

НАЦИОНАЛНА СИГУРНОСТ

КВАНТОВАТА ТРАНСФОРМАЦИЯ НА ГЛОБАЛНАТА СИГУРНОСТ: СТРАТЕГИЧЕСКИ РИСКОВЕ ЗА КРИТИЧНАТА ИНФРАСТРУКТУРА, КРИПТОГРАФСКАТА ЗАЩИТА И ДЪРЖАВНИЯ СУВЕРЕНИТЕТ

СТАРШИ КОМИСАР ПРОФ. Д-Р ИЛИН САВОВ, Д.Н.

РЕКТОР НА АКАДЕМИЯ НА МИНИСТЕРСТВОТО
НА ВЪТРЕШНИТЕ РАБОТИ



Резюме: Статията изследва квантовата трансформация като въпрос на националната и международната сигурност, който вече не се изчерпва с перспективата за по-мощни изчисления. Разгледани са различните равнища на технологична готовност при квантовите изчисления, комуникации и сензори, уязвимостта на използваните днес асиметрични криптографски механизми и рисковете за дългосрочно защитаваната информация. Анализирани са възможните последиствия за енергетиката, транспорта, здравеопазването, финансовите услуги и държавните информационни системи. Предложен е модел Q-SHIELD за оценка и управление на квантовия риск, който поставя в обща рамка жизнения цикъл на информацията, зависимостите от доставчици, критичността на услугите и институционалната отговорност.

Ключови думи: квантови технологии, национална сигурност, критична инфраструктура, постквантова криптография, криптографска устойчивост, стратегическа автономия, държавен суверенитет

THE QUANTUM TRANSFORMATION OF GLOBAL SECURITY: STRATEGIC RISKS TO CRITICAL INFRASTRUCTURE, CRYPTOGRAPHIC PROTECTION AND STATE SOVEREIGNTY

SENIOR COMMISSIONER PROF. ILIN SAVOV, PHD, DSC

RECTOR OF THE ACADEMY OF THE MINISTRY OF INTERIOR

Abstract: This article examines the quantum transformation as a national and international security issue extending beyond the prospect of greater computing power. It distinguishes the technological maturity of quantum computing, communications and sensing, and analyses the vulnerability of widely deployed public-key cryptography and the exposure of information requiring long-term confidentiality. The implications for energy, transport, healthcare, financial services and government systems are

discussed. An Q-SHIELD conceptual model is proposed to connect information lifetime, supplier dependencies, service criticality and institutional accountability. The central argument is that quantum readiness must be treated as a strategic governance capability rather than a one-off replacement of encryption algorithms.

Keywords: quantum technologies, national security, critical infrastructure, post-quantum cryptography, cryptographic resilience, strategic autonomy, state sovereignty

ВЪВЕДЕНИЕ

Държавите отдавна измерват силата си чрез територия, икономика, въоръжени сили и контрол върху ключови комуникации. Към тези измерения постепенно се прибавя способността да се управлява доверието в цифровата среда. Когато гражданин получава електронен документ, болница предава медицински данни или електроенергийна система приема команда от отдалечен център, всяко действие разчита на невидима основа: криптографски механизми, които удостоверяват участниците и защитават обменната информация. Именно тази основа е изправена пред необходимост от технологична промяна.

Квантовата трансформация не означава, че съществуващите средства за защита са изгубили практическата си стойност днес. Тя означава, че част от математическите предпоставки, върху които е изградена съвременната публичноключова криптография, могат да бъдат преодолені от бъдещи достатъчно мощни квантови изчислителни системи.

Целта на настоящата статия е да изведе квантовия преход от тесния технически разговор и да го постави в полето на националната сигурност. Методът е сравнителен анализ на академични разработки, стандарти и стратегически документи, допълнен с концептуален модел за институционална оценка. Не се представят емпирични измервания на квантова атака или прогноза за определена година.

