ВІЙСЬКОВА АКАДЕМІЯ (м. ОДЕСА)

# СПІЛЬНІ ДІЇ ВІЙСЬКОВИХ ФОРМУВАНЬ І ПРАВООХОРОННИХ ОРГАНІВ ДЕРЖАВИ: ПРОБЛЕМИ ТА ШЛЯХИ ВИРІШЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

Збірник тез доповідей
VI Міжнародної науково-практичної конференції

18 жовтня 2024 року

Міністерство освіти і науки України
Міністерство оборони України
**ВІЙСЬКОВА АКАДЕМІЯ (м. ОДЕСА)**

СПІВОРГАНІЗАТОРИ:
Одеський державний університет внутрішніх справ
Інститут Військово-Морських Сил Національного університету «Одеська морська академія»

**Збірник тез доповідей**
**VI Міжнародної науково-практичної конференції**

# СПІЛЬНІ ДІЇ ВІЙСЬКОВИХ ФОРМУВАНЬ І ПРАВООХОРОННИХ ОРГАНІВ ДЕРЖАВИ: ПРОБЛЕМИ ТА ШЛЯХИ ВИРІШЕННЯ В УМОВАХ ВОЄННОГО СТАНУ

**18 жовтня 2024 року**

м. Одеса

## ПРОГРАМНИЙ КОМІТЕТ

КОВАЛЬЧУК А.Т.
ЛІСОВЕНКО Д.В., канд. техн. наук, доц.
ГОНЧАРУК А.А., канд. техн. наук, с.н.с.
САЄНКО І.В., канд. політ. наук, доц.
ГЕОРГІЄВ В.М., канд. пед. наук, доц.
МАКСИМЕНКО Ю.А., канд. техн. наук, доц.
НІКУЛ С.О. канд. техн. наук, доц.
ДРУЖИНІН В.С., доктор філософії
ГОРЛІЧЕНКО М.Г., канд. пед. наук, доц.
МІНАСОВ Р.В
ЛУХАНІН В.В
КОЛЕСНИК О.В

## ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Голова організаційного комітету: заступник начальника академії з наукової роботи, начальник відділу, кандидат технічних наук, доцент, полковник Д. ЛІСОВЕНКО.

Заступник голови організаційного комітету: начальник наукового центру, кандидат технічних наук, старший науковий співробітник, полковник А. ГОНЧАРУК.

Секретар конференції: молодший науковий співробітник науково-організаційного відділу, працівник ЗС України О. АЛЬБЕЩЕНКО.

Члени організаційного комітету:

заступник начальника відділу, підполковник О. ШТОГРІН;

старший помічник начальника науково-організаційного відділу, майор В. ЩЕРБАКАН;

провідний науковий співробітник науково-організаційного відділу, кандидат психологічних наук, працівник ЗС України Ю. ОВСЮК;

начальник редакційно-видавничого відділення, працівник ЗС України В. МІЛОВАНОВ;

ад'юнкт науково-організаційного відділу підполковник І. МІКРЮКОВ;

доцент кафедри оргіназації розвідувально-інформаційної роботи та технічних засобів розвідки, доктор філософії, підполковник В. ДІДИК;

викладач кафедри ракетно-артилерійського озброєння майор Д. МАКСИМЧУК;

старший викладач кафедри забезпечення військ (сил) підполковник О. ФРОЛОВ;

викладач кафедри тактики та загальновійськових дисциплін підполковник Є. ЖУКОВ;

старший викладач кафедри фундаментальни х наук працівни к ЗС України О. СОЛОВЙОВ;

старший викладач кафедри управління повсякденною діяльністю підрозділів, кандидат юридидичних наук, підполковник Ю. НОРЧУК;

ад'юнкт науково-організаційного відділу майор Ю. БРИЖЕНЮК.

