РОЗДІЛ 9. КРИМІНАЛЬНИЙ ПРОЦЕС ТА КРИМІНАЛІСТИКА; СУДОВА ЕКСПЕРТИЗА; ОПЕРАТИВНО-РОЗШУКОВА ДІЯЛЬНІСТЬ

УДК 343.14
DOI https://doi.org/10.24144/2307-3322.2024.83.3.26

ЩОДО ПИТАННЯ ПРО ВИКОРИСТАННЯ ДОКАЗІВ, ОТРИМАНИХ З ВІДКРИТИХ ДЖЕРЕЛ, У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Бабаєва О.В.,
кандидат юридичних наук,
доцент кафедри кримінального процесу
Національного юридичного університету
імені Ярослава Мудрого

Авербах Д.В.,
студент 3 курсу
факультету міжнародного та європейського права
Національного юридичного університету
імені Ярослава Мудрого

Бабаєва О.В., Авербах Д.В. Щодо питання про використання доказів, отриманих з відкритих джерел, у кримінальному провадженні.

Стаття присвячена вивченню питання використання доказів, отриманих з відкритих джерел, у кримінальному провадженні. Звернено увагу на відсутність загальновизнаного визначення терміну «інформація з відкритих джерел», наведено перелік основоположних рис даного виду інформації, серед яких виокремлюють: 1) доступність інформації для широкого загалу; 2) автор інформації може бути не встановлений; 3) доступ до інформації може надаватися як на оплатній, так і на безоплатній основі. Наголошено на відсутності належного обсягу нормативно-правових актів, спрямованих на регулювання порядку використання доказів, отриманих з відкритих джерел.

Проаналізовано зміст Протоколу Берклі, який був створений Школою права Каліфорнійського університету в Берклі спільно з представниками Організації Об'єднаних Націй. Зокрема, наведено: перелік закріплених у Протоколі Берклі принципів, які поділяються на професійні, методологічні та етичні, їхній зміст; цикл розслідування, що викладений у Протоколі Берклі, та складається з наступних стадій: 1) онлайн-пошук; 2) попередня оцінка; 3) збір інформації; 4) збереження інформації; 5) верифікація інформації; 6) розвідувальний аналіз.

Звернено увагу на проблеми, які виникають у процесі використання доказів, отриманих з відкритих джерел. Досліджуються вимоги належності, допустимості та достовірності доказів, отриманих з відкритих джерел. Розглянуто стан регулювання питання використання доказів, отриманих з відкритих джерел в національному законодавстві. Виокремлено характерні ознаки електронних (цифрових) доказів, що відрізняють їх від інших видів доказів та обумовлюють необхідність виокремлення їх в кримінальному процесуальному законодавстві як окремого виду доказів. Розглянуто практику національних судових установ та Міжнародного кримінального суду, пов'язану з використанням доказів, отриманих з відкритих джерел. Підкреслено особливу роль даного виду доказів для встановлення обставин або складу злочинів проти основ національної безпеки, особливо з початку повномасштабної російської агресії проти України.

Ключові слова: кримінальне провадження**,** розвідка з відкритих джерел, Протокол Берклі, електронні (цифрові) докази, судова практика, Міжнародний кримінальний суд.

Babayeva O.V., Averbakh D.V. Regarding the question of usage of open-source evidence in criminal proceedings.

The article is devoted to the study of the issue of using open-source evidence in criminal proceedings. Attention is drawn to the lack of a universally recognized definition of the term "open-source information", a list of fundamental features of this type of information is provided, among which are: 1) accessibility of the information to the general public; 2) the author of the information may not be determined; 3) access to information can be provided both on a paid and free basis. The lack of an adequate volume of legislation aimed at regulating the procedure for usage of open-source evidence is emphasized.

A study of the Berkeley Protocol, which was created jointly by the University of California, Berkeley School of Law and representatives of the United Nations, was carried out. In particular, the following is outlined: a list of the principles enshrined in the Berkeley Protocol, divided into professional, methodological and ethical, their content; the investigation process put forward in the Berkeley Protocol, that consists of the following stages: 1) online inquiries; 2) preliminary assessment; 3) collection of information; 4) preservation of information; 5) verification of information; 6) investigative analysis.

Problems that may arise in the process of using open-source evidence are emphasized. The requirements of propriety, admissibility and reliability of open-source evidence are studied. The state of legal regulation of the issue of the usage of open-source evidence in national legislation is considered. The specific features of electronic (digital) evidence are singled out, which distinguish them from other types of evidence and determine the need to separate them in the criminal procedural legislation as a different type of evidence. The practice of national and international judicial institutions related to the use of open-source evidence is considered. The special role of this type of evidence for establishing the corpus delicti or circumstances of crimes against the foundations of national security, especially since the beginning of full-scale Russian aggression against Ukraine, is emphasized.

