

М. Уткіна,
доктор юридичних наук, доцент,
доцент кафедри кримінально-правових дисциплін та судочинства
Навчально-наукового інституту права
Сумського державного університету

ЦИФРОВІ ТЕХНОЛОГІЇ: ВИКЛИК ЧИ МОЖЛИВІСТЬ ДЛЯ ПРОТИДІЇ ФІНАНСОВІЙ ЗЛОЧИННОСТІ?¹

Постановка проблеми. На сучасному етапі розвитку цифрові технології докорінно змінюють фінансовий сектор, підходи до його регулювання, відкриваючи нові можливості для розвитку економіки, підвищення рівня безпеки фінансових операцій, протидії й боротьби із фінансовими злочинами. У той же час, слід констатувати, що поряд із новими можливостями, ці технології та цифровізація в цілому створює і нові серйозні виклики, сприяючи зміні підходів до фінансової злочинності та появи нових схем шахрайства. Дані виклики вимагають відповідного нормативно-правового регулювання та ефективних заходів контролю.

З одного боку, цифровізація сприяє автоматизації процесів моніторингу, аналізу та виявлення підозрілих транзакцій, допомагаючи правоохоронним органам і фінансовим установам ефективніше протидіяти фінансовій злочинності. З іншого боку, зловмисники активно використовують інновації, зокрема криптовалюти, штучний інтелект, блокчейн технології й анонімні транзакції, щоб ухилятися від контролю та здійснювати фінансові махінації.

Аналіз останніх досліджень і публікацій. Аналізуючи роботи

представників наукової спільноти, слід наголосити, що останнім часом питання використання цифрових технологій в контексті протидії фінансовій злочинності дедалі частіше є предметом досліджень. Зокрема, К. Озілі, К. Маркевич, Б. Депутат, Г. Матвієнко В. Літкевич та ін. розглядали питання використання новітніх цифрових технологій (штучного інтелекту, технології блокчейн) й ін. як одних із можливих та дієвих в системі протидії фінансовій злочинності.

Постановка завдання. Відповідно до зазначеного вище, метою статті є комплексний аналіз можливостей застосування цифрових технологій в контексті протидії фінансовій злочинності й розгляду їх позитивних та проблемних аспектів.

Виклад основного матеріалу. З урахуванням зазначеного, питання цифрових технологій у сфері фінансової безпеки має двоїстий характер: вони можуть бути як потужним інструментом у боротьбі з фінансовими злочинами, так і засобом їх ускладнення та розширення.

Цифровізація розглядається як тривалий процес (в усіх сферах), при якому відбувається перехід на цифрові технології задля того, аби модернізувати кожен з напрямів і в цілому

¹ Робота виконана в рамках проекту «Інтеграційна парадигма цифрової трансформації в системі протидії фінансовій злочинності: синергетичний підхід до превенції та боротьби» (номер державної реєстрації 0125U000602).



систему роботи, продуктивності тощо [1, с. 84]. Автори в ході проведеного дослідження визначили функції цифровізації:

– фінансовий контроль та регулювання (цифровізація сприяє прозорості у розподілі, залученні і використанні ресурсів);

– фінансовий аналіз – завдяки процесам автоматизації збору, опрацювання і зберігання даних забезпечується швидкий доступ до актуальної інформації для планування і коригування бюджетів на макро-, мезо-, мікрорівнях;

– комунікативна функція – цифровізація створенню ефективних комунікацій як у рамках управлінської ієрархії, так і на міжгалузевому рівні, забезпечуючи обмін інформацією та координацію між учасниками різних сфер або всередині конкретної галузі;

– підвищення ефективності використання ресурсів забезпечується завдяки більш об'єктивному розподілу фінансів з урахуванням результативності проектів, на які вони спрямовуються, а також заощадженню коштів через перехід від паперових процесів до електронного адміністрування [1, с. 84].

І. Грабчук, Д. Кусяк та Р. Макуха також підкреслили використання цифрових технологій для діагностики проблем в багатьох сферах економіки, а також і для повсякденних завдань [2, с. 21]. Проте, тотальна цифровізація суспільства має зворотній бік, негативним проявом якого є поява нових кримінальних ризиків [3, с. 171]. О. Шевченко та Л. Рудич [4] наголошують на необхідності дотримання збалансованого підходу в сфері державного регулювання процесів цифровізації: з одного боку створювати умови для впровадження сучасних цифрових інструментів та технологій, а з іншого – організувати належний контроль для мінімізації ризиків, пов'язаних з їх впровадженням.