ОТ ФИЗИЧЕСКИЯ ПРОБИВ КЪМ СТРАТЕГИЧЕСКИЯ РИСК

Под общото наименование „квантови технологии“ стоят поне три различни направления. Квантовите изчисления търсят предимство при определени изчислителни задачи. Квантовите комуникации разработват способности за разпределяне на ключове и други протоколи на основата на квантови физични свойства. Квантовите сензори използват висока чувствителност към физически величини, което може да подобри измерване, навигация и наблюдение. Трите направления имат различни ограничения, нива на готовност и оперативни приложения. Смесването им създава погрешното впечатление, че всяко развитие в лабораторията е непосредствена заплаха за всички национални системи.

Стратегическият проблем се поражда от неравномерното време. Научните разработки се движат с една скорост, стандартизацията с друга, а обновяването на голяма публична инфраструктура често изисква години. Една държава може да разполага с модерни системи и все пак да не знае кои от тях използват уязвими механизми в периферни устройства, междусистемни връзки и договори с външни доставчици. Така технологичната неопределеност се превръща в управленски риск.

Пътната карта на НАТО, публикувана на 29 септември 2026 г., потвърждава именно многопластовия характер на промяната. Алиансът разглежда едновременно изчисленията, комуникациите и сензорите, като включва стандартизация, обучение, изпитване, оперативна съвместимост и защита на критични системи. Документът не е доказателство, че определена квантова способност вече е оперативно разпространена. Той е знак, че военната и гражданската готовност трябва да се планират преди окончателната зрялост на всички технологии.

КРИПТОГРАФСКАТА ЗАЩИТА: КЪДЕ ЗАПОЧВА РЕАЛНИЯТ ПРЕХОД

Дискусията за постквантова сигурност рядко започва с въпроса кой алгоритъм е „най-сигурен“. За държавните системи по-важният първи въпрос е къде всъщност се използва криптография. Тя присъства в защитените връзки, удостоверяването на служители, подписването на софтуерни обновления, електронните регистри, архивирането, оборудването за отдалечен достъп и машинните идентичности. Не всички тези компоненти могат да бъдат подменени по един и същ график.

Постквантовата криптография не е равнозначна на квантова комуникация. Първата използва алгоритми, изпълними върху обичайни компютри и устройства; втората изисква специфична физическа инфраструктура и не отменя всички останали въпроси за удостоверяване, сигурност на крайните точки и управление на ключове. Затова национална стратегия, изградена само около закупуване на квантово оборудване, би пропуснала голяма част от действителните криптографски зависимости.

Практическият преход изисква криптографски инвентар, технически изпитвания, контрол на доставчиците и възможност за замяна на алгоритми без цялостно преработване на информационната система. Това качество обикновено се

обозначава като криптографска гъвкавост. То обхваща конфигурация, управление на сертификати, поддръжка на протоколи и процедура за обновяване. При липса на такава гъвкавост дори добре избран стандарт може да се окаже трудно приложим в реалната инфраструктура.

Особено внимание заслужава дълготрайността на данните. Информация с кратък срок на полезност и секретност има различен профил на риск от архив с медицински досиета, разузнавателни материали или информация за стратегически обекти. Следователно преходът следва да започне не от произволна класация на технологии, а от съотношението между очакван живот на данните, време за внедряване на защита и вероятен хоризонт на заплахата. Неопределеността по последния показател не премахва необходимостта от първите два.

КРИТИЧНАТА ИНФРАСТРУКТУРА: КВАНТОВ РИСК ОТВЪД КОМПЮТЪРНИЯ ЦЕНТЪР

Енергетиката, водоснабдяването, транспортът, здравеопазването и финансовите услуги не са просто набор от мрежи. Те представляват взаимозависими обществени функции, чието прекъсване може да предизвика последици далеч извън организацията, от която е започнало. Европейските правила за киберсигурност по Директива (ЕС) 2022/2555 и за устойчивост на критичните субекти по Директива (ЕС) 2022/2557 предоставят различни, но допълващи се основания за управление на такива зависимости. Самите директиви не въвеждат универсално изискване всяка система незабавно да бъде преобразувана към конкретен постквантов алгоритъм.

