квантових алгоритмів. Це означає, що у разі появи масштабованих квантових комп'ютерів такі алгоритми можуть бути повністю скомпрометовані.

Натомість симетричні алгоритми шифрування, зокрема AES, є менш вразливими до квантових атак. Використання алгоритму Гровера дозволяє лише квадратично прискорити перебір ключів, що фактично зменшує ефективну довжину ключа вдвічі. У практичному вимірі це означає необхідність переходу на довші ключі (наприклад, використання AES-256 замість AES-128) для збереження належного рівня безпеки [3]. Подібний підхід застосовується і до криптографічних хеш-функцій. Квантові алгоритми знижують їх стійкість до пошуку колізій, однак не призводять до повної компрометації. Відповідно, підвищення рівня безпеки досягається шляхом використання хеш-функцій із більшою довжиною вихідного значення.

З огляду на зазначені ризики, ключовим завданням є підготовка IT-інфраструктури до поступового переходу на квантово-стійкі механізми захисту. Одним із базових принципів такої підготовки є впровадження підходу crypto-agility — здатності систем гнучко змінювати криптографічні алгоритми без суттєвих змін архітектури. Першочерговим кроком є інвентаризація криптографічних залежностей, включаючи TLS, VPN, PKI, API та системи управління секретами. Це дозволяє визначити критичні компоненти інфраструктури та пріоритети їх модернізації. Важливим аспектом є централізоване управління ключами та сертифікатами, що спрощує їх ротацію та подальший перехід на нові алгоритми. Додатково доцільним є впровадження гнучких конфігурацій безпеки, зокрема підтримки змінюваних криптографічних наборів і гібридних рішень.

У висновку слід зазначити, що підготовка до квантової епохи не є одноразовим заходом, а тривалим процесом трансформації IT-інфраструктури. Впровадження принципів гнучкості, централізації управління криптографією та поступової міграції дозволить знизити ризики та забезпечити стійкість систем у майбутньому.

1. Kumar M. Post-quantum cryptography Algorithm's standardization and performance analysis. Array. – 2022. – Vol. 15. – Article 100242.
2. Воробець П. А., Горпенюк А. Я., Опірський І. Р. Перехід до постквантових криптографічних систем: виклики, стандартизація та перспективи // Безпека інформації. – 2024. – Т. 30, № 2. – С. 306–315
3. Alagic G., et al. Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8545. – 2025. – 54 p.

З історії становлення національної системи захисту інформації. 1992–1999 рр.

УДК 94:35.083.8(045)

Валерій Ворожко

СБ України, wp06vv@gmail.com

Першим законодавчим актом, що стверджував інформаційний суверенітет України, став Закон України «Про інформацію», прийнятий ВР України 2 жовтня 1992 р. Цей Закон визначив режим доступу до інформації, поділивши її на відкриту інформацію та інформацію з обмеженим доступом, закріпив за державою право й обов'язок здійснювати контроль за режимом доступу до інформації. Указом Президента України від 1 грудня 1992 р. № 593/92 була створена Державна служба України з питань технічного захисту інформації (далі – ДС ТЗІ), на яку покладалися функції щодо реалізації державної політики, організаційного, нормативного, інженерно-технічного забезпечення технічного захисту інформації. На той час уся діяльність у цій сфері здійснювалася на підставі нормативних документів, затверджених Держтехкомісією СРСР/РФ. ДС ТЗІ підписала декілька угод про співробітництво з Держтехкомісією РФ та перебувала у фарватері політики РФ у сфері технічного захисту інформації.

Одним із питань на підготовчому етапі формування власної системи охорони державної таємниці (далі – СОДТ) було визначення державного органу як спеціально уповноваженого органу державної влади з головним завданням реалізації державної політики у цій сфері діяльності. У той період існувала думка, що формування СОДТ, аналогічної радянському режиму, могло б створити передумови для зловживань щодо застосування таємної інформації, порушень прав і свобод людини. Демократизація правовідносин у сфері, пов'язаній з державною таємницею, повинна була передбачати розширення прав і, водночас, підвищення відповідальності керівників усіх рівнів за режим секретності та персоніфікацію питань щодо віднесення відомостей до державної таємниці та їхнього засекречування. Тому було прийнято рішення про створення окремого спеціального уповноваженого органу державної влади з питань охорони державної таємниці відповідно до досвіду США та в цілому євроатлантичної СОДТ. Ця ідея тоді викликала спротив у проросійської частини української верхівки, яка з часом значно посилилася й після 1999 р. українську СОДТ значною мірою повернули до радянсько-російської моделі.