Останніми роками цифрові технології стали важливим інструментом

боротьби з фінансовими злочинами, особливо завдяки використанню штучного інтелекту, аналізу великих даних та блокчейн-технологій. Проте, також необхідно зазначити і трансформативний характер фінансових злочинів, що викликає основну складність у протидії та боротьбі із ними. Фінансові злочини часто охоплюють кілька юрисдикцій, що дозволяє злочинцям використовувати різні правові системи для приховування походження незаконних коштів. Відсутність єдиних стандартів і недостатня координація між країнами сприяють розвитку таких злочинів [5, с. 164]. З урахуванням цього, використання цифрових технологій може слугувати потужним інструментом у боротьбі з фінансовими злочинами.

Розглядаючи можливості цифровізації в цілому та цифрових технологій зокрема, слід наголосити, що штучний інтелект, машинне навчання та технології блокчейн можуть слугувати й використовуватись із метою автоматичного виявлення підозрілих операцій та аналізу транзакцій у реальному часі, що є надзвичайно важливим. З урахуванням того, що зазначені технології дають змогу провадити автоматизований моніторинг транзакцій, це значно знижує ризик шахрайства й інших злочинних дій.

Аналізуючи цифрові технології в контексті протидії фінансовій злочинності, у першу чергу, увагу слід звернути на доцільність і можливість застосування й використання штучного інтелекту. Звертаючись до визначення категорії «штучний інтелект», слід зазначити, що серед представників наукової спільноти відсутня єдність щодо трактування категорії. Зокрема, Oxford English Dictionary [6] визначає «штучний інтелект» як (1) здатність комп'ютерів або інших машин демонструвати або імітувати інтелектуальну поведінку; галузь дослідження, пов'язану з цим; (2) програмне забезпечення, яке використовується для виконання



завдань або отримання результатів, які раніше вважалися потребуваними людського інтелекту, особливо за допомогою машинного навчання для екстраполяції великих колекцій даних. Ю. Кравицький [7, с. 92] та М. Великанова [8, с. 186] зазначають, що наразі підходи до розуміння категорії «штучний інтелект» варіюються від ототожнення із робототехнікою до сприйняття штучного інтелекту як інноваційного напрямку розвитку науки й техніки, що спрямований на створення інтелектуальних машин та інтелектуальних комп'ютерних програм. Таким чином, питання дослідження категорії «штучний інтелект» має необхідність у подальшому дослідженні й уточненні його ролі та можливостей використання у різних сферах життєдіяльності та галузях.

З урахуванням зазначеного вище, й повертаючись до використання штучного інтелекту у протидії фінансовій злочинності, слід наголосити на його можливостях для автоматизації процесів моніторингу та аналізу фінансових транзакцій, виявляючи аномальні та підозрілі операції. Доцільність й актуальність використання штучного інтелекту щодо протидії фінансовій злочинності, у першу чергу, обґрунтовується можливістю аналізу величезних обсягів даних, інформації в режимі реального часу (*real-time tracking*), виявляючи аномалії та незвичайні паттерни, які можуть свідчити про можливі фінансові злочини. Підозрілими фінансовими операціями (діяльністю) відповідно до Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення» [9] вважаються такі фінансові операції або спроба їх проведення незалежно від суми, на яку вони проводяться, якщо суб'єкт первинного фінансового моніторингу має підозру або має достатні підстави для підозри, що вони є результатом

злочинної діяльності або пов'язані чи стосуються фінансування тероризму або фінансування розповсюдження зброї масового знищення. Такий аналіз значного обсягу інформації в режимі реального часу дозволяє своєчасно реагувати на загрози, а таким чином, забезпечити стабільність фінансової системи від загроз і викликів.

