний, який став основним у реконструкції головних етапів формування нормативно-правової бази та інституційної структури української криптографічної системи; історико-порівняльний, на базі якого проведено аналіз українських криптографічних стандартів і світових аналогів; історико-системний для з'ясування взаємозв'язків між різними компонентами української криптографічної системи.

Джерельну базу дослідження склали законодавчі та нормативно-правові акти України у сфері криптографії та кібербезпеки, державні стандарти України, технічні специфікації та наукові публікації українських криптографів, інформація з офіційних сайтів функціональних підрозділів НТУУ «Київський політехнічний інститут імені Ігоря Сікорського» та НТУ «Харківський політехнічний інститут», офіційна документація та матеріали спеціалізованих видань.

Результати дослідження та їх обговорення. У момент проголошення незалежності України криптографічна система держави повністю ґрунтувалася на радянських стандартах. Основним державним стандартом шифрування залишався ГОСТ 28147-89, ухвалений у СРСР у 1989 р. Вже 19 серпня 1992 р. постановою Кабінету Міністрів України (КМУ) створено Державну технічну комісію при Службі безпеки України (ДТК при СБУ)[4], яка виконувала функції контролю за технічним захистом інформації. Перехідний період характеризувався складністю адаптації пострадянських криптографічних систем до потреб незалежної держави.

31 серпня 1998 р. постановою КМУ створено Державну службу спеціального зв'язку та захисту інформації при Службі безпеки України

[4] Про утворення Державної технічної комісії при Службі безпеки України: постанова КМУ від 19 серпня 1992 р. № 486. *Зібрання постанов Уряду України*. 1992. № 10. Ст. 238. URL: https://zakon.rada.gov.ua/laws/show/486-92-%D0%BF/print (дата звернення: 15.01.2025).

(ДСТСЗІ СБУ)[5] на базі ліквідованих ДТК при СБУ та Управління урядового зв'язку при КМУ. ДСТСЗІ СБУ отримала широкі повноваження щодо технічного та криптографічного захисту інформації, ліцензування діяльності у цій сфері та сертифікації засобів захисту. У березні 2001 р. постановою КМУ створено спеціальний факультет СБУ в складі Національного технічного університету України «Київський політехнічний інститут (НТУУ «КПІ»)[6] для підготовки фахівців із криптографії та захисту інформації.

23 лютого 2006 р. ухвалено Закон України «Про Державну службу спеціального зв'язку та захисту інформації України»[7]. На виконання цього Закону 1 січня 2007 р. на базі ліквідованого ДСТСЗІ СБУ утворено Державну службу спеціального зв'язку та захисту інформації України (Держспецзв'язку) як центральний орган виконавчої влади зі спеціальним статусом. 27 грудня 2006 р. розпорядженням КМУ[8] на базі спецфакультету СБУ в складі НТУУ «КПІ» створено Інститут спеціального зв'язку та захисту інформації. 5 жовтня 2017 р. ухвалено Закон України «Про основні засади забезпечення кібербезпеки України»[9]. Нарешті, 26 серпня 2021 р. указом Президента України[10] затверджено Стратегію кібербезпеки України на період до 2025 р.

Найважливішим досягненням стало ухвалення національних стандартів криптографічного захисту. 29 грудня 2014 р. наказом Мінеконом-

---

[5] Про утворення Державної служби спеціального зв'язку та захисту інформації при Службі безпеки України: Указ Президента України від 31 серпня 1998 р. № 954/98. URL: https://zakon.rada.gov.ua/laws/show/954/98/print (дата звернення: 15.01.2025).

[6] Про створення спеціального факультету Служби безпеки України у складі Національного технічного університету України «Київський політехнічний інститут»: Постанова КМУ від 22 березня 2001 р. № 269. *Офіційний вісник України*. 2001. № 12. Ст. 491. URL: https://zakon.rada.gov.ua/laws/show/269-2001-%D0%BF/print (дата звернення: 15.01.2025).

[7] Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV. *Відомості Верховної Ради України*. 2006. № 30. Ст. 258. URL: https://zakon.rada.gov.ua/laws/show/3475-15 (дата звернення: 15.01.2025).