Інформаційна політика росії набула характеру цілеспрямованої інформаційної війни проти України: необ'єктивність, маніпуляції, перекручування фактів, відверта неприхована брехня, кібератака (використання компютерних технік для проникнення в інформаційні системи, крадіжки даних, або знищення важливої інформації), путінсько – кремлівська пропаганда як частина політики кремля в цілому. Робота ЗМІ ведеться за типом жовтої преси. Залучена величезна кількість акторів – громадян росії, України та інших країн – а також інших спеціалістів на території України для отримання потрібної телевізійної картинки. Ми можемо з впевненістю сказати, що інформаційна зброя постає в сьогоденні як новий і унікальний вид зброї.

Головними механізмами протистояння брехливій, перекрученій, неперевіреній інформації в умовах війни є такі: насамперед, це підвищення медіа грамотності населення, що дозволяє йому захищатися від дезінформаційних впливів та допомагати підтримувати інформаційну безпеку держави; можливість орієнтуватися в інформаційному просторі, який є просто гігантським, а часу на повноцінне його вивчення бракує; через значні обсяги контенту, а також через неможливість критично сприймати інформацію через прихильність тільки конкретним ЗМІ. Нині стало зрозумілим, що інформаційна війна є елементом повномасштабної війни, що вироблення стійкості до впливу дезінформації є питаннями національної безпеки. Ми бачимо, як Росія докладає всіх зусиль, аби очорнити українців в очах світу та розбити єдність українців. А тому, щоб оминути пастки проросійських ресурсів й не поширювати дезінформацію, необхідно по-перше, застосовувати критичне мислення, а саме чітко бачити для чого використовується в певному медіа той чи інший контент як інструмент пропаганди чи маніпуляці, яке завдання ставить перед собою і зміст недійного матеріалу і сам цей медіа, в чому виявляється їхня шкода.

В сучасних умовах російсько – української війни, характер боротьби змінився, набувши якостей не лише інформаційної війни. Але при цьому вплив на суспільство інформаційної зброї не зменшується. Інформаційна війна – це одна з граней широкомасштабного вторгнення російської федерації в Україну. Вона розкривається через сукупність певних ідей, які руйнують національну самосвідомість. Запобігання впливу на інформаційний простір нашої країни та її електронні ресурси, а також системи державного управління, в тому числі автоматизовані системи управління військового призначення, особливо в умовах ведення повномасштабної збройної агресії, є першочерговим завданням, вирішення якого забезпечить дотримання відповідного рівня національної безпеки держави в частині однієї з її основних складових – інформаційної безпеки на належному рівні.

Інформаційна зброя принципово відрізняється від інших засобів ведення війни тим, що з її допомогою ведуться неоголошені і, найчастіше, невидимі війни, та що об'єктами впливу є, насамперед, суспільство і держави – економічні, політичні, соціальні, тощо. Крім того, військова стратегія використання інформаційної зброї виявилася тісно пов'язаною із цивільним сектором і стала багато в чому від нього залежати.

**ЗАВАЛЬНЮК Володимир**, канд. фіз.-мат. наук
*Військова академія (м. Одеса)*
**МАРЧЕНКО Сергій**
*Одеський національний медичний університет*

## ПОСТ-КВАНТОВА КРИПТОГРАФІЯ: НОВІ СТАНДАРТИ ТА ВИКЛИКИ БЕЗПЕЦІ

13 серпня 2024 р. Національний інститут стандартів і технологій США (NIST) опублікував фінальну версію трьох перших федеральних стандартів обробки інформації (FIPS) пост-квантової криптографії, робота над якими велася біля семи років. Ці стандарти описують квантово стійкі криптографічні схеми для обміну ключами (FIPS 203) та цифрового підпису (FIPS 204 і FIPS 205).

Розробка цих стандартів була розпочата у відповідь на значне підвищення ризиків компрометації таких алгоритмів шифрування з відкрити ключем, як алгоритм RSA та алгоритми на основі еліптичних кривих, які сьогодні є стандартними і безперечно надійними засобами обміну ключами шифрування при передачі переважної більшості інформації у глобальній мережі. Причиною зростання вказаних ризиків став стрімкий прогрес у розробці квантових обчислювальних машин, що намітився біля десяти років тому. І хоча проблема забезпечення безпеки в умовах загроз, пов'язаних із квантовими комп'ютерами була відома задовго до їх появи, сьогодні вона вже є цілком нагальною, тож затвердження перших стандартів у сфері пост-квантової криптографії є вкрай важливим кроком, необхідним для забезпечення належного захисту інформації вже у найближчому майбутньому.

