УДК 343.144.5

КАЗЬМІРУК С.Д., аспірант Київського університету права НАН України.
ORCID: https://orcid.org/0000-0001-8101-732X.
ЛЕОНОВ Б.Д., *доктор юридичних наук, професор*,
головний науковий співробітник МНДЦ при РНБО України.
ORCID: https://orcid.org/0000-0002-2488-7377.

ПРАВОВЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ СИСТЕМ ДЕТЕКЦІЇ БРЕХНІ ВІД КІБЕРАТАК В УМОВАХ ВОЄННОГО СТАНУ

DOI...

Анотація. *Стаття присвячена дослідженню проблемних питань щодо кіберзахисту систем детекції брехні. Висвітлюються аспекти правового регулювання застосування комп'ютерного поліграфа (детектора брехні) в секторі безпеки і оборони України. В статті обґрунтовується інноваційний підхід до кіберзахисту комп'ютерних систем виявлення прихованої і недостовірної інформації та підвищення ефективності застосування детектора брехні. Зроблено висновок про доцільність розробки нових та вдосконалення існуючих інструментів і механізмів правового та організаційного забезпечення кіберзахисту систем детекції брехні від кібератак. Вказано можливі шляхи запровадження комп'ютерного поліграфа та кіберзахисту інформації для підвищення ефективності виявлення прихованої та недостовірної інформації в складових сектору безпеки і оборони України в умовах воєнного стану.*

Ключові слова: *кібербезпека, воєнна безпека, НАТО, правове регулювання, психофізіологічне дослідження, комп'ютерний поліграф.*

Summary*. The article is devoted to exploring problematic issues regarding the cyber protection of lie detection systems. Aspects of the legal regulation of the use of a polygraph (lie detector) in the security and defense sector of Ukraine are highlighted. The article contains an innovative approach to the cyber protection of computer systems, the detection of hidden and unreliable information, and the improvement of the effective use of the lie detector. A conclusion was drawn on the practicality of developing new and improving existing tools and mechanisms of legal and organizational support for the cyber protection of lie detection systems against cyber attacks. Possible ways of introducing a polygraph and cyber protection of information to increase the effectiveness of detecting hidden and unreliable information in the security and defense sector of Ukraine in the conditions of martial law are indicated.*

Keywords: *cyber security, military security, NATO, polygraph system, legal regulation, psychophysiological detection of deception (polygraph).*

Постановка проблеми. З початку повномасштабної війни на об'єкти критичної інфраструктури України було здійснено більше 1,2 млн. кібератак. Тільки у 2022 році українські організації та установи, де застосовуються комп'ютерні системи для обробки інформації, пережили понад 2000 кібератак. Понад 300 з них були спрямовані на безпековий і оборонний сектор, більш ніж 400 – на цивільне життя, включно з комерційними, енергетичними, фінансовими і телекомунікаційними компаніями. Ще понад 500 атак припали на урядові об'єкти, де застосовуються інформаційні системи захисту та обробки конфіденційної інформації [1].

Такий стан справ зумовлює потребу застосування всіх можливих кіберінструментів для забезпечення кіберзахисту об'єктів критичної інфраструктури України.

Одним із таких інноваційних інструментів є системи детекції брехні (polygraph systems), застосування яких ускладняються низкою проблем нормативно-правового,

організаційного та методичного характеру. Зокрема, недостатньо дослідженим є методологічне забезпечення таких систем під час перевірки прийняття на окремі види публічної служби, службового розслідування тощо.

Проблемним залишається використання результатів психофізіологічного дослідження із застосуванням детектора брехні як доказу у кримінальному процесі, оскільки на даний час нормами Кримінального процесуального кодексу України не передбачена можливість перевірки достовірності показань особи із застосуванням комп'ютерного поліграфа або прийняття судом як доказу отриманих таким чином відомостей. У кримінальному провадженні результати використання комп'ютерного поліграфа можуть бути застосовані лише у сукупності з іншими належними та допустимими доказами.