[8] Про утворення Інституту спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут»: Розпорядження КМУ від 27 грудня 2006 р. № 658-р. *Офіційний вісник України*. 2007. № 1. Ст. 31. URL: https://zakon.rada.gov.ua/laws/show/658-2006-%D1%80/print (дата звернення: 15.01.2025).

[9] Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-15/print (дата звернення: 15.01.2025).

[10] Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26 серпня 2021 р. № 447/2021. *Офіційний вісник України.* 2021. № 67. Ст. 2352. URL: https://zakon.rada.gov.ua/laws/show/447/2021/print (дата звернення: 15.01.2025).

розвитку[11] ухвалено ДСТУ 7624:2014 «Алгоритм симетричного блокового перетворення»[12], який визначав алгоритм симетричного блокового шифрування «Калина». Стандарт розроблено задля поступової заміни міждержавного стандарту ДСТУ ГОСТ 28147:2009. Алгоритм «Калина» створено колективом українських криптографів під керівництвом Р. Олійникова та І. Горбенка у результаті національного криптографічного конкурсу, що тривав з 2007 по 2010 рр. [2]. До конкурсу подано 17 алгоритмів від різних наукових колективів України і переможцем обрано «Калину».

2 грудня 2014 р. наказом Мінекономрозвитку[13] ухвалено ДСТУ 7564:2014 «Функція гешування»[14]: криптографічну геш-функцію «Купина» для забезпечення цілісності даних та електронного цифрового підпису.

Порівняльний аналіз ДСТУ 7624:2014 з провідними світовими стандартами демонструє конкурентоспроможність українських розробників. Американський стандарт AES[15], що ґрунтується на алгоритмі *Rijndael* [3], підтримує лише фіксований розмір блоку 128 біт. Український стандарт «Калина» є більш гнучким, оскільки підтримує три варіанти розмірів блоків (128, 256, 512 біт) та відповідні розміри ключів [4]). Офіційно стандартизовано п'ять варіантів: «Калина-128/128», «Калина-128/256», «Калина-256/256», «Калина-256/512», «Калина-512/512». Криптоаналіз показав, що запас криптографічної стійкості «Калини» перевищував мінімально необхідний рівень [5].

Основні етапи становлення національної криптографічної системи наведено у табл. 1.

Становлення української криптографічної системи нерозривно пов'язане з розвитком системи підготовки фахівців. Начальником Інституту спеціального зв'язку та захисту інформації при НТУУ «КПІ імені Ігоря Сікорського»[16] з моменту його створення є О.О. Пучков, кандидат філо-

[11] Про прийняття національного стандарту України: Наказ Міністерства економічного розвитку і торгівлі України від 29 грудня 2014 р. № 1484. URL: https://zakon.rada.gov.ua/rada/show/v1484731-14/print (дата звернення: 15.01.2025).

[12] ДСТУ 7624:2014 «Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення». Київ: Мінекономрозвитку України, 2015.

[13] Про прийняття національного стандарту України: Наказ Міністерства економічного розвитку і торгівлі України від 2 грудня 2014 р. № 1431. URL: https://zakon.rada.gov.ua/rada/show/v1431731-14/print (дата звернення: 15.01.2025).

[14] ДСТУ 7564:2014 «Інформаційні технології. Криптографічний захист інформації. Функція гешування». Київ: Мінекономрозвитку України, 2015.

[15] FIPS PUB 197. Advanced Encryption Standard (AES). National Institute of Standards and Technology, 2001. URL: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf (дата звернення: 15.01.2025).

[16] Офіційний сайт Інституту спеціального зв'язку та захисту інформації при НТУУ «КПІ імені Ігоря Сікорського». URL: https://iszzi.kpi.ua/ (дата звернення: 15.01.2025).