Проте, слід наголосити, що різний рівень доступу країн світу до технологій штучного інтелекту, а також значні відмінності в антилегалізаційних підходах країн визначають порядок денний міжнародних організацій. Зокрема, це стосується використання можливостей штучного інтелекту для вдосконалення кримінальних механізмів протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, а також розробки інструментів міжнародного контролю за фінансовими потоками. Використання штучного інтелекту у зазначеній вище сфері також вимагає розробки правових стандартів щодо відповідальності за прийняття рішень системами ШІ та захисту персональних даних, оброблюваних такими системами. За В. Літкевичем [10] наразі на міжнародному рівні відбувається активне формування глобальних принципів і правил щодо застосування штучного інтелекту, зокрема і у сфері протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом. Ці напрацювання стають основою для подальшого створення нормативно-правових рамок, що регулюватимуть належне використання систем штучного інтелекту у зазначеній сфері.

Слід також наголосити на важливості подальшого удосконалення національного законодавства зокрема шляхом гармонізації його положень щодо правого регулювання застосування штучного інтелекту у відповідності до міжнародних стандартів та європейських положень.

Наступною категорією, яку потрібно розглянути в контексті про-



тидії фінансовій злочинності, є технології Big Data (аналіз великих даних), що безпосередньо дозволяє обробляти великі масиви інформації, виявляючи закономірності, що можуть вказувати на шахрайство або відмивання коштів. Аналізуючи визначення категорії Big Data, знаходимо визначення у Звіті Європейського банківського управління про великі дані та розширену аналітику (EBA Report on Big Data and Advanced Analytics) [11]. У Звіті зазначено, що категорія «Big Data» стосується технологічних розробок, пов'язаних із збором, зберіганням, аналізом і додатками даних, що часто характеризується збільшенням обсягу, швидкості та різноманітності створюваних даних (три V – volume, velocity and variety) і зазвичай стосується (але не обмежується) даними з Інтернету. Великі дані відносяться до динамічних і величезних обсягів даних, які створюються людьми, інструментами та машинами з постійно зростаючою швидкістю [2, с. 22].

Виходячи із цього, Big Data також відіграє значну роль у протидії фінансовій злочинності, забезпечуючи ефективний аналіз великих обсягів транзакційної інформації, виявлення аномалій та прогнозування загроз. Використання технологій Big Data значно підвищує ефективність боротьби з фінансовою злочинністю, дозволяючи:

- виявляти шахрайські схеми. Зокрема, завдяки аналізу поведінкових паттернів користувачів та транзакційних даних, Big Data дозволяє ідентифікувати підозрілі операції та запобігати фінансовим махінаціям, таким як, шахрайство з кредитними картками, фальсифікація транзакцій й легалізація доходів, одержаних шляхом;

- провадити автоматизований моніторинг та аналітику. Використання алгоритмів машинного навчання на основі великих даних дає змогу автоматично аналізувати великі

обсяги фінансових операцій у режимі реального часу, що значно прискорює виявлення потенційних загроз;

- протидіяти кіберзлочинності. Використання Big Data сприяє виявленню та запобіганню кіберзагрозам (зокрема, це атаки на банківські системи, крадіжка персональних даних та злам фінансових акаунтів);

- здійснювати аналіз соціальних зв'язків (Social Network Analysis). За допомогою аналізу взаємозв'язків між особами та організаціями можна виявляти так звані фінансові злочинні мережі та відстежувати рух коштів між різними учасниками економічних процесів;

- прогнозувати фінансові ризики. Зокрема, моделі прогнозного аналізу на основі Big Data дозволяють фінансовим установам заздалегідь виявляти ризики та вживати заходів для їх мінімізації, запобігаючи фінансовим злочинам ще до їх реалізації.

Проте, слід погодитись із позицією Н.Вакшинської та О. Шандрівської [12, с. 247], які виокремили також, окрім позитивних аспектів використання технологій Big Data, наголошено й на ризиках та небезпеках. Зокрема, науковці виокремили наступні:

- безпека даних;
- недостатня якість даних;
- етичні питання;
- залежність від технологій;
- великий обсяг затрат.

Таким чином, використання технологій Big Data значно підвищує ефективність протидії фінансовій злочинності, дозволяючи виявляти шахрайські схеми, аналізувати ризики та забезпечувати відповідність регуляторним вимогам. Проте, для досягнення максимальної ефективності важливо розвивати алгоритми аналізу даних, забезпечувати їхню безпеку та узгоджувати із законодавчими нормами.