Результати аналізу наукових публікацій. Дослідженням актуальних напрямів використання систем детекції брехні та застосування комп'ютерних поліграфів в безпековій сфері успішно займалися зарубіжні фахівці: В. Марстон (W. Marston) [2], Дж. Ларсон (J. Larson) [3], Л. Кілер (L. Keeler), Дж. Рід (J. Reid), К. Бекстер (C. Backster), Р. Нельсон (R. Nelson), Н. Гордон (N. Gordon), Д. Крапол (D. Krapohl) [4] та інші.

Значний внесок у розробку програми і запровадження поліграфологічної програми (OCONUS) здійснив Ч. Морган (Ch.Morgan) та інші американські дослідники [5].

Серед українських дослідників цієї проблеми можна виділити роботи О. Мотляха, О. Хорватової, Р. Яремчук та ін.

На жаль, в Україні бракує спеціальних досліджень у сфері застосування комп'ютерних поліграфів з урахуванням міжнародних стандартів та кращих зарубіжних практик. Недостатньо дослідженою залишається і проблема забезпечення кіберзахисту комп'ютерних систем детекції брехні та підвищення ефективності застосування детектора брехні в секторі безпеки і оборони України. Ця проблематика набуває особливої актуальності в умовах війни та реформування сектору безпеки і оборони за стандартами НАТО [6].

Метою статті є удосконалення кіберзахисту та правового забезпечення комп'ютерних систем детекції брехні в контексті запровадження нової системи гарантій безпеки для України (U-24. United for peace).

Виклад основного матеріалу. Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України [7]. З початку інтенсивної кібервійни проти нашої держави досліджено десятки сценаріїв на кіберфронтах.

Як зазначається у звіті Державної служби спеціального зв'язку та захисту інформації України "Russia's Cyber Tactics Lessons Learned 2022", цілі російських хакерів зазнали істотних змін, від масових актів кібершпигунства на початку війни до кібератак, спрямованих на крадіжку баз даних, кібершахрайства, кіберрозвідку тощо. Кібератаки стають дедалі більш руйнівними, зачіпаючи всі сфери життєдіяльності держави. Це свідчить про те, що російська влада використовує кіберкомпонент як засіб кібервійни [8; 9].

Вважаємо, що таким кіберкомпонентом можуть бути не сертифіковані програмні продукти, які використовують державні органи та приватні компанії, які задіяні у секторі безпеки й оборони України. Особливо це стосується програмного забезпечення комп'ютерних систем детекції брехні.

Отже, суб'єктам сектору безпеки і оборони України, що є потенційно уразливими з точки зору кіберінцидентів, слід приділяти більше уваги кіберзахисту інформаційних ресурсів від кібератак та здійснювати своєчасне виявлення шпигунських програмних засобів. У цьому контексті дослідженню підлягає й програмне забезпечення партнерів і постачальників детекторів брехні.

Варто зауважити, що програмне забезпечення комп'ютерних систем детекції брехні нині експертно не досліджено і може створювати кіберзагрози з огляду на те, що комп'ютерні поліграфи активно застосовуються в державних органах, комерційних структурах та окремими приватними особами.

Зокрема, психофізіологічне дослідження із застосуванням комп'ютерних поліграфів проводиться правоохоронними органами під час перевірки кандидатів на службу, проведення службових розслідувань (перевірок), протидії корупції та виявленні інших суспільно небезпечних ризиків.

Правові засади проведення з особами психофізіологічного опитування із застосуванням поліграфа під час вступу на службу та проходження служби, зокрема, передбачені ст. 26 Закону України "Про Державне бюро розслідувань", ст. 24 Закону України "Про Бюро економічної безпеки України", ст. 50 Закону України "Про Національну поліцію".

В Інструкції про порядок проведення службових розслідувань та службових перевірок стосовно військовослужбовців Служби безпеки України, затвердженій наказом ЦУ СБУ від 02.03.16 р. № 45, передбачена можливість опитування особи за її згодою із застосуванням поліграфа відповідно до законодавства[9]. Порядок такого опитування, зазвичай, визначається відомчими нормативно-правовими актами.