Таблиця 1. **Основні етапи становлення національної криптографічної системи України (1992—2020)**

Рік	Подія	Значення
1992	Створення Державної технічної комісії при Службі безпеки України	Початок формування національної системи контролю за захистом інформації
1998	Створення Державної служби спеціального зв'язку та захисту інформації при Службі безпеки України	Об'єднання функцій технічного захисту та урядового зв'язку
2001	Створення спецфакультету СБУ в НТУУ «КПІ»	Початок підготовки фахівців із криптографії
2006	Ухвалення Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» (Держспецзв'язку)	Створення правової основи діяльності у сфері криптографічного захисту
2007	Створення Держспецзв'язку	Формування центрального органу в сфері кібербезпеки
2014	Ухвалення ДСТУ 7624:2014 та ДСТУ 7564:2014	Створення національних криптографічних стандартів
2017	Ухвалення Закону України «Про основні засади забезпечення кібербезпеки України»	Формування комплексної системи кібербезпеки держави
2020	Подання стандартів ДСТУ 7624:2014 та ДСТУ 7564:2014 до *ISO/IEC*	Міжнародне визнання української криптографічної системи
2021	Затвердження Стратегії кібербезпеки України на період до 2025 р.	Затвердження Стратегії кібербезпеки України на 2021—2025 рр. як пріоритетного напряму забезпечення кібербезпеки держави

Джерело: складено автором за даними нормативно-правових актів України у сфері криптографії та кібербезпеки.

софських наук, професор, бригадний генерал. Інститут здійснював підготовку бакалаврів, магістрів і докторів філософії за спеціальностями «Кібербезпека» й «Інформаційні системи та технології», проводив наукові дослідження у сфері криптографії, захисту інформації та кібербезпеки, співпрацював з Держспецзв'язку в розробленні національних стандартів.

2 серпня 1999 р. у складі НТУУ «КПІ» створено кафедру інформаційної безпеки [17], науковим керівником якої став О.М. Новіков, доктор технічних наук, професор, директор Навчально-наукового Фізико-технічного ін-

[17] Офіційний сайт кафедри інформаційної безпеки при НТУУ «КПІ імені Ігоря Сікорського». URL: https://is.ipt.kpi.ua/is/istoriya/ (дата звернення: 15.01.2025).

ституту КПІ ім. Ігоря Сікорського, член-кореспондент НАН України, заслужений діяч науки і техніки України. О.М. Новіков опублікував близько 300 наукових праць, зокрема монографію «Моделі та методи кібернетичного захисту інформаційно-комунікаційних систем на основі логіко-ймовірнісного підходу» [6].

30 березня 2000 р. в НТУУ «КПІ» створено кафедру математичних методів захисту інформації (ММЗІ)[18]. З моменту заснування і до вересня 2021 р. кафедру очолював М.М. Савчук, доктор фізико-математичних наук, доцент, член-кореспондент НАН України, лауреат Державної премії України в галузі науки і техніки — один із провідних учених України у сфері криптографії. Від вересня 2021 р. виконувачем обов'язків завідувача кафедри є С.В. Яковлєв, кандидат технічних наук, лауреат Премії Президента для молодих вчених, який захистив дисертацію на тему «Аналітичні оцінки стійкості немарковських блокових шифрів до диференціального криптоаналізу». Кафедра ММЗІ зосередилася на розробленні математичних методів криптографічного захисту інформації, дослідженнях у сфері комбінаторного аналізу, симетричної та асиметричної криптографії, криптоаналізу блокових шифрів та *ARX*-криптосистем.

11 січня 2022 р. в Національному технічному університеті «Харківський політехнічний інститут» (НТУ «ХПІ») створено кафедру кібербезпеки та інформаційних технологій[19], яку очолив С. П. Євсеєв, доктор технічних наук, професор. На кафедрі працює 11 викладачів, з них три доктори технічних наук, п'ять кандидатів технічних наук, три професори, вісім доцентів. Наукові дослідження на кафедрі зосереджені на постквантових алгоритмах на основі криптокодових конструкцій, методології захисту кіберфізичних систем та об'єктів критичної інфраструктури. Кафедра є співорганізатором міжнародного конгресу *Human-Computer Interaction, Optimization and Robotic Applications* (*IEEE*, 1—3 червня 2023 р., м. Анкара, Туреччина) та Міжнародної конференції «Інформаційна безпека та інформаційні технології» у межах форуму «Цифрова реальність» (листопад 2023 р., Харків, Україна). Кафедра активно співпрацює з провідними ІТ-компаніями: *Distributed Lab*, *Сайфер*, *Microcrypt Technologies*.

Паралельно з державною криптографією в Україні розвивалася приватна криптографічна діяльність, зосереджена навколо блокчейн-технологій та криптовалют. Українські фахівці активно долучилися до світових блокчейн-проєктів. Валерій Вавілов заснував у 2011 р. компанію *Bitfury* — одного з найбільших виробників обладнання для майнінгу *Bitcoin* і провайдера блокчейн-інфраструктури[20].

