УДК 004.056.55:530.145:004.77 DOI https://doi.org/10.35546/kntu2078-4481.2025.4.2.15

О. А. МЕЛЬНИКОВА
кандидат технічних наук,
доцент кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0000-0001-8843-9648

С. В. ГРАСМІК
студентка бакалаврату кафедри безпеки інформаційних технологій
Харківський національний університет радіоелектроніки
ORCID: 0009-0008-5521-9831

СТАНОВЛЕННЯ ТА РОЗВИТОК КВАНТОВО-СТІЙКИХ КРИПТОГРАФІЧНИХ ТЕХНОЛОГІЙ У НІМЕЧЧИНІ

У статті досліджено сучасні підходи Німеччини до переходу на квантово-стійкі криптографічні технології в умовах зростання ризиків, пов'язаних з розвитком квантових обчислень. Розглянуто фактори, що зумовлюють необхідність відмови від класичних криптографічних алгоритмів, уразливих до квантових атак, та проаналізовано нормативні, технічні й організаційні кроки, які здійснює Федеральне відомство з безпеки інформаційних технологій Німеччини (BSI) для формування національної стратегії переходу.

Особливу увагу приділено криптографічним механізмам, які визначаються перспективними для довгострокового захисту, зокрема кодовим схемам, хеш-орієнтованим підписам та решітковим алгоритмам обміну ключами. Окреслено їхні ключові властивості, можливі сфери застосування та обмеження. Додатково розглянуто роль гібридних криптографічних конструкцій як проміжного інструмента забезпечення сумісності між класичними та постквантовими алгоритмами.

Проаналізовано готовність німецького ринку до впровадження квантово-стійких рішень, зокрема виклики, пов'язані з модернізацією апаратного забезпечення, складністю оновлення вбудованих систем та потребою у криптографічній гнучкості. Підкреслено значення міждержавної координації в межах Європейського Союзу та необхідність гармонізації стандартів для забезпечення узгодженого рівня безпеки.

Зроблено висновок, що Німеччина формує системний, стратегічно орієнтований підхід до впровадження постквантової криптографії, поєднуючи наукові дослідження, технічну стандартизацію та практичну взаємодію з промисловістю. Така модель демонструє ефективний приклад підготовки до майбутніх квантових загроз та може бути використана як основа для формування аналогічних стратегій в інших країнах.

Ключові слова: *постквантова криптографія, квантові обчислення, квантові загрози, криптографічні стандарти, Classic McEliece, XMSS, SPHINCS+, ML-KEM, гібридні схеми, BSI, інформаційна безпека, критична інфраструктура.*

O. A. MELNYKOVA
Candidate of Technical Sciences,
Associate Professor at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0000-0001-8843-9648

S. V. HRASMIK
Bachelor's Student at the Department of Information Technology Security
Kharkiv National University of Radio Electronics
ORCID: 0009-0008-5521-9831

FORMATION AND DEVELOPMENT OF QUANTUM-RESISTANT CRYPTOGRAPHIC TECHNOLOGIES IN GERMANY

The article examines modern approaches taken by Germany in its transition to quantum-resistant cryptographic technologies amid growing risks associated with the development of quantum computing. It considers the factors that necessitate abandoning classical cryptographic algorithms vulnerable to quantum attacks and analyzes the regulatory,

technical, and organizational steps undertaken by the Federal Office for Information Security of Germany (BSI) to form a national transition strategy.

Particular attention is given to cryptographic mechanisms considered promising for long-term protection, including code-based schemes, hash-based signatures, and lattice-based key exchange algorithms. Their key properties, potential areas of application, and limitations are outlined. Additionally, the role of hybrid cryptographic constructions as an intermediate tool for ensuring compatibility between classical and post-quantum algorithms is examined.

The readiness of the German market to implement quantum-resistant solutions is analyzed, including challenges related to hardware modernization, the complexity of updating embedded systems, and the need for cryptographic flexibility. The importance of interstate coordination within the European Union and the necessity of standard harmonization to ensure a consistent level of security are emphasized.

It is concluded that Germany is forming a systematic, strategically oriented approach to the implementation of post-quantum cryptography, combining scientific research, technical standardization, and practical cooperation with industry. This model demonstrates an effective example of preparing for future quantum threats and can serve as a foundation for developing similar strategies in other countries.