Наступними напрямками цифровізації фінансового сектору є Regulatory Technology (RegTech). Завдяки авто-



матизованим рішенням у сфері комплаєнсу (відповідності регуляторним вимогам), RegTech допомагає фінансовим установам забезпечувати швидку та точну перевірку клієнтів (KYC – Know Your Customer); виявляти підозрілі операції та формувати звіти для регуляторних органів; використовувати аналітичні інструменти для прогнозування ризиків. А AML-системи є тісно інтегрованими в RegTech і спрямовані на виявлення та запобігання легалізації доходів, одержаних злочинним шляхом. Використання цих технологій є критично важливим у контексті протидії фінансової злочинності.

Особливу увагу необхідно звернути на технологію блокчейн, на основі якої функціонує криптовалютна індустрія. «Блокчейн» слід розглядати як очевидні та стійкі до втручання цифрові «книжки» (або ж системи), реалізовані розподіленим способом (тобто без центрального сховища) і зазвичай без центрального органу (тобто банку, компанії чи уряду) [13]. Зокрема, Ю. Калайда зазначає, що технологія блокчейн має такі переваги: 1) стабільність; 2) безпечність; 3) прозорість роботи з даними; 4) транскордонний характер операцій з обміну даними [3, с. 177].

На сьогодні існує широкий спектр сфер та способів застосування технології блокчейн, що зумовлено її численними перевагами. Зокрема, ця технологія сприяє: скороченню кількості посередників та зниженню вартості міжнародних переказів; оптимізації процесів фінансування торгівлі та спрощенню міжнародних торговельних операцій; зменшенню ризику людських помилок і забезпеченню цілісності записів у бухгалтерському обліку та аудиті. Крім того, блокчейн пришвидшує оформлення кредитів під заставу завдяки смарт-контрактам, які автоматично ініціюють певні події, такі як здійснення платежів або повне погашення кредиту. Також ця технологія забезпечує безпечний та зруч-

ний механізм перевірки та передачі прав власності при реєстрації операцій з нерухомістю. Шифрування, як невід’ємна складова блокчейну, відіграє важливу роль у захисті даних, протидії відмиванню грошей та збереженні конфіденційності особистої інформації [2, с. 24].

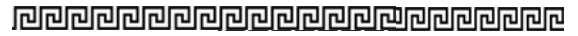
З урахуванням зазначеного вище, цифровізація й цифрові технології суттєво змінюють фінансовий сектор, сприяючи підвищенню ефективності регулювання, зміцненню безпеки фінансових операцій і створенню нових механізмів протидії фінансовим злочинам. Використання сучасних технологій, зокрема штучного інтелекту, аналізу великих даних (Big Data), блокчейну та RegTech, дозволяє автоматизувати процеси моніторингу, виявлення підозрілих операцій і прогнозування ризиків.

Однак, поряд із перевагами, виникають і нові виклики. Відмінності в доступі країн до технологій та різні підходи до регулювання створюють труднощі у впровадженні єдиних стандартів боротьби з фінансовими злочинами. Кіберзлочинці також активно використовують цифрові інструменти для того, щоб обійти системи контролю, що ускладнює виявлення та запобігання фінансовим махінаціям.

До основних викликів цифрових технологій у протидії фінансовій злочинності слід виокремити наступні:

- кіберзагроза та безпека даних. Використання цифрових технологій збільшує ризик кібератак, витоків даних та маніпуляцій із фінансовою інформацією, оскільки кіберзлочинці застосовують новітні методи для обходу систем безпеки, зокрема атаки на алгоритми штучного інтелекту та розподілені фінансові реєстри (блокчейн). Також в контексті даної загрози слід виокремити відсутність належного захисту даних у фінансових установах, що створює загрозу їх компрометації та зловживання;

- недостатність нормативно-правового правового регулювання. Дана



проблема виникає через відсутність єдиних міжнародних стандартів у регулюванні цифрових фінансових технологій, що, у свою чергу, ускладнює боротьбу з фінансовими злочинами, що мають транскордонний характер. Регуляторні органи не завжди встигають адаптуватися до стрімкого розвитку технологій, а також можливість виникнення складнощів з визначенням відповідальності за рішення, ухвалені на основі штучного інтелекту, особливо у випадках фінансових порушень.