[18] Офіційний сайт кафедри математичних методів захисту інформації при НТУУ «КПІ імені Ігоря Сікорського». URL: https://kpi.ua/mmzi (дата звернення: 15.01.2025).

[19] Офіційний сайт кафедри кібербезпеки та захисту інформації НТУ «ХПІ». URL: https://cybersecurity.khpi.edu.ua/ (дата звернення: 15.01.2025).

[20] Мельник Т. Тягне на дно. FTX встигла проінвестувати в засновані українцями Solana, NEAR Protocol і Subsocial…

Таблиця 2. **Участь українських фахівців у провідних світових блокчейн-проєктах**

Проєкт	Засновник (українець)	Рік створення	Напрям діяльності
Bitfury	Валерій Вавілов	2011	Виробництво обладнання для майнінгу *Bitcoin*
Solana	Анатолій Яковенко	2017	Високопродуктивна блокчейн-платформа
NEAR Protocol	Ілля Полосухін, Олександр Скіданов	2018	Масштабована платформа для *dApps*
Trust Wallet	Віктор Радченко	2017	Криптовалютний гаманець
zkSync	Алекс Гловер, Алекс Власов	2019	Масштабування *Ethereum* через *zkSNARKs*
WhiteBIT	Володимир Носов	2018	Криптовалютна біржа
Hacken	Дмитро Будорін	2017	Аудит безпеки блокчейн-проєктів

Джерело: складено автором за даними [Антонюк Д. Українець Анатолій Яковенко створює найшвидший у світі блокчейн…; Мельник Т. Тягне на дно. FTX встигла проінвестувати в засновані українцями Solana, NEAR Protocol і Subsocial…; «В первую ночь в Долине я спал в машине на холме с сильным туманом»…].

Анатолій Яковенко у 2017 р. опублікував технічний опис проєкту *Solana* [7] — високопродуктивного блокчейну з інноваційним механізмом консенсусу *Proof of History* (*PoH*). *Solana* стала однією з найшвидших блокчейн-платформ у світі[21]. Ілля Полосухін та Олександр Скіданов стали співзасновниками *NEAR Protocol* — масштабованої платформи для децентралізованих додатків (*dApps*), де використано технологію *sharding* для досягнення високої пропускної здатності[22]. Віктор Радченко у листопаді 2017 р. заснував *Trust Wallet* — некастодіальний мультивалютний криптовалютний гаманець, придбаний у липні 2018 р. біржею *Binance*. *Trust Wallet* підтримував понад 160 блокчейнів і майже 4,5 млн токенів[23]. Алекс Гловер та Алекс Власов стали співзасновниками *Matter Labs* — компанії, що розробила *zkSync*, рішення для масштабування *Ethereum* на основі технології *zero-knowledge proofs*[24]. Володимир Носов

[21] Антонюк Д. Українець Анатолій Яковенко створює найшвидший у світі блокчейн…

[22] Мельник Т. Тягне на дно. FTX встигла проінвестувати в засновані українцями Solana, NEAR Protocol і Subsocial…

[23] «В первую ночь в Долине я спал в машине на холме с сильным туманом»...

[24] Мельник Т. Тягне на дно. FTX встигла проінвестувати в засновані українцями Solana, NEAR Protocol і Subsocial…

у 2018 р. заснував *WhiteBIT* — одну з найбільших європейських централізованих криптовалютних бірж, що отримала ліцензії у кількох європейських юрисдикціях[25]. Дмитро Будорін у 2017 р. створив у Києві компанію *Hacken* — міжнародного лідера з розроблення інфраструктури безпеки для блокчейну, яка провела аудит понад 1200 проєктів і майже 50 криптобірж[26]. Відомості про участь українських фахівців у провідних блокчейн-проєктах систематизовано у табл. 2.

За оцінками видання *Forbes Ukraine*, понад 80 українських *Web3*-стартапів станом на 2022 р. залучили більше 1 млрд дол. інвестицій. Успіхи українських криптографів у світових блокчейн-проєктах свідчать про міжнародне визнання української криптографічної школи та здатність її членів розробляти інноваційні технологічні рішення світового рівня.