Питання застосування детектора брехні обговорювалося під час засідання РНБО України (23 червня 2023 року) стосовно судової реформи. За результатами засідання Голова Верховної Ради Руслан Стефанчук поінформував, що при доборі суддів і при подальшій діяльності суддів використовуватиметься детектор брехні, для чого буде зроблена ціла низка заходів організаційного і правового характеру. З цією метою РНБО України рекомендувала Кабінету Міністрів України прискорити підготовку відповідного законопроекту [10].

За результатами засідання РНБО України було прийняте рішення "Про прискорення судової реформи та подолання проявів корупції у системі правосуддя", зміст якого, зокрема, передбачає необхідність внесення змін до законів України "Про судоустрій і статус суддів" та "Про Вищу раду правосуддя" щодо запровадження психофізіологічного опитування із застосуванням поліграфа як умови при доборі кандидатів на посаду судді місцевого суду, конкурсу на зайняття вакантних посад суддів апеляційних судів, вищих спеціалізованих судів та Верховного Суду з метою вироблення оптимальної та ефективної процедури перевірки відповідності кандидатів у судді критеріям доброчесності, професійної етики або існування інших обставин, які можуть негативно вплинути на суспільну довіру до судової влади у зв'язку з призначенням такого кандидата на посаду судді [11].

Підтримуючи цю ідею, вважаємо, що її реалізація передбачає запровадження серед заходів проведення спеціальної перевірки щодо кандидата на посаду судді психофізіологічне опитування із застосуванням поліграфа (за аналогією із ст. 24 Закону України "Про Бюро економічної безпеки України", ст. 26 Закону України "Про Державне бюро розслідувань").

Метою такого дослідження є виявлення корупційних ризиків, а також можливих правопорушень, вчинених у минулому особою, яка претендує на посаду в суді, виявлення серед кандидатів осіб з ознаками девіантної поведінки (форм особистої поведінки кандидата, що суперечать загальноприйнятим моральним або правовим (дисциплінарним) нормам), утрудненої або уповільненої адаптації, несформованої мотивації або поведінки, яка не відповідає критерію доброчесності чи професійної етики, або виявлення інших

обставин, які можуть негативно вплинути на суспільну довіру до судової влади у зв'язку з призначенням такого кандидата на посаду судді.

Результати психофізіологічного дослідження із застосуванням детектора брехні не є підставою для ухвалення рішення про відмову особі в обійманні посади, а використовуватимуться під час проведення співбесіди виключно як інформація ймовірного характеру, яка сприяє формуванню оцінювання кандидата. Відмова кандидата від участі в психофізіологічному дослідженні із застосуванням комп'ютерного поліграфа є підставою для відмови в розгляді його кандидатури.

Таке опитування із застосуванням комп'ютерного поліграфа особи за її згодою може проводитися у ході службової перевірки або у разі переведення судді до іншого суду. Порядок проведення психофізіологічного дослідження із застосуванням поліграфа затверджуватиме Вища рада правосуддя України, при якій доцільно створити Центр системи виявлення прихованої або недостовірної інформації.

Отже, кіберзахищені комп'ютерні системи детекції брехні можуть використовуватися з метою забезпечення охорони державної безпеки від зовнішніх і внутрішніх загроз, а також встановлення відповідності кандидатів на окремі види публічної служби критерію доброчесності чи професійної етики, виявлення серед них осіб з ознаками девіантної поведінки, або інших обставин, які можуть негативно вплинути на суспільну довіру до правоохоронних органів або органів судової влади у зв'язку з призначенням такого кандидата на посаду представника правоохоронного органу чи судді.

Застосування комп'ютерного поліграфа згідно з міжнародними стандартами дозволяє ефективно вирішувати завдання: 1) забезпечення прозорої кадрової політики, об'єктивності у разі прийняття на публічну службу, зокрема підвищення ефективності добору кандидатів на посади судді; 2) проведення службових розслідувань (перевірок); 3) виявлення та запобігання корупції, а також інших ризиків, що можуть виникати у процесі діяльності посадових і службових осіб, які перебувають на публічній службі [11].