Традиційні криптографічні алгоритми, такі як RSA, DSA і протоколи на основі еліптичних кривих, значною мірою покладаються на математичні проблеми, які є складними для вирішення класичними комп'ютерами, але легко вирішуються вже існуючими квантовими алгоритмами, такими як алгоритм Шора для факторизації чисел. Це робить сучасні криптосистеми вкрай вразливими в умовах неминучого наближення квантової ери – квантові комп'ютери здатні ефективно розв'язувати складні задачі факторизації великих чисел та обчислення дискретних логарифмів, що дозволить їм легко зламати більшість існуючих криптографічних систем з відкритим ключем, що критично вплине на безпеку передачі даних у сучасних інформаційних системах. Тобто необхідність створення та широкого впровадження вже у найближчому майбутньому криптографічних алгоритмів, стійких до квантових атак, є однією із найважливіших проблем у тому числі й сектору безпеки.

Сучасні квантові комп'ютери, все ще залишаючись доволі примітивними та вкрай дорогими, вже наближаються до того рівня, коли вони зможуть розв'язувати проблеми, недоступні класичним машинам. Практично всі існуючі схеми шифрування з відкритим ключем базуються на тому принципі, що хоча алгоритм їх злому фактично є відомим, проте його успішне виконання навіть на сучасних суперкомп'ютерах займатиме таку кількість часу, що отримана в результаті зламу інформація вже не матиме практичної цінності. Однак квантові комп'ютери завдяки заснованим на квантовому паралелізмі алгоритмах здатні виконувати цілий перелік операцій, складних для класичних обчислювальних машин, за порівняно незначну кількість операцій (тобто часу).

Більш того, інший важливий квантовий алгоритм – алгоритм Гровера – дозволяє знаходити значення у невідсортованій базі даних за час, рівний квадратному кореню з кількості елементів у базі. Цей алгоритм хоча й не дозволяє повністю зламати існуючі криптографічні системи (як це робить алгоритм Шора із криптографією з відкритим ключем), проте значно пришвидшує процес атак «грубою силою», тобто перебором всіх можливих варіантів ключа. Як наслідок, шифрування за допомогою симетричних алгоритмів, таких як AES, стає вдвічі менш стійким. Тобто для забезпечення колишнього рівня захисту доведеться подвоювати довжину ключа, що призведе до значного підвищення обчислювальної складності відповідних алгоритмів.

Всі передові країни світу вже кілька десятиліть активно розвивають квантові обчислювальні системи та системи передачі даних. Наприклад, Китай ще з 2016 року відкрито тестує супутникові системи квантового шифрування, а у 2020 році повідомив про успішне здійснення першого квантового обміну ключами між двома наземними станціями за допомогою супутникового каналу (супутник «Micius»), що доводить технічну можливість реалізації подібних схем вже сьогодні та відкриває нові перспективи для квантово-безпечної комунікації на великих відстанях.

Окрім самих алгоритмів є важливою і квантова криптографія на рівні ліній передачі даних –квантовий розподіл ключів, який забезпечує передачу ключа шифрування через квантові канали. Головною особливістю квантових ліній передачі даних є те, що будь-яка спроба перехоплення ключа змінює квантові стани, якими закодовані біти ключа, призводячи до виникнення специфічних помилок, наявність яких і дозволяє виявити атаку.

Квантово-стійкі алгоритми шифрування базуються на таких математичних проблемах, які вважаються складними для обчислення як на класичних, так і на квантових комп'ютерах. Найбільш відомими серед них є задачі теорії граток (схема шифрування Голдрайха, Голдвассера і Галеві; алгоритми CRYSTALS-Kyber і CRYSTALS-Dilithium та інші), задачі дешифрування лінійних кодів (наприклад, алгоритм McEliece, розроблений ще у 1970-х роках) та багато інших.