Особено чувствителни са зависимостите между информационни и оперативни технологии. Подмяната на алгоритъм в административна уеб услуга обичайно може да се тества отделно. Промяна в промишлено устройство с ограничен капацитет, изискване за непрекъсната работа или строг режим на сертификация може да наложи различен подход. Непроверена миграция сама може да създаде отказ на критична услуга. Следователно правилната цел не е максимално бърза подмяна на всяка цена, а контролирана промяна, съвместима с безопасността и непрекъсваемостта.

ДЪРЖАВНИЯТ СУВЕРЕНИТЕТ В УСЛОВИЯТА НА ТЕХНОЛОГИЧНА ВЗАИМОЗАВИСИМОСТ

Понятието суверенитет често се свежда до това къде физически се намират данните. Местоположението има значение, но не изчерпва проблема. Защитен национален архив може да зависи от чуждестранен доставчик на ключов хардуерен модул, софтуерна библиотека, сертифицираща инфраструктура или услуга за поддръжка. При такава зависимост националният контрол трябва да се оценява по способността за одит, промяна, възстановяване и продължаване на дейността.

Квантовите технологии усилват това разграничение. Страни с голяма научна база и технологична индустрия биха могли да придобият предимства в изчисленията, прецизните измервания или отбранителните приложения. Но притежаването на определена лабораторна способност само по себе си не означава военно превъзходство. Оперативната стойност зависи от надеждност, интеграция, подготовка на персонала, разходи и приложимост в конкретна среда.

Суверенната позиция на една държава не предполага изолация от международните стандарти. Напротив, международно признатите алгоритми и отворените, проверими спецификации могат да намалят риска от зависимост от непрозрачни собствени решения. Националният интерес изисква обаче самостоятелна способност за оценяване на риска, за избор на приоритети и за проверка на резултатите. Ако институциите само приемат удостоверения от производителя, без да разбират архитектурата, контролът остава формален.

В този смисъл възниква нова форма на стратегическа уязвимост: асиметрията между държавата като носител на отговорност и доставчиците като носители на знание за реалното състояние на системите. Тя не е неизбежна. Намалява се чрез договорни изисквания, национална експертиза, публични процедури за тестване, независим одит и умение да се извършва подмяна на критични компоненти. За малките и средните държави тези управленски способности могат да бъдат по-важни от стремежа да развият самостоятелно всички квантови направления.

ЕВРОПЕЙСКИЯТ И СЪЮЗНИЧЕСКИЯТ ОТГОВОР: ОТ СТАНДАРТИ КЪМ ГОТОВНОСТ

Европейската комисия публикува препоръка за координиран преход към постквантова криптография през април 2024 г., а през юни 2025 г. държавите членки, с подкрепата на Комисията, представиха обща пътна карта. Тази последователност е показателна: първо се признава общият проблем, след което се търси съгласуван ред за действие. Причината е практическа. В цифровия единен пазар комуникациите, удостоверяването и веригите на доставки пресичат граници; несъгласуваното обновяване може да създаде оперативни затруднения дори когато отделна организация използва надежден алгоритъм.

Пътната карта на НАТО от септември 2026 г. развива допълващо измерение: квантова готовност за избраната и съюзническата съвместимост. Документът включва изследване на оперативни приложения, изпитване на решения, стандартизация, защита от квантови рискове и обучение на специалисти. Тук преходът се разглежда не само като защита на информация, а като част от бъдещата способност за възпиране и отбрана.

При тълкуването на тези документи трябва да се спазва граница между обявени намерения и изпълнени резултати. Пътната карта е инструмент за управление и координация, не сертификат, че всяка система в ЕС или НАТО е квантово устойчива. Същото важи за техническите стандарти: публикацията на алгоритъм позволява внедряване, но не доказва, че конкретна организация е анализирила зависимостите си, тествала е натоварването и е разработила план за възстановяване.

Най-големият практически риск е разминаването между стратегическа декларация и системна инвентаризация. Ако една публична администрация не знае какви сертификати, протоколи и хардуерни компоненти използва, тя не може да определи реален срок за миграция. Ако пък знае, но няма бюджет, компетентни специалисти и контрол върху доставчиците, инвентарът остава архивна справка. Готовността изисква превръщане на тези знания в решения, срокове и ясна отговорност.