Зазначені завдання можуть бути вирішені за допомогою якісного та професійного психофізіологічного дослідження із застосуванням комп'ютерного поліграфа для отримання ймовірної та орієнтувальної інформації, яку іншим способом отримати не можливо.

Ефективне вирішення наявних завдань зумовлене потребою реалізації державної політики у сфері безпеки і оборони, що має відповідати актуальним потребам сучасності та формату взаємодії з країнами-членами НАТО [12].

12 червня 2020 року НАТО визнала Україну партнером з розширеними можливостями. Цей статус є частиною ініціативи НАТО з питань взаємодії, підтримки і поглиблення співпраці між країнами-членами та партнерами Альянсу.

Напрям активізації військово-технічного співробітництва з міжнародними партнерами для залучення інноваційних технологій є важливим аспектом воєнної безпеки щодо реформування й розвитку сектору безпеки і оборони України [13; 14].

Психофізіологічне дослідження із застосуванням комп'ютерного поліграфа складно уявити за відсутності належної освіти (підготовки та перепідготовки) поліграфологів на основі міжнародних стандартів і професійного застосування спеціального високотехнологічного інструментарію – комп'ютерного поліграфа (computerized polygraph system). У контексті зазначеного ключовими питаннями є: використання спеціальних методик – високотехнологічного інструментарію (computerized polygraph system), спеціального програмного забезпечення (polygraph software), які

відповідають вимогам кібербезпеки та міжнародним стандартам (ASTM International); професійна діяльність поліграфолога відповідно до кодексу Етики (Code of Ethics) поліграфолога, який рекомендований Американською Асоціацією Поліграфологів (American Polygraph Association) [15].

За цими рекомендаціями поліграфолог у своїй діяльності повинен дотримуватись таких правил Кодексу Етики: 1) не порушувати норми чинного законодавства; 2) не зловживати своїм службовим становищем; 3) не розповсюджувати службову інформацію; 4) не проводити дослідження у разі конфлікту інтересів; 5) не брати участь у інформаційних або публічних заходах, які не відповідають умовам проведення психофізіологічного дослідження; 6) не передавати персональні дані; 7) не брати участь у діяльності громадських організацій без дозволу керівництва (на посаді в державних органах); 8) не надавати неправдиву або недостовірну інформацію; 9) не проводити дослідження, якщо суб'єкт фізично або психічно непридатний; 10) не проводити дослідження у разі прямого підпорядкування особі, яка є суб'єктом дослідження; 11) не вимагати та не приймати гонорари, грошові винагороди, подарунки тощо [16].

Вважаємо, що для підвищення кібербезпеки інформації (Information Protection and Cyber Security) поліграфологам слід дотримуватися таких заходів: 1) захист паролем: поліграфологи повинні використовувати надійні паролі для захисту своїх пристроїв і облікових записів, рекомендується використовувати двох факторну автентифікацію; 2) шифрування: конфіденційна інформація повинна бути зашифрована, щоб запобігти несанкціонованому доступу; 3) резервне копіювання даних: важливо регулярно створювати резервні копії даних, щоб захистити від втрати або пошкодження; 4) захист брандмауером: для фільтрації шкідливого та потенційно небезпечного контенту та з'єднань, брандмауер слід використовувати для блокування несанкціонованого доступу до мережі та пристроїв поліграфолога. 5) регулярні оновлення: поліграфологи повинні регулярно оновлювати програмне забезпечення та програми для захисту від кібер вразливостей; 6) програмне забезпечення комп'ютерного поліграфа: необхідно встановлювати за прикладом інструктора; 7) ноутбук повинен мати програму: Microsoft Word (або еквівалент) для написання звітів та Adobe Free Reader для опрацювання наукової літератури; 8) застосування ноутбука: тільки для поліграфологічних завдань; 9) поінформованість поліграфолога про кібербезпеку, регулярне підвищення кваліфікації щодо актуальних технологій і інновацій у сфері інформаційної безпеки.