Початок повномасштабної російської агресії у лютому 2022 р. створив безпрецедентні виклики для української криптографії та кібербезпеки. Національна система кібербезпеки, побудована на основі вітчизняних стандартів ДСТУ 7624:2014 та ДСТУ 7564:2014, забезпечувала захист державних комунікацій та критичної інформації. Водночас війна стимулювала розвиток нових напрямів, зокрема у сфері постквантових криптографічних алгоритмів.

Висновки і перспективи подальших досліджень. Дослідження трансформації національної криптографічної системи в Україні в період 1991—2022 рр. дало змогу встановити, що за три десятиліття Україна здійснила перехід від повної залежності від пострадянських криптографічних систем (ГОСТ 28147-89) до створення власної національної школи криптографії з оригінальними стандартами ДСТУ 7624:2014 («Калина») та ДСТУ 7564:2014 («Купина»), які за технічними характеристиками не поступалися провідним світовим аналогам.

Визначено три основні етапи інституційного становлення національної криптографічної системи: перехідний період (1992—2006) — використання пострадянських стандартів та створення ДТК при СБУ і ДСТСЗІ СБУ; період формування національної системи (2006—2014) — створення Держспецзв'язку та проведення національного криптографічного конкурсу; період консолідації та міжнародного визнання (2014—2022 рр.) — ухвалення національних стандартів криптографічного захисту та їх подання до *ISO/IEC*. Доведено, що успіхи українських криптографів у світових блокчейн-проєктах (*Bitfury*, *Solana*, *NEAR Protocol*, *zkSync*, *Trust Wallet*, *WhiteBIT*, *Hacken*) із залученням понад 1 млрд дол. інвестицій стали наслідком розвитку національної криптографічної сис-

[25] Мельник Т. Тягне на дно. FTX встигла проінвестувати в засновані українцями Solana, NEAR Protocol і Subsocial…

[26] Там само.

теми та свідченням здатності українських спеціалістів створювати інноваційні технологічні рішення світового рівня.

Подальші дослідження будуть присвячені питанням розвитку постквантових криптографічних алгоритмів в Україні після 2022 р. в умовах посиленого кіберпротистояння; розвитку національних криптографічних систем країн Центральної та Східної Європи у пострадянський період; впливу повномасштабної російської агресії на трансформацію системи кібербезпеки та прискорення впровадження нових криптографічних рішень у секторах критичної інфраструктури.

СПИСОК ЛІТЕРАТУРИ

1. Історія криптології & секретного зв'язку / Відп. ред. Потій О. Київ: ІСЗЗІ КПІ ім. Ігоря Сікорського, 2022. 548 с.
2. Yakovenko A. Solana: A new architecture for a high performance blockchain. White paper. 2017. URL: https://solana.com/solana-whitepaper.pdf (дата звернення: 15.01.2025).
3. Ruzhentsev V., Sokurenko V., Ulyanchenko Y. Analysis of probabilities of differentials for block cipher "Kalyna" (DSTU 7624:2014). *Eastern-European Journal of Enterprise Technologies*. 2018. Vol. 4. No. 9 (94). P. 14—19. https://doi.org/10.15587/1729-4061.2018.139682
4. Oliynykov R., Gorbenko I., Kazymyrov O., Ruzhentsev V., Kuznetsov O., Gorbenko Y., et al. A New Encryption Standard of Ukraine: The Kalyna Block Cipher. *Cryptology ePrint Archive*. 2015. Paper 2015/650. URL: https://eprint.iacr.org/2015/650 (дата звернення: 15.01.2025).
5. Daemen J., Rijmen V. The Design of Rijndael: AES — The Advanced Encryption Standard. Berlin: Springer-Verlag, 2002. 238 p.
6. Новіков О.М., Родіонов А.Н., Тимошенко А.А. Моделі та методи кібернетичного захисту інформаційно-комунікаційних систем на основі логіко-ймовірнісного підходу. Київ: НТУУ «КПІ», 2015. 274 с.
7. Oliynykov R., Gorbenko I., Dolgov V., Ruzhentsev V. Results of Ukrainian national public cryptographic competition. *Tatra Mountains Mathematical Publications*. 2010. Vol. 47. No. 1. P. 99—113. https://doi.org/10.2478/v10127-010-0033-6