Key words: *post-quantum cryptography, quantum computing, quantum threats, cryptographic standards, Classic McEliece, XMSS, SPHINCS+, ML-KEM, hybrid schemes, BSI, information security, critical infrastructure.*

Постановка проблеми

Стрімкий розвиток квантових обчислень має вплив на уявлення довгострокової безпеки сьогоднішніх криптографічних систем.

Наразі криптографія з відкритим ключем широко використовується для захисту наших даних. Вона є одними із надійніших можливих варіантів на сьогоднішній день, але останні роки ведуться дослідження, які можуть привести до загрози – квантового комп'ютера, який буде здатний зламувати традиційні схеми, наприклад такі як RSA і ECC.

Квантові алгоритми ще не досягли промислової реалізації, але наявні оцінки ризиків на те, що продовження використання класичних криптографічних механізмів може призвести до створення вразливості для державних інформаційних систем, бізнесу, критичної інфраструктури. Особливо в небезпеці дані, що мають довгострокову цінність. "Захопи зараз – розшифруй потім" – принцип при якому інформацію перехоплюють та зберігають до можливості її розшифрування за допомогою квантових обчислювальних систем необхідної потужності.

Таким чином проблема полягає у необхідності переходу до криптографічних рішень, стійких до квантових атак, та у формуванні нормативної, технологічної і організаційної основи для цього переходу. Федеральне відомство з безпеки інформаційних технологій Німеччини визначає підготовку до переходу на нове покоління криптографічних стандартів як пріоритет державної політики, оскільки захист інформації має бути гарантований у перспективі десятиліть.

Аналіз останніх досліджень і публікацій

Дослідження у сфері постквантової криптографії охоплюють широкий спектр питань – від математичних основ криптографічних алгоритмів до аналізу стану квантових технологій, технологічних рекомендацій і стратегічних підходів до переходу на нові стандарти захисту інформації. Одним із фундаментальних напрямів є криптографія на основі решіток, якій приділяється значна увага в сучасних наукових роботах. У дослідженні аналізу решіткових задач, детально описано властивості задач LWE та SIS, обґрунтовуючи їх придатність як основи для стійких криптографічних механізмів, що не дає можливості їх зламати за допомогою квантових алгоритмів. [1]

В огляді розвитку квантових комп'ютерів зазначено, що хоча практичні машини, які здатні зламувати широко застосовані схеми, ще не створені, темпи розвитку вказують на потребу завчасної підготовки використовування нових алгоритмів. [2] Більш стратегічне бачення цих ризиків представлене у документах, де визначено ключові напрями захисту від квантових загроз та сформовано базові принципи забезпечення криптографічної стійкості на майбутні роки. [3]

У низці технічних рекомендацій систематизовано параметри безпеки, придатні до практичного використання, наведено порівняння криптографічних схем та окреслено їхню ефективність залежно від застосування. Документи серії TR-02102 містять узагальнені вимоги до симетричних алгоритмів, хеш-функцій, цифрових підписів, а також рекомендації щодо параметрів до та після переходу на постквантові стандарти. [4-7]

Окрема частина досліджень стосується питань гібридних криптографічних конструкцій, які поєднують класичні та постквантові алгоритми. У технічних документах щодо цього методу описано можливості комбінування алгоритмів електронного підпису та обмінів ключів, що підвищує стійкість системи до невизначеностей, пов'язаних із подальшим розвитком криптоаналізу. [8]

У роботах, які орієнтовані на практичне впровадження, наголошується наголошується на можливості криптографічної гнучкості, яка дозволяє системам адаптуватися до майбутніх змін без значних технічних витрат. [9-10]

Інша сторона досліджень – готовність ринку до переходу на постквантові алгоритми. З опитувань та аналізу підкреслюється, що сфери з високими регуляторними вимогами, такі як фінанси, охорона здоров'я та телекомунікації, демонструють найбільшу зацікавленість у впровадженні нових стандартів. [11]

У спільних європейських документах підкреслюється важливість координації між державами та формування загальних підходів до вибору алгоритмів, вимог до їх впровадження та строки виконання. Такі документи створюють основу для формування єдиної криптографічної інфраструктури Європи та визначають роль національних установ у забезпеченні безпеки цифрового простору. [12]

Узагальнення цих робіт демонструє, що сучасні дослідження постквантової криптографії охоплюють як фундаментальні математичні аспекти, так і прикладні організаційні питання. Наявний обсяг робіт показує комплексне уявлення про перспективні криптографічні алгоритми, потенційні ризики та вимоги до майбутньої інфраструктури захисту.