МОДЕЛ Q-SHIELD ЗА ОЦЕНКА НА КВАНТОВИЯ РИСК

За целите на настоящото изследване се предлага концептуалният модел Q-SHIELD (Quantum Security, Heritage, Infrastructure, Exposure, Lifecycle and Dependencies). Той представлява шест взаимосвързани измерения за управленски анализ: критичност на сигурността, наследени технологии, инфраструктурна зависимост, експозиция на информацията, жизнен цикъл и зависимости от външни доставчици. Моделът не е международен стандарт и към момента не е емпирично валидиран. Неговата задача е да структурира въпросите, които институциите трябва да поставят, преди да определят приоритетите на прехода.

Първото измерение е критичността на сигурността (Security Criticality). Необходимо е да се установи какво би последвало при компрометиране на поверителността, целостта или автентичността. Един и същ алгоритъм може да защитава публична справка и оперативни данни със съвсем различна тежест за националната сигурност. Затова началната оценка трябва да изхожда от услугата, а не от популярността на използваната технология.

Второто измерение са наследените технологии (Heritage Systems). То отчита дългия живот на оборудването, ограниченията за обновяване, липсата на документация и зависимостта от прекратена продуктова поддръжка. Често най-трудната миграция не е там, където са най-много данните, а там, където не може безопасно да се смени протокол или криптографска библиотека.

Третото измерение е инфраструктурната взаимозависимост (Infrastructure Interdependence). Оценява се дали една промяна може да засегне други институции, оператори и системи. Например подмяната на механизъм за удостоверяване трябва да бъде съвместима с реалните контрагенти и с аварийните процедури. За критичните услуги добрата криптографска защита е неразделна от оперативната непрекъсваемост.

Четвъртото измерение е експозицията (Exposure). Тук се разглежда колко дълго информацията трябва да остане защитена, дали може да бъде прихваната при пренос, къде се съхраняват копия и какви права имат трети страни. Именно това

измерение поставя проблема за събраната днес информация, чиято стойност за противник може да се запази и след бъдещ технологичен пробив.

Петото измерение е жизненият цикъл (Lifecycle). Системата се оценява спрямо времето за избор, закупуване, тестване, внедряване и последващо обновяване. Отделно се предвиждат критерии за отказ от ново решение, ако тестовите покажат риск за надеждността. Квантовата готовност не може да бъде постигната чрез еднократно административно указание без технически цикъл на проверка.

Шестото измерение са зависимостите (Dependencies). Проследяват се доставчиците, лицензите, затворените компоненти, външните удостоверителни услуги и способността на организацията да променя решенията си. В контекста на суверенитета това е ключово: институцията трябва да може да посочи не само какво използва, но и кой действително контролира възможността то да бъде заменено.

Шестте измерения не трябва да се превръщат автоматично в произволен сбор от точки. По-полезен е експертен профил, в който се описват доказателства, несигурности и необходими действия. Приоритет се получава при едновременно наличие на висока критичност, дълъг живот на поверителността и ниска способност за своевременно обновяване. Моделът позволява да се сравняват институционални ситуации, но изисква бъдещо емпирично изпитване, за да бъдат определени надеждни показатели и прагове.

ПРАКТИЧЕСКИ НАСОКИ ЗА БЪЛГАРИЯ

За България реалистичният първи етап е национално съгласуван преглед на криптографските зависимости в държавните системи и критичните услуги. Такъв преглед следва да разграничава информационни системи с дълъг срок на поверителност, системи за електронна идентичност и подписване, устройства с трудна поддръжка и мрежови връзки към външни организации. Събирането на тази информация трябва да се извършва при ясно определени права на достъп, защото самият криптографски инвентар може да бъде чувствителен документ.

Вторият етап е разработване на практически критерии за обществени поръчки, договори за

поддръжка и приемателни изпитвания. При нови проекти следва да се изисква описание на използваната криптография, документирана процедура за актуализация и доказателства за съвместимост. Това не предполага механично включване на едни и същи изисквания във всеки договор; критичността и възможностите на оборудването трябва да определят конкретния обхват.