REFERENCES

1. Potii, O. (Ed.). (2022). *A history of cryptology & secret communications*. Kyiv: Institute for Special Communications and Protection of Information, National Technical University "Igor Sikorsky Kyiv Polytechnic Institute" [in Ukrainian].
2. Yakovenko, A. (2017). Solana: A new architecture for a high performance blockchain. White paper. URL: https://solana.com/solana-whitepaper.pdf (last accessed: 15.01.2025).
3. Ruzhentsev, V., Sokurenko, V., & Ulyanchenko, Y. (2018). Analysis of probabilities of differentials for block cipher "Kalyna" (DSTU 7624:2014). *Eastern-European Journal of Enterprise Technologies*, 4 (9), 14—19. https://doi.org/10.15587/1729-4061.2018.139682
4. Oliynykov, R., Gorbenko, I., Kazymyrov, O., Ruzhentsev, V., Kuznetsov, O., Gorbenko, Y., et al. (2015). A New Encryption Standard of Ukraine: The Kalyna Block

Cipher. *Cryptology ePrint Archive*, Paper 2015/650. URL: https://eprint.iacr.org/2015/650 (last accessed: 15.01.2025).
5. Daemen, J., & Rijmen, V. (2002). *The Design of Rijndael: AES — The Advanced Encryption Standard*. Berlin: Springer-Verlag.
6. Novikov, O.M., Rodionov, A.N., & Tymoshenko, A.A. (2015). *Models and methods of cybernetic protection of information and communication systems, based on the logic-probability approach.* Kyiv: National Technical University "Igor Sikorsky Kyiv Polytechnic Institute" [in Ukrainian].
7. Oliynykov, R., Gorbenko, I., Dolgov, V., & Ruzhentsev, V. (2010). Results of Ukrainian national public cryptographic competition. *Tatra Mountains Mathematical Publications*, 47 (1), 99—113. https://doi.org/10.2478/v10127-010-0033-6

Одержано / Received 03.02.2026
Прорецензовано / Revised 22.02.2026
Підписано до друку / Accepted 25.05.2026

P.O. Makarenko, post-graduate student
National Technical University "Kharkiv Polytechnic Institute"
2, Kyrpychov str., Kharkiv, 61002, Ukraine
e-mail: Pavlo.Makarenko@sgt.khpi.edu.ua
https://orcid.org/0009-0002-9728-2456

THE FORMATIVE STAGES OF THE NATIONAL CRYPTOGRAPHIC SYSTEM IN UKRAINE (1991—2022)

The article focuses on the formation and development of the Ukrainian cryptographic system during Ukraine's independence period (1991—2022), from the establishment of a regulatory framework for cryptographic protection and the founding of relevant academic departments in leading Ukrainian universities to the development of national encryption standards and the active participation of Ukrainian specialists in leading global blockchain projects. The research sources included Ukrainian legislative and regulatory acts in the field of cryptography and cybersecurity, State Standards of Ukraine, technical specifications and scientific publications of Ukrainian cryptographers, information from official websites of the National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute" and the National Technical University "Kharkiv Polytechnic Institute", official documentation and materials from specialized publications. Three main phases in the institutional formation of the national cryptographic system were identified: the transitional period (1992—2006 — using post-Soviet standards and establishing the State Technical Commission under the Security Service of Ukraine (SCU) and the State Service of Special Communications and Information Protection under SCU; the period of national system formation (2006—2014) — establishing the State Service of Special Communications and Information Protection of Ukraine and holding the national cryptographic competition; the period of consolidation and international recognition (2014—2022) — adopting national cryptographic protection standards, with their submission to ISO/IEC. Emphasis is placed on the Ukrainian specialists' involvement in global blockchain projects (Bitfury, Solana, NEAR Protocol, zkSync, Trust Wallet, WhiteBIT, Hacken), demonstrating international recognition of the Ukrainian cryptographic system and the ability of Ukrainians to create innovative world-class technological solutions. It was found that the Ukrainian cryptographic system evolved from using post-Soviet state standards to creating original national algorithms and globally competitive innovative solutions.

Keywords: *Ukrainian cryptographic system, information protection, cryptocurrency, cybersecurity, national security, Ukrainian state standards, blockchain, digital technologies.*