Формулювання мети дослідження

Метою дослідження є аналіз підходів, які застосовуються у Німеччині для забезпечення криптографічної стійкості в умовах розвитку квантових обчислень. Дослідження спрямоване на визначення ключових аспектів та рекомендацій, що стосуються математичних основ квантово-стійких алгоритмів, аналізу підходів до впровадження гібридних криптографічних механізмів як перехідного етапу, розглянути участь Німеччини у формуванні стратегій постквантового захисту.

Викладення основного матеріалу дослідження

Розвиток квантових технологій сформував новий клас криптографічних ризиків, пов'язаний з тим, що більшість існуючих алгоритмів базується на задачах, для яких ефективні квантові методи розв'язання. Математичний фундамент квантових атак давно встановлений: алгоритм Шора, який демонструє можливість поліноміального розв'язання задач факторизації цілих чисел і обчислення дискретного логарифма, використовуючи квантову суперпозицію та властивість періодичних функцій. Саме ці задачі є основою безпеки RSA, Diffie-Hellman та криптографії на еліптичних кривих, тому в довгостроковій перспективі вони не можуть вважатися надійними. Хоча практичні квантові комп'ютери ще не мають такої сили, сам факт їх існування є загрозою, що носить не гіпотетичний, а технологічно обґрунтований характер.

Існуючі квантові комп'ютери належать до класу NISQ-систем, що характеризується невеликою кількістю кубітів, високим рівнем шумів і значним обмеженням в реалізації складних квантових схем. Технологічні бар'єри, зокрема недостатня когерентність кубітів і складність корекції квантових помилок, залишаються ключовими факторами, що стримують створення криптографічно релевантних квантових комп'ютерів. Для реалізації атак на сучасні криптографічні системи необхідні тисячі логічних кубітів, підтриманих мільйонами фізичних кубітів. Такі масштаби поки є неможливими, однак світові тенденції – це активні інвестиції, розвиток промислових платформ, поява хмарного доступу до квантових систем – свідчать про швидке наближення наступних етапів. Також підкреслюється, що саме невизначеність у темпах розвитку технології робить завчасну підготовку до переходу необхідною.

Криптографічні механізми, рекомендовані для переходу

Classic McEliece

Одним із ключових квантово-стійких механізмів, які BSI визначає пріоритетними для переходу на постквантові стандарти, є схема шифрування Classic McEliece, що належить до класу кодових криптосистем. Її стійкість базується на складності задач декодування лінійних кодів, що вважається надійною як проти класичних, так і проти квантових атак.

На відміну від більшості сучасних криптосистем, які спираються на дискретні логарифми або факторизацію, криптологія на основі кодів не піддається прискоренню за допомогою кантових алгоритмів. Саме це зробило McEliece одним із найстабільніших механізмів для довгострокового захисту криптографічних даних та інформаційних систем.

Схема Classic McEliece використовує побудову з приватним Goppa-кодом та випадковим лінійним перетворенням, що маскує структуру цього коду у відкритий ключ.Криптосистема складається з генерації ключів, шифрування та розшифруання.

При генерації ключів формується приватний Goppa-код із певним параметром розміру та ступенем полінома. Відкритий ключ утворюється як матриця генератора коду, замаскованого випадковими перестановками та лінійними перетвореннями.

На етапі шифрування повідомлення кодується за допомогою відкритого ключа з додаванням контрольованої кількості помилок.

При розшифруванні приватне знання структури Goppa-коду дозволяє ефективно виправити помилки та відновити початкове повідомлення.

Перевагами даного механізму є насамперед довгострокова безпека, бо механізм зберігає стійкість до відомих на сьогоднішній день типів квантових атак. Також проблема декодування випадкових лінійних кодів все ще залишається достатньо складною.

Основним недоліком є розмір відкритих ключів, що ускладнює інтеграцію в мобільні або ресурсно-обмежні системи.

XMSS та SPHINCS+

Хеш-орієнтовані схеми цифрового підпису розглядаються у німецьких рекомендаціях як один із найбільш зрілих напрямів постквантової криптографії. Їхня безпека ґрунтується на властивостях криптографічних хеш-функцій, що дає змогу мінімізувати залежність від недостатньо досліджених математичних структур, характерних для інших PQC-підходів. У технічних документах BSI підкреслюється, що саме хеш-підписи демонструють найвищі рівні криптостійкості в умовах довготривалих квантових ризиків. Вони приділяють особливу увагу двом представникам цих механізмів – XMSS та SPHINCS+.