Для забезпечення конфіденційності та безпеки інформації при застосуванні програмного забезпечення комп'ютерних поліграфів бажано скористатися існуючим позитивним зарубіжним досвідом у сфері кіберзахисту інформації і персональних даних, врахування якого сприятиме удосконаленню правового регулювання застосування систем виявлення прихованої та недостовірної інформації.

Зокрема, американський досвід свідчить про суворе дотримання виробниками політики санкціонованого продажу комп'ютерних поліграфів згідно ліцензії на експорт. Заслуговує на увагу й успішний досвід підготовки поліграфологів, що передбачає: базовий курс навчання поліграфологів (Basic Polygraph Examiner Course), курс тестування осіб, які вчинили сексуальні злочини (PCSOT Course), та інші курси підвищення кваліфікації (Advanced Examiner's Course). Важливим аспектом є проведення психофізіологічного дослідження із застосуванням детектора брехні та інтерпретації отриманих результатів згідно з міжнародними стандартами ASTM International: ASTM E1954-05(2017) та ASTM E2229-09(2018) [15; 16].

Висновки.

Професійне застосування систем психофізіологічного виявлення прихованої і недостовірної інформації (Research in Psychophysiological Detection of Deception (Polygraph) та програмного забезпечення, яке відповідає вимогам кібербезпеки (polygraph software), сприяє ефективному й оперативному вирішенню ключових завдань: 1) судової експертизи із застосуванням спеціального засобу комп'ютерного поліграфу; 2) реалізації прозорої кадрової політики – під час прийняття на публічну службу в правоохоронних органах, її проходження, службових розслідувань (перевірок); 3) застосування комп'ютерного поліграфа для добору кандидатів на посаду судді під час спеціальної перевірки, службових розслідувань, а також переведення до іншого суду.

Враховуючи викладене, існує потреба у посиленні заходів державного контролю з дотриманням вимог чинного законодавства у сфері технічного та криптографічного захисту інформації щодо: застосування систем детекції брехні, які відповідають нормативно-правовим актам у сфері кіберзахисту інформації; закупки обладнання та програмного забезпечення у надійного постачальника; застосування комплексних систем захисту інформації з підтвердженою відповідністю.

Особливої уваги потребують: 1) захищені системи з доступом в Інтернет і рішення для віддаленого доступу (Secure Internet-facing systems and remote access solutions); 2) рішення для захисту від зловмисного програмного забезпечення (Anti-malware solutions and endpoint). Це має посилити спроможності національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі та перспективі створення об'єднання (U-24. United for peace) Союзу відповідальних держав [17].

Вважаємо, що напрямами удосконалення забезпечення кіберзахисту за допомогою застосування систем виявлення прихованої та недостовірної інформації є: 1) розробка єдиної системи підготовки поліграфологів та проведення дослідження; 2) запровадження вітчизняного кодексу Етики поліграфолога; 3) розгляд питання внесення змін до Кримінального процесуального кодексу України для надання висновку поліграфолога статусу доказу у кримінальному провадженні; 4) перевірка обладнання та програмного забезпечення, що застосовується під час досліджень (polygraph equipment, software) на відповідність вимогам законодавства та кібербезпеки; 5) розробка та запровадження "Інструкції про порядок організації та проведення поліграфологічних досліджень у системі судової влади України" (у разі внесення відповідних змін до Закону України "Про судоустрій і статус суддів").

Актуальним напрямом подальшої взаємодії в безпековій сфері з державами-членами НАТО є ефективне застосування комп'ютерних систем виявлення прихованої і недостовірної інформації у складових сектора безпеки і оборони України та органах судової влади із використанням досвіду країн-членів НАТО, що зумовлюється потребою переходу на єдині міжнародні стандарти [18].