– використання цифрових технологій для скоєння фінансових злочинів. Цифрові можливості, цифрові технології доволі часто використовуються для легалізації доходів, одержаних злочинним шляхом, ухилення від оподаткування та фінансування незаконної діяльності. Це означає, що такі зазначені нами цифрові рішення як штучний інтелект та машинне навчання, технологія блокчейн можуть використовуватися не лише для протидії шахрайству, а й для його вдосконалення, створення підроблених цифрових ідентичностей та автоматизації шахрайських схем;

– етичні питання та захист персональних даних. Автоматизований моніторинг транзакцій може порушувати конфіденційність та права людини, особливо якщо державні органи отримують безконтрольний доступ до фінансової інформації громадян. Аналіз Big Data може призводити до дискримінації або упереджених рішень через алгоритмічні помилки та некоректне трактування даних. Використання біометричних даних та технологій розпізнавання обличчя у фінансовому секторі викликає питання щодо збереження приватності;

– технологічні бар'єри та нерівномірний доступ до цифрових інструментів. Різний рівень доступу до сучасних технологій у різних країнах створює дисбаланс у протидії фінансовим злочинам.

Висновки. Зважаючи на зазначене вище, слід констатувати, що цифровізація фінансового сектору відкриває нові можливості для ефективної протидії фінансовим злочинам, проте водночас створює низку викликів, що вимагають вдосконалення правового регулювання та запровадження сучасних механізмів контролю. Використання RegTech, AML-систем, штучного інтелекту та технології блокчейн сприяє підвищенню прозорості фінансових операцій та зниженню рівня фінансової злочинності. Водночас для ефективного функціонування цих технологій необхідно адаптувати правові механізми до сучасних умов цифрової трансформації фінансового сектору.

Цифровізація фінансового сектору наразі розглядається через призму нових можливостей у сфері протидії фінансовій злочинності. Проте, як неодноразово зазначалось представниками наукової спільноти, новітніх цифрові технології також наряду із можливостями створюють і нові виклики, що вимагають конкретних напрямів вирішення. Автор у статті аналізує роль цифрових технологій у системі протидії фінансовій злочинності, питання їх нормативно-правового регулювання, а також виклики, які постають перед правоохоронними органами, фінансовими інституціями та державними регуляторами. Стаття зосереджує увагу на впливі цифровізації на механізми запобігання й розслідування так званих фінансових злочинів, зокрема використання штучного інтелекту, технологій аналізу великих даних (Big Data) й блокчейн. Автор у статті також акцентує увагу на Regulatory Technology (RegTech) та AML-системах як одних із ключових компонентів цифровізації у сфері протидії фінансовій злочинності, що забезпеченню фінансової безпеки та прозорості.



Із урахуванням розвитку криптовалютного ринку, децентралізованих фінансових платформ постають нові виклики у сфері легалізації доходів, одержаних злочинним шляхом, та фінансування тероризму. Автор виокремлює сучасні підходи до питання їх регулювання, заходи міжнародних організацій щодо контролю за цифровими активами.

Стаття також розглядає питання кібербезпеки у фінансовій сфері, включаючи правові аспекти застосування біометричних технологій (зокрема використання біометричних даних), багаторівневої аутентифікації, а також систем моніторингу транзакцій у режимі реального часу. Було зазначено, що водночас цифрові технології потребують удосконалення правових механізмів для збереження балансу між фінансовою безпекою та правами користувачів. У статті автор робить висновок, що цифрові технології є не лише ефективним інструментом протидії фінансовим злочинам, а й потенційним джерелом формування нових загроз, зумовлюючи необхідність адаптації правових механізмів до сучасних умов цифрової трансформації фінансового сектору.

Ключові слова: протидія фінансовій злочинності, фінансова злочинність, фінансовий моніторинг, цифрова безпека, цифровізація.

Utkina M. Digital Technologies: a Challenge or an Opportunity for Combating Financial Crime?