XMSS став одним із перших постквантових підписів, що отримав формальну стандартизацію та був рекомендований BSI задовго до завершення міжнародного конкурсу NIST. Його центральним принципом є використання дерев Меркла для організації великої кількості одноразових ключів. Кожен підпис базується у схемі на окремому ключі, а автентичність забезпечується шляхом побудови та перевірки шляху в дереві Меркла.

Ключовою особливістю цього механізму є те, що він вимагає ведення внутрішнього лічильника використаних ключів. Повторне застосування одного й того самого ключа призводить до критичної помилки, яка здатна компрометувати безпеку всієї схеми. Тому в технічних документах підкреслюється необхідність суворого контролю стану. Це є одним із недоліків цієї схеми, адже це ускладнює її використання у багатокористувацьких і високонавантажених системах.

Проте якщо у системах оновлення відбуваються рідко механізм може себе показати як надзвичайно ефективний і надійний. В німецьких рекомендаціях вказано, що він підходить для підписування прошивок та оновлень у критично важливих компонентах, автентифікації вбудованих пристроїв, середовищ, де кількість підписів обмежена і може бути точно спрогнозована.

Другим ключовим механізмом є SPHINCS+, який на відміну від XMSS не потребує відстеження стану ключів. Це усуває ризики помилок під час експлуатації і робить його набагато зручнішим для інтеграції в масштабовані інфраструктури, де ключі використовуються часто та багатьма незалежними сервісами.

BSI описує SPHINCS+ як “універсальну” схему підпису, що придатна для широкого спектра застосувань. Вона вважається перспективною для серверних систем із високою інтенсивністю підписів; хмарних сервісів; середовищ, де важлива масштабованість і автоматизація.

Проте BSI також вказує на певні недоліки, одними з яких є розмір підписів та відносно велика обчислювальна вартість.

ML-KEM

ML-KEM є гібридним модульно-решітковим механізмом шифрування ключів, чия безпека базується на задачі модульно навчання з помилками (MLWE). У німецькій системі технічних рекомендацій цей алгоритм займає особливе місце, оскільки поєднує високу криптографічну стійкість з ефективністю, необхідною для масштабного впровадження.

На відміну від класичних рішень, що не використовують алгебраїчної структури, ML-KEM забезпечує значно менші розміри ключів та високу швидкість обміну повідомленнями. Саме тому він розглядається як базовий механізм для захисту каналів зв’язку, побудови протоколів обміну ключами та оновлення існуючих стандартів шифрування. Ефективність алгоритму дозволяє застосовувати його як у високопродуктивних серверних середовищах, так і в ресурсно-обмежених пристроях.

Гібридні криптографічні схеми

Під час переходу до постквантової криптографії ключовими завданнями є забезпечення сумісності між існуючими класичними алгоритмами та новими квантово-стійкими механізмами. Оскільки перехід за один момент є технічно неможливим, BSI передбачають використання гібридних схем, у яких класичні алгоритми працюють з квантовими паралельно.

Одним із запропонованих гібридів є підписи ECDSA та SPHINCS+. Він поєднує класичний алгоритм еліптичних кривих із квантово-стійким хеш-підписом.

Перевагами такого поєднання є: зворотня сумісність та підвищений рівень безпеки. Перша вказує на те, що підписи можуть бути перевірені системами, що не підтримують постквантові алгоритми, а друга, що у разі прориву ECDSA квантовим комп’ютером, SPHINCS+ продовжить гарантувати автентичність повідомлення.

Напрям переходу Німеччини на постквантову криптографію

Німеччина вибудовує перехід до квантово-стійких криптографічних механізмів як довгострокову державну стратегію, що охоплює нормативне регулювання, технічні стандарти, дослідницькі програми та співпрацю з промисловістю. Центральну роль у цьому процесі відіграє Федеральне відомство з безпеки інформаційних технологій, яке формує вимоги до криптографічних параметрів, визначає алгоритми, рекомендовані для використання, та здійснює координацію між державним сектором, виробниками обладнання і постачальниками цифрових послуг.

Одним із ключових напрямів є оцінювання готовності ринку до впровадження нових криптографічних стандартів. Проведене загальнонаціональне опитування стану криптографії та квантових обчислень засвідчило неоднорідний рівень підготовки німецьких організацій. Більшість компаній визнає необхідність переходу на

постквантові механізми, але лише незначна частина вже має практичні плани або реалізовані пілотні впровадження. Найбільшими перешкодами названо високі витрати міграції, значну складність модернізації криптографічних модулів та залежність від зовнішніх постачальників, які ще не інтегрували PQC у своє програмне забезпечення. Особливо проблемним виявилося питання оновлення вбудованих систем, промислової електроніки та IoT-пристроїв, де ресурси обчислення та пам'яті є обмеженими.