Визначений ВР України політичний курс щодо формування СОДТ був реалізований відповідними рішеннями уряду держави. Постановою КМУ від 4 травня 1993 р. № 327 було створено Державний комітет України з питань державних секретів, який функціонально був побудований схожим до Управління з нагляду за інформаційною безпекою (Information Security Oversight Office, далі – ISOO), у складі NARA (Національне агентство з питань документації і архівів) США. ISOO відповідає за впровадження та реалізацію президентських виконавчих наказів у сфері таємниць; розробляє стандарти для засекречування і розсекречування документів та типові інструкції з охорони таємних відомостей, займається підвищенням кваліфікації спеціалістів РСО; проводить перевірки в установах на їхню відповідність політиці уряду у галузі інформаційної безпеки; реагує на скарги та пропозиції установ і громадян щодо засекречування та розсекречування інформації; вносить пропозиції Президентові щодо змін у політиці інформаційної безпеки; збирає відповідні звіти з установ, узагальнює їх і готує щорічний звіт з інформаційної безпеки Президенту США тощо. ВР України вже на етапі прийняття законів, які

регламентували діяльність СБ України, залишила за цим державним органом лише функції спеціальної компетенції як правоохоронного органу.

У жовтні 1997 р. постановою КМУ № 1126 затверджена «Концепція технічного захисту інформації в Україні», яка визначала основи державної політики у сфері захисту інформації інженерно-технічними заходами і засобами. Реалізація Концепції забезпечувала єдність принципів формування і проведення державної політики в усіх сферах життєдіяльності особи, суспільства та держави. Зазначено, що необхідність розвитку ТЗІ зумовлена зростанням загроз для інформації, спричинених лібералізацією суспільних та міжнародних відносин, кризовим станом економіки, застосуванням технічних засобів оброблення інформації та засобів зв'язку іноземного виробництва, поширенням засобів несанкціонованого доступу до інформації та впливу на неї. На виконання положень «Концепції технічного захисту інформації в Україні», 16 лютого 1998 р. постановою № 180 Кабінетом Міністрів України затверджене «Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах». Це «Положення» визначило основи організації, завдання, права, обов'язки суб'єктів правовідносин та порядок забезпечення режиму секретності під час обробки секретної інформації в автоматизованих системах.

Забезпечення безпеки мікроконтролерних систем у робототехнічних комплексах

УДК 004.056

Гануля Роман , Козбур Ігор

Тернопільський національний технічний університет імені Івана Пулюя, Hanularoma@gmail.com Kozbur.igor@gmail.com

Актуальність проблеми. Мікроконтролерні системи є базовим рівнем керування у сучасних робототехнічних комплексах, включаючи промислові роботи, автономні системи та IoT-пристрої. Зростання кількості підключених пристроїв, а також інтеграція робототехніки у промислові та побутові сфери призводять до значного збільшення кіберзагроз, що можуть суттєво порушити роботу систем, викликати втрату даних або фізичну шкоду. Найпоширенішими проблемами є несанкціонований доступ до апаратного забезпечення, підміна прошивки, перехоплення та модифікація даних у комунікаційних каналах, а також атаки побічними каналами (side-channel attacks), що використовують інформацію про споживання енергії чи електромагнітне випромінювання. За даними NIST [1], більшість сучасних IoT-пристроїв мають критичні вразливості на рівні прошивки та автентифікації, що робить їх потенційною мішенню для атак на робототехнічні комплекси. З огляду на це, забезпечення безпеки мікроконтролерних систем є надзвичайно актуальним завданням, яке поєднує в собі апаратні, програмні та комунікаційні аспекти захисту.

Мета роботи. Метою цього дослідження є аналіз основних загроз безпеці мікроконтролерних систем у робототехнічних комплексах та визначення ефективних методів їх захисту. Крім того, робота спрямована на розробку та дослідження комплексного підходу, що поєднує апаратні та програмні засоби