Третият етап включва целеви пилотни проекти. Уместно е да се започне от контролирани среди, в които може да се измери въздействието на постквантовите алгоритми върху латентност, размер на съобщенията, управление на сертификати и производителност. Едва след такава проверка може да се планира мащабиране към услуги, чието прекъсване би имало обществена цена. При оперативни технологии изпитванията следва да включват експертите по безопасност и непрекъсваемост.

Четвъртият етап е изграждане на национална компетентност. Не са достатъчни специалисти, които познават математическата теория, ако липсват администратори, одитори, служители по обществени поръчки и ръководители, способни да преведат техническите ограничения в управленско решение. Академичните институции, централите за научни изследвания и органите за сигурност могат да имат обща програма за обучение, техническа оценка и обмен на резултати.

Последният етап е периодичен независим преглед. Технологичната несигурност налага актуализация на решенията, включително когато се появяват нови стандарти, уязвимости или доказателства за напредък в квантовите изчисления. Една национална политика е устойчива не ако обещава окончателна защита, а ако създава механизъм навреме да се откриват и коригират неверни предпоставки.

ЗАКЛЮЧЕНИЕ

Квантовата трансформация променя глобалната сигурност още преди да е настъпил моментът на практическо квантово преодоляване на широко използваните криптографски системи. Това е възможно, защото сигурността винаги се изгражда с решения, взети по-рано от появата на конкретната заплаха. Дългосрочната тайна, жизненият цикъл на инфраструктурата и технологич-

ната зависимост правят изчакването неутрално само на пръв поглед.

Най-същественият стратегически риск не е един бъдещ компютър, който внезапно ще обезсили всичко съществуващо. Той е натрупването на известни, но неуправлявани зависимости: неизвестни криптографски компоненти, невъзможност за обновяване, фрагментирана отговорност, непрозрачни договори и информация, която трябва да остане защитена десетилетия. Срещу такава комбинация не помага нито технологичен оптимизъм, нито алармизъм. Необходими са последователни институционални решения.

Предложеният модел Q-SHIELD цели да постави тези решения в обща рамка. Той свързва криптографската промяна с критичността на обществената услуга, с експозицията на данните и с реалната способност на държавата да контролира собствените си технологични зависимости. Това е концептуално предложение, което следва да се проверява в отделни сектори, преди да придобие характер на инструмент за измерване.

Силната държава не е тази, която заявява, че е готова за всяка бъдеща технология. Силната държава е тази, която знае кои нейни системи са уязвими, кой носи отговорност за промяната и как ще продължи да защитава гражданите, когато технологичните правила се променят.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

1. Shor, P. W. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on

a Quantum Computer." *SIAM Journal on Computing*, 26(5), 1997, pp. 1484–1509.

2. Moody, D.; Perlner, R.; Regenscheid, A.; Robinson, A.; Cooper, D. *Transition to Post-Quantum Cryptography Standards*. NIST IR 8547, Initial Public Draft, 2024.
3. Grover, L. K. "A Fast Quantum Mechanical Algorithm for Database Search." *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 1996, pp. 212–219.
4. North Atlantic Treaty Organization. *Quantum Technology Roadmap*. Public version, 29 September 2026.
5. National Institute of Standards and Technology. *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. FIPS 203. Gaithersburg, MD: NIST, 2024.
6. Европейски парламент и Съвет на ЕС. Директива (ЕС) 2022/2555 от 14 декември 2022 г. относно мерките за високо общо ниво на киберсигурност в Съюза (NIS2). ОВ L 333, 27.12.2022, с. 80-152.
7. Европейски парламент и Съвет на ЕС. Директива (ЕС) 2022/2557 от 14 декември 2022 г. относно устойчивостта на критичните субекти. ОВ L 333, 27.12.2022, с. 164–198.
8. NIS Cooperation Group / European Commission. *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*. European Commission, 23 June 2025. <https://digital-strategy.ec.europa.eu/en/library/>