Паралельно зі збором ринкових даних Німеччина формує технологічну карту переходу. У стратегічних рекомендаціях визначено етапність впровадження нових криптографічних механізмів: спочатку впровадження гібридних схем у критичних компонентах, поступове оновлення протоколів у державних інформаційних системах, підвищення вимог до постачальників програмного забезпечення та модернізація інфраструктури керування ключами. Важливою складовою є забезпечення сумісності між старими та новими механізмами, щоб уникнути збоїв у сервісах, які мають високу залежність від безперервності роботи.

У внутрішній політиці особливе значення надається промисловості та сектору критичної інфраструктури. Для таких сфер, як енергетика, транспорт, телекомунікації та охорона здоров'я, рекомендується дострокове планування переходу через великий життєвий цикл обладнання. До того ж, німецькі технічні рекомендації відзначають необхідність створення криптографічно гнучких систем, здатних змінювати алгоритми без повної реконструкції апаратних або програмних компонентів.

Важливим елементом є інтеграція Німеччини у європейські ініціативи. Спільні заяви європейських установ, у яких Німеччина бере активну участь, спрямовані на узгодження стандартів, єдиних вимог до параметрів безпеки та підходів до впровадження PQC у державному секторі. Така гармонізація має забезпечити однаковий рівень захисту в усіх країнах ЄС та спростити транскордонну взаємодію цифрових сервісів.

У цілому, внутрішня криптографічна політика Німеччини формує збалансовану модель переходу: вона поєднує науково обґрунтовані рекомендації, детальні технічні стандарти, економічний аналіз готовності ринку та поступову еволюцію національної інфраструктури з урахуванням довгострокових загроз квантових технологій.

Висновки

Перехід до квантово-стійкої криптографії стає критично важливим елементом національної та європейської стратегії цифрової безпеки. Дослідження внутрішніх німецьких нормативів і технічних документів свідчить, що Німеччина вже сформувала комплексний підхід до впровадження нових криптографічних механізмів, який охоплює як наукові основи алгоритмів, так і практичні аспекти їх інтеграції у державні та комерційні системи.

Аналіз показує, що Німеччина приділяє особливу увагу механізмам, здатним забезпечити довготривалу безпеку, серед яких провідне місце займають кодові криптосистеми та хеш-підписи. Водночас визначено важливість перехідного періоду, протягом якого застосовуються гібридні криптографічні схеми, здатні гарантувати сумісність із чинними протоколами та поступовість оновлення інфраструктури. Наукова база, технічні стандарти та аналіз ризиків інтегровані у єдину систему, що дозволяє приймати обґрунтовані рішення щодо вибору алгоритмів та їх параметрів.

Внутрішній ринковий аналіз продемонстрував, що бізнес усвідомлює необхідність переходу, але стикається зі значними практичними бар'єрами. Це підкреслює важливість державної координації, що спрямована на зменшення економічних і технологічних ризиків для підприємств. Гармонізація національних стандартів з європейськими ініціативами додатково підсилює узгодженість політики безпеки та забезпечує рівномірну підготовку до появи квантових обчислювальних потужностей.

Проведений аналіз дозволяє зробити висновок, що Німеччина є одним із провідних європейських центрів у сфері переходу до постквантової криптографії. Системність підходів, орієнтація на довгострокову безпеку та тісна взаємодія між державою, наукою й промисловістю формують модель, яка може слугувати орієнтиром для інших країн у процесі підготовки до нової ери цифрових загроз.

Список використаної літератури

1. Buchmann J., Dahmen E., Hülsing A. (2017). Gitterbasierte Verfahren. Darmstadt: TU Darmstadt. URL: /mnt/data/Gitterbasierte_Verfahren.pdf

2. Bundesamt für Sicherheit in der Informationstechnik. (2021). Entwicklungsstand Quantencomputer. Zusammenfassung V2.1. Bonn. URL: /mnt/data/Entwicklungsstand_QC_Zusammenfassung_V_2_1.pdf

3. Bundesamt für Sicherheit in der Informationstechnik. (2022). Quantum-Sichere Kryptografie: Positionspapier. Bonn. URL: /mnt/data/Quantum_Positionspapier.pdf