Key words: criminal proceedings, open-source intelligence, Berkeley Protocol, electronic (digital) evidence, court practice, International Criminal Court.

Постановка проблеми. Всеохоплююча діджиталізація життєдіяльності людини вимагає від органів кримінальної юстиції, у боротьбі зі злочинністю, здійснювати пошук та збір інформації не тільки у їх традиційному розумінні, з матеріальних носіїв, а й з відповідних інформаційних ресурсів. Так, поряд з традиційними процесуальними джерелами доказів, серед яких показання, документи, висновки експертів та речові докази, зростає роль електронних (цифрових) доказів, зокрема тих, що можуть бути отримані з відкритих джерел. Концепція добування і використання інформації з відкритих джерел для оцінки загроз, прийняття рішень або відповіді на конкретні запитання відома як OSINT (абревіатура від Open-Source Intelligence, укр. розвідка на основі відкритих джерел). Основними джерелами OSINT є засоби масової інформації, Інтернет, відкриті державні дані, наукові публікації, тощо. Методи OSINT активно використовується в багатьох галузях людської діяльності, включаючи журналістику, бізнес, кібербезпеку та розвідку. У зв'язку з цим у доктрині постає питання про можливість використання засобів OSINT під час здійснення кримінального провадження.

Аналіз останніх досліджень і публікацій. Дослідженню питання використання доказів отриманих з відкритих джерел у кримінальному процесі присвячені роботи таких іноземних вчених як Е. де Бюссер, П. Левуліс, Ф. Семпсон, Е. Стеніфорт, С. Тревізан, Л. Фріман, К. Хайатт та інших. З огляду на його актуальність, дане питання активно розглядається також вітчизняними вченими, серед яких, зокрема, Д.О. Алєксєєва-Процюк, Н.М. Ахтирська, Ю.О. Виходець, О.В. Малахова, А.В. Ратнова, А.В. Скрипник, Г.К. Тетерятник. На особливу увагу заслуговує новітній підручник О.О. Торбаса під назвою "OSINT при розслідуванні кримінальних правопорушень", в якому найбільш детально висвітлено питання використання даних із відкритих джерел у процесі здійснення кримінальних проваджень. Необхідність подальшого вивчення даного питання обумовлена неоднорідним характером практики судових органів та неналежним рівнем нормативно-правового врегулювання, що призводить до значного рівня невизначеності.

Мета статті - дослідити практику національних та міжнародних судових органів у питанні використання доказів отриманих з відкритих джерел, нормативно-правове регулювання використання даної категорії доказів.

Виклад основного матеріалу. Термін "інформація з відкритих джерел", незважаючи на досить активне його використання, не має єдиної загальновизнаної дефініції. Визначення залежить

від того, які ознаки покладаються в його основу дослідником. Так, на думку Е. де Бюссер, головною рисою є доступність інформації для широкого загалу. При цьому, вона не обов'язково має існувати в цифровій формі. Така інформація може бути створена та поширена будь-якою особою. У багатьох випадках її автор залишається невідомим, що впливає на надійність інформації, однак не на відкритий характер, адже надійність та достовірність не є необхідними ознаками інформації з відкритих джерел. Чи є доступ до інформації платним або безкоштовним також не має значення для віднесення її до категорії інформації з відкритих джерел. Визначальною ознакою, якою має володіти інформація з відкритих джерел, є її доступність для достатньо широкого та невизначеного кола осіб. Інформація ж, доступ до якої має визначене коло осіб та можливість поширення якої обмежена, не може вважатися інформацією з відкритих джерел. Таким чином, на думку дослідниці, інформацією з відкритих джерел є будь-яка інформація, доступ до якої не обмежений чітко визначеною групою осіб та яка не обов'язково є надійною або точною [1, с. 95–98].

У разі, якщо інформація з відкритих джерел вказує на наявність або відсутність обставин, що підлягають доказуванню у кримінальному провадженні, вона може бути використана як доказ. Зокрема, її активно використовують під час розслідування воєнних злочинів, кримінальних правопорушень у сфері обігу наркотичних засобів, тощо. Однак, незважаючи на активне використання інформації з відкритих джерел правоохоронними органами в процесі здійснення своєї діяльності, має місце брак нормативно-правового регулювання даного роду діяльності.