The digitalisation of the financial sector is currently viewed through the prism of new opportunities in the field of combating financial crime. However, as repeatedly noted by representatives of the scientific community, along with opportunities, new digital technologies also create new challenges that require specific areas

of solution. The article's author analyses the role of digital technologies in combating financial crime, the issues of their regulatory and legal regulation, and the challenges facing law enforcement agencies, financial institutions and state regulators. The article focuses on the impact of digitalisation on the mechanisms of prevention and investigation of so-called financial crimes, particularly the use of artificial intelligence, big data analysis technologies (Big Data) and blockchain. The article's author also focuses on regulatory technology (RegTech) and AML systems as one of the key components of digitalisation in combating financial crime and ensuring financial security and transparency.

Considering the development of the cryptocurrency market and decentralised financial platforms, new challenges arise in money laundering and terrorist financing. The author highlights modern approaches to the issue of their regulation and measures of international organisations to control digital assets.

The article also considers the issue of cybersecurity in the financial sector, including the legal aspects of using biometric technologies (in particular, biometric data), multi-level authentication, and real-time transaction monitoring systems. It was noted that, at the same time, digital technologies require the improvement of legal mechanisms to maintain a balance between financial security and user rights. In the article, the author concludes that digital technologies are an effective tool for combating financial crimes and a potential source of new threats, making it necessary to adapt legal mechanisms to modern conditions of digital transformation in the financial sector.

Key words: combating financial crime, financial crime, financial monitoring, digital security, digitalisation.

**Література:**

1. Шендерківська Л., Букань Л. Цифровізація: актуальні завдання, які вона вирішує / IV Міжнародна науково-практична конференція «Бізнес, інновації, менеджмент: проблеми та перспективи». С. 84-85. <https://confmanagement-proc.kpi.ua/article/view/279871>.
2. Грабчук І., Кусяк Д., Макуха Р. Цифрові інструменти в боротьбі з візмиванням коштів та фінансуванням тероризму: основні характеристики. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство*. 2023. Випуск 47. С. 21-24.
3. Калайда Ю. Можливість блокчейн-технологій у розслідуванні кримінальних правопорушень, вчинених у кіберпросторі. *Інформація і право*. 2021. № 4 (39). С. 170-178.
4. Шевченко О., Рудич Л. Розвиток фінансових технологій в умовах цифровізації економіки України. *Ефективна економіка*. 2020. № 7. <http://www.economy.nauka.com.ua/?op=1&z=8053>.
5. Шаренко М., Чумаченко В. Роль міжнародного фінансового права у протидії відмиванню коштів. *Науковий вісник Ужгородського Національного університету. Серія: Право*. 2024. Випуск 86: частина 4. С. 163-167.
6. *Oxford English Dictionary*. URL: <https://surl.li/jokchb>
7. Кравицький Ю. Штучний інтелект як інструмент правової реформи: потенціал, тенденції та перспективи. *Науковий вісник Національної академії внутрішніх справ*. 2021. № 2 (119). С. 90-101. <https://orcid.org/0000-0002-7063-4725>
8. Великанова М. Штучний інтелект: правові проблеми та ризики. *Вісник Національної академії правових наук України*. 2020. Т. 27. С. 185-298. DOI: 10.37635/jnalsu.27(4).2020.185-198
9. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення : Закон України від 06 грудня 2019 р. № 361-IX. *Відомості Верховної Ради України*. URL: <https://zakon.rada.gov.ua/laws/show/361-20/conv#n591>
10. Літкевич В. Штучний інтелект у системі протидії відмиванню коштів: формування глобальних принципів і правил. *Scientific Review*. 2024. № 7 (99). DOI 10.26886/2311-4517.7(99)2024.2.
11. EBA Report on Big Data and Advanced Analytics. *European Banking Authority*. January 2020. URL: <https://surl.gd/mlukwy>
12. Вакишинська Н., Шандрівська О. Специфіка розвитку ринку Big Data для потреб відновлення економіки України в поствоєнний період. *Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку*. 2023. № 2 (9). С. 244-256.
13. Yaga, D., Mell, P., Roby, N., Scarfone, K. *Blockchain Technology Overview*. National Institute of Standards and Technology. 2018. 57 p. <https://doi.org/10.6028/NIST.IR.8202>