Основними викликами при впровадженні квантово-стійкої криптографії є необхідність значних інвестицій часу та ресурсів у розробку відповідних алгоритмів і їх неперервну перевірку на стійкість до нових квантових алгоритмів (які неодмінно будуть з'являтися по мірі вдосконалення квантових комп'ютерів), оновлення інформаційної інфраструктури і впровадженням систем передачі й обробки квантових даних, координація на міжнародному рівні для уникнення проблем сумісності.

Підсумовуючи, варто додати, що запровадження новітніх криптографічних стандартів матиме значний вплив на всі сфери інформаційної безпеки, зокрема на урядові та комерційні системи (особливо банківську). Для забезпечення підтримки нових стандартів розробникам як програмного, так і апаратного забезпечення доведеться оновити свої криптографічні протоколи та інтегрувати підтримку нових стандартів у свої рішення. А на міжнародному рівні ці стандарти мають стати основою для гармонізації підходів до пост-квантової безпеки, стимулюючи дослідження і впровадження технологій, що забезпечать надійний захист даних у довгостроковій перспективі.

**ЗАДЕРІЄНКО Сергій,** канд. військ. наук, доц.
*Національна академія сухопутних військ імені гетьмана Петра Сагайдачного (м. Львів), Україна*

## ДОСВІД ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ У ХОДІ ПРОВЕДЕННЯ ПУБЛІЧНИХ ЗАКУПІВЕЛЬ ТОВАРІВ, РОБІТ І ПОСЛУГ

Порядок придбання у якості замовників військовими організаційними структурами (з'єднаннями, військовими частинами (підрозділами), військовими навчальними закладами, установами та організаціями Сил оборони України) товарів, робіт і послуг, з точки зору законодавства постійно зазнає змін. Уповноваженим особам чи іншим службовим (посадовим) особам, які визначені замовниками відповідальними за організацію та проведення процедур закупівель і спрощених закупівель, у воєнний час слід більш ретельно підходити до чутливої інформації та змісту даних, які розміщуються у електронній системі.

Процес створення, розміщення, оприлюднення, обмін тендерною інформацією і документами в електронному вигляді регулюється Законом України «Про публічні закупівлі» та Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» і допомагає військовим організаційним структурам не розкривати своє місцезнаходження та іншу конфіденційну інформацію, в той же час залишати закупівлі достатньо ефективними.

Конфіденційною або чутливою інформацією вважаються будь-які відомості, знаючи які, можна ідентифікувати учасника державних закупівель. У ході формування уповноваженою особою оголошення про проведення закупівлі конфіденційною не може бути визначена інформація про запропоновану ціну, інші критерії оцінки, технічні умови, технічні специфікації та документи, що підтверджують відповідність кваліфікаційним критеріям.

Державне підприємство «Prozorro» і Міністерство економіки разом з іншими міністерствами постійно працюють над удосконаленням механізмів конфіденційності замовників та постачальників товарів, робіт і послуг для того щоб знайти баланс, який дозволить ефективно проводити закупівлі і в той же самий час не надавати противнику додаткової інформації яка дозволить йому викривати райони дислокації військових підрозділів чи інші стратегічні плани.

# *СПІЛЬНІ ДІЇ ВІЙСЬКОВИХ ФОРМУВАНЬ І ПРАВООХОРОННИХ ОРГАНІВ ДЕРЖАВИ: ПРОБЛЕМИ ТА ШЛЯХИ ВИРІШЕННЯ В УМОВАХ ВОЄННОГО СТАНУ*

Видання віддруковано з готового оригінал-макета

Комп'ютерний набір *Колесніченко М.М.*
Дизайн обкладинки *Ушаков О.Є.*

Здано до набору 27.11.2024 р. Підписано до друку 12.12.2024 р.
Формат паперу 297×420/4. Авт.арк.– 21,91. Обл.вид.арк –22,01,.
Друкарські аркуші – 120,5. Умовні друк.арк. – 27,72. Папір офсетний.
Гарнітура Times New Roman. Замовлення №426-2024 РВВ ВА. Тираж 3 прим.