З метою стандартизації процедур та забезпечення методичних вказівок для розслідувань, сприяння особам, що займаються розслідуваннями з використанням відкритих даних, був розроблений Протокол Берклі (далі – Протокол). Даний "практичний посібник" був створений спільно Школою права Каліфорнійського університету в Берклі та представниками Організації Об'єднаних Націй. У ньому сформульовано міжнародні стандарти проведення онлайн-розслідувань можливих порушень міжнародного права прав людини, міжнародного гуманітарного та кримінального права, містяться рекомендації з проведення процедур збору, аналізу та збереження цифрової інформації [2].

У главі II Протоколу наводиться перелік принципів, згідно з якими має здійснюватися розслідування. Вони поділяються на три категорії: професійні, методологічні та етичні. До професійних принципів відносяться: 1) відповідальність – необхідність несення особами, що проводять розслідування, відповідальності за свої дії; 2) компетенція - наявність належного ступеня підготовки та навичок для проведення розслідування; 3) об'єктивність – недопустимість впливу особистих, культурних та структурних упереджень на розслідування; 4) законність - необхідність дотримання норм чинного законодавства під час проведення розслідування; 5) обізнаність у сфері безпеки - наявність базових знань у галузі оперативної безпеки, мінімізація цифрового сліду та усвідомлення потенційних ризиків [2, с. 11–13].

Серед методологічних принципів виокремлюють: 1) точність – необхідність мінімізувати вірогідність необ'єктивного відбору, інтерпретації та представлення даних; 2) мінімізація даних – збір даних має бути виправданим для сформульованої мети, необхідним для її досягнення та пропорційним можливості її виконання; 3) збереження – необхідність короткострокового та довгострокового збереження інформації для забезпечення її доступності та придатності для подальшого використання; 4) безпека за замовчуванням – організації, що проводять розслідування, мають застосовувати та інвестувати в технічні та структурні заходи безпеки, для того щоб розслідування були безпечні та належним чином анонімізовані [2, с. 13-14].

Основоположними етичними принципами є: 1) гідність – норми, що стосуються прав людини, мають бути керівними стандартами для проведення розслідувань з використанням відкритих даних; 2) скромність – особи, які проводять розслідування з використанням інформації з відкритих джерел, мають визнавати свої помилки, повинен існувати механізм для звітування та виправлення помилок; 3) інклюзивність – має бути забезпечено врахування різних точок зору та досвіду під час проведення розслідувань; 4) незалежність – особи, які проводять розслідування, мають захищати себе та своє розслідування від неналежного впливу; 5) прозорість – не можна допускати щоб особа, яка проводить розслідування, видавала себе за іншу особу [2, с. 14-15].

У главі VI Протоколу пропонується цикл розслідування, який складається з 6 етапів: 1) онлайн-пошук, який може відбуватися у форматі власне пошуку, тобто виявлення інформації та її джерел за допомогою загальної або розширеної методології пошуку, та моніторингу, який являє собою виявлення нової інформації шляхом послідовного вивчення постійних джерел; 2) попере-

ня оцінка виявленого матеріалу з метою уникнення збору надлишкової інформації та порушення права на недоторканість приватного життя; 3) збір, що являє собою отримання онлайн інформації шляхом її конвертування, завантаження або іншої форми фіксації; 4) збереження інформації протягом тривалого терміну таким чином, щоб вона залишалася зрозумілою для потенційних користувачів незалежно від контексту та мала достатній рівень підтвердження її автентичності; 5) верифікація, тобто процес встановлення точності та правдивості зібраної інформації; 6) розвідувальний аналіз, який являє собою процедуру розгляду та інтерпретації інформації для формулювання висновків, що мають значення для прийняття рішень по справі [2, с. 55–67].

Незважаючи на те, що Протокол не має обов'язкової юридичної сили, викладені в ньому стандарти та рекомендації є орієнтиром для представників правоохоронних органів держав світу в процесі здійснення розслідування з використанням відкритих цифрових даних, їх дотримання сприятиме точності та надійності зібраних доказів, зменшує вірогідність визнання доказів неприйнятними.

Однією з головних проблем, які постають в процесі проведення розслідування з використанням інформації з відкритих джерел, є "легалізація" отриманих доказів, оскільки кримінальне провадження має відбуватися в передбаченому кримінальним процесуальним законодавством порядку, а способи збирання та закріплення доказів мають відповідати встановленим законодавцем вимогам.