Це дозволить запровадити новітні підходи та технології, які ефективно застосовуються країнами-членами НАТО у сфері виявлення прихованої та недостовірної інформації. Такий підхід враховуватиме найкращі європейські практики й світові стандарти в секторі безпеки і оборони України та сприятиме подальшій системній інтеграції України до Європейського Союзу та НАТО [19].

Використана література

1. LB.UA. Російські хакери посилюють кібератаки на цивільні цілі, щоб тероризувати українців. – (Посадовець АНБ). URL: https://lb.ua/society/2023/01/12/542313_rosiyski_hakeri_posilyuyut.html

2. Papers of William Moulton Marston, 1852-1975. Lie detectors and detection. United States. URL: https://hollisarchives.lib.harvard.edu/repositories/8/resources/9462

3. John Larson. The Polygraph Museum John Larson's Breadboard Polygraph. URL: http://www.lie 2me.net/thepolygraphmuseum/id16.html

4. Krapohl, D., & Rosales T. (2014). Decision Accuracy for the Relevant-Irrelevant Screening Testing: A Partial Replication. Polygraph. 43(1)(1), 20-29. URL: https://polygraph.org/docs/decision_ accuracy_of_the_ri_screening_test.pdf

5. Outside continental United States (OCONUS) polygraph program implementation. Chip Morgan, Gil Witte, Ben Blalock. URL: https://peakcatc.com/downloads/oconus.pdf

6. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

7. Про Стратегію кібербезпеки України: Рішення Ради національної безпеки і оборони України від 14.05.21 р., введено в дію Указом Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013

8. Victor Zhora. State Service of Special Communications and Information Protection of Ukraine. Russia's Cyber Tactics: Lessons Learned. 2022. URL: https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-aga inst-ukraine

9. CERT-UA. Кібератака, спрямована на порушення цілісності та доступності державних інформаційних ресурсів (CERT-UA#6060). URL: https://cert.gov.ua/article/3947787

10. Під головуванням Президента України Володимира Зеленського відбулося засідання РНБО України. URL: https://www.rnbo.gov.ua/ua/Diialnist/6430.html

11. Про прискорення судової реформи та подолання проявів корупції у системі правосуддя: Рішення Ради національної безпеки і оборони України від 23.06.23 р., введено в дію Указом Президента України від 30.06.23 р. № 359. URL: https://www.president. gov.ua/documents/ 3592023-47185

12. НАТО визнає Україну партнером з розширеними можливостями. URL: https://www.nato. int/cps/uk/natohq/news_176327.htm

13. Про Стратегію національної безпеки України: Рішення Ради національної безпеки і оборони України від 14.09.20 р., введено в дію Указом Президента України від 14.09.20 р. № 392/2020. URL: https://www.president.gov.ua/documents/3922020-35037

14. Про Стратегію воєнної безпеки України: Рішення Ради національної безпеки і оборони України від 25.03.21 р., введено в дію Указом Президента України від 25.03.21 р. № 121. URL: https://www.president.gov.ua/documents/1212021-37661

15. ASTM International. URL: https://www.astm.org

16. American Polygraph Association. URL: https://www.polygraph.org

17. Промова Президента України Володимира Зеленського перед Конгресом США від 16 березня 2022 р. URL: https://www.president.gov.ua/news/promova-prezidenta-ukrayini-volodimira-zelenskogo-pered-kong-73609.

18. Microsoft. Clint Watts - General Manager, Digital Threat Analysis Center. Preparing for a Russian cyber offensive against Ukraine this winter. URL: https://blogs.microsoft.com/on-the-issues/ 2022/12/03/preparing-russian-cyber-offensive-ukraine

19. Казьмірук С.Д., Морган К.Ч., Міщенко В.О. Правові основи запровадження інноваційних систем виявлення прихованої і недостовірної інформації та комп'ютерних поліграфів у секторі безпеки і оборони України. *Часопис Київського університету права.* 2022. № 1. URL: http://kul.kiev. ua//images//A/Chasopis/CHAS22_1.pdf

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~