4. Bundesamt für Sicherheit in der Informationstechnik. (2025). BSI TR-02102-1: Cryptographic Mechanisms – Recommendations and Key Lengths. Bonn. URL: /mnt/data/BSI-TR-02102.pdf

5. Bundesamt für Sicherheit in der Informationstechnik. (2025). BSI TR-02102-2: Cryptographic Mechanisms – Symmetric Mechanisms. Bonn. URL: /mnt/data/BSI-TR-02102-2.pdf

6. Bundesamt für Sicherheit in der Informationstechnik. (2025). BSI TR-02102-3: Cryptographic Mechanisms – Hash Functions. Bonn. URL: /mnt/data/BSI-TR-02102-3.pdf

7. Bundesamt für Sicherheit in der Informationstechnik. (2025). BSI TR-02102-4: Cryptographic Mechanisms – Digital Signatures. Bonn. URL: /mnt/data/BSI-TR-02102-4.pdf

8. Bundesamt für Sicherheit in der Informationstechnik.(2023). Kryptografie quantensicher gestalten. Bonn. URL: /mnt/data/Kryptografie-quantensicher-gestalten.pdf

9. Bundesamt für Sicherheit in der Informationstechnik. (2023). BSI TR-03111: Hybrid Cryptographic Mechanisms. Bonn. URL: /mnt/data/BSI-TR-03111_V-2-1_pdf.pdf

10. Bundesamt für Sicherheit in der Informationstechnik. (2020). Post-Quantum Cryptography: Recommendations for Action. Bonn. URL: /mnt/data/Post-Quanten-Kryptografie.pdf

11. KPMG & Bundesamt für Sicherheit in der Informationstechnik. (2023). Marktumfrage Kryptografie und Quantencomputing. Berlin. URL: /mnt/data/Marktumfrage_Kryptografie_Quantencomputing.pdf

12. European PQC Partnership. (2025). Joint Statement on the Transition to Post-Quantum Cryptography. URL: /mnt/data/PQC-joint-statement-2025.pdf

References

1. Buchmann, J., Dahmen, E., & Huelsing, A. (2017). *Gitterbasierte Verfahren* [Lattice-based methods]. Darmstadt: TU Darmstadt. [in German].

2. Bundesamt für Sicherheit in der Informationstechnik. (2021). *Entwicklungsstand Quantencomputer. Zusammenfassung V2.1* [State of development of quantum computers. Summary V2.1]. Bonn. [in German].

3. Bundesamt für Sicherheit in der Informationstechnik. (2022). *Quantum-Sichere Kryptografie: Positionspapier* [Quantum-secure cryptography: Position paper]. Bonn. [in German].

4. Bundesamt für Sicherheit in der Informationstechnik. (2025). *BSI TR-02102-1: Cryptographic Mechanisms – Recommendations and Key Lengths*. Bonn. [in German].

5. Bundesamt für Sicherheit in der Informationstechnik. (2025). *BSI TR-02102-2: Cryptographic Mechanisms – Symmetric Mechanisms*. Bonn. [in German].

6. Bundesamt für Sicherheit in der Informationstechnik. (2025). *BSI TR-02102-3: Cryptographic Mechanisms – Hash Functions*. Bonn. [in German].

7. Bundesamt für Sicherheit in der Informationstechnik. (2025). *BSI TR-02102-4: Cryptographic Mechanisms – Digital Signatures*. Bonn. [in German].

8. Bundesamt für Sicherheit in der Informationstechnik. (2023). *Kryptografie quantensicher gestalten* [Designing quantum-secure cryptography]. Bonn. [in German].

9. Bundesamt für Sicherheit in der Informationstechnik. (2023). *BSI TR-03111: Hybrid Cryptographic Mechanisms*. Bonn. [in German].

10. Bundesamt für Sicherheit in der Informationstechnik. (2020). *Post-Quantum Cryptography: Recommendations for Action*. Bonn. [in German].

11. KPMG & Bundesamt für Sicherheit in der Informationstechnik. (2023). *Marktumfrage Kryptografie und Quantencomputing* [Market survey on cryptography and quantum computing]. Berlin. [in German].

12. European PQC Partnership. (2025). *Joint Statement on the Transition to Post-Quantum Cryptography*. [in English].

Дата першого надходження рукопису до видання: 23.11.2025
Дата прийнятого до друку рукопису після рецензування: 22.12.2025
Дата публікації: 31.12.2025