Як зазначає О.О. Торбас, на даний момент у кримінальному процесуальному законодавстві, на відміну від інших галузей національного права, електронні докази як окремий вид фактично ігноруються. Так, відсутнє легальне визначення електронних доказів, найближче формулювання якого міститься у п. 1 ч. 2. ст. 99 Кримінального процесуального кодексу України (далі – КПК України), де вказано що до документів, крім інших, можуть відноситись матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації. Окрім цього, вказівки на електронні докази немає серед переліку процесуальних джерел доказів, що міститься у ч. 2 ст. 84 КПК України [3, с. 101]. В той самий час, введення до кримінального процесуального законодавства електронних доказів як окремого виду доказів вбачається доцільним, зокрема, з огляду на їхні унікальні характеристики. Науковці Д.О. Алєксєєва-Процюк та О.М. Брисковська виокремлюють наступні особливості електронних доказів: 1) існують у нематеріальному вигляді; 2) можуть бути створені людиною або бути результатом функціонування інформаційної системи; 3) не існують поза межами технічного носія або каналу зв'язку; 4) зв'язок з матеріальним носієм не є нерозривним; 5) можуть вільно переміщуватися в електронній мережі без технічного носія; 6) сприймаються лише за допомогою технічних засобів та програмного забезпечення; 7) можуть бути скопійовані або переміщені на інший носій без втрати своїх характеристик; 8) можуть бути змінені або знищені дистанційно; 9) потребується специфічний порядок збирання, перевірки та оцінки [4, с. 252].

Електронні докази, як і будь-які докази що використовуються в кримінальному провадженні, повинні відповідати вимогам належності, допустимості та достовірності. Відповідно до положень ст. 85 КПК України, належними є докази, які прямо чи непрямо підтверджують існування чи відсутність обставин, що підлягають доказуванню у кримінальному провадженні, та інших обставин, які мають значення для кримінального провадження. Обов'язок доводити зв'язок електронного доказу з кримінальним провадженням покладений на сторону обвинувачення. Окрім цього, необхідним є доводити порядок отримання доказів, оскільки збирання доказів на основі відкритих джерел є складним та багатоетапним процесом, кожна зі стадій якого повинна здійснюватися відповідно до положень закону. В іншому випадку доказ, отриманий з відкритих джерел, може бути визнаний судом недопустимим на основі доктрини плодів отруйного дерева [3, с. 106–112].

Під достовірністю доказу варто розуміти його відповідність дійсності. Оцінка достовірності електронних доказів супроводжується значною кількістю проблем. Так, в електронні докази досить легко вносити зміни, існує вірогідність допущення технічних помилок під час їх отримання, застосування невідповідних інструментів для збереження та доступу до них, тощо. Це значно зменшує їхню надійність. Одним зі способів перевірки достовірності електронних доказів, який пропонує О.О. Торбас, є перевірка хеш-суми, що являє собою певне значення, обчислене на основі набору даних із застосуванням одного із математичних алгоритмів, що використовуються для перевірки цілісності даних при їхній передачі або збереженні. Так, якщо створюється копія певного файлу, то хеш-суми оригіналу та копії будуть збігатися. У разі ж заміни принаймні одного символу, хеш-сума буде відрізнятися [3, с. 112–118].

Докази, отримані з відкритих джерел, є особливо важливими для розслідування злочинів проти основ національної безпеки. Для доведення винуватості особи у вчиненні цих злочинів, особливо з початку повномасштабної російської агресії проти України, активно використовуються фото, відео, аудіо та текстові матеріали, які правоохоронні органи отримують в результаті дослідження соціальних мереж, відеохостингових платформ, веб-сайтів, тощо. Це підтверджує судова практика.

Так, Юр'ївським районним судом Дніпропетровської області було розглянуто кримінальне провадження за обвинуваченням особи у вчиненні злочинів, передбачених ч. 2 ст. 110 та ч. 5 ст. 111-1 КК України. Доказами винуватості особи, серед іншого, був протокол огляду розміщеної в Telegram-каналі публікації, присвяченої проведенню незаконного референдуму з питання входження ЛНР до складу РФ, де зображена дана особа [5].

Варто зазначити, що одними з найбільш використовуваних джерел є соціальні мережі та месенджери. Окрім вищенаведеного прикладу, у справі № 750/11291/23, одним з доказів винуватості особи у вчиненні кримінального правопорушення, передбаченого ч. 1 ст. 111 КК України, стало графічне зображення, на якому обвинувачений зображений у військовій формі збройних сил Російської Федерації, яке було знайдене під час огляду особистої сторінки особи на інтернет-ресурсі "ВКонтакте" [6].

Для дослідження здобутої внаслідок огляду відкритих джерел інформації може бути використана передбачена кримінальним процесуальним законодавством можливість залучати експерта. Так, у справі № 461/1790/19, одним з доказів винуватості особи був висновок експерта, встановлений в результаті проведення лінгвістичної експертизи висловлювань особи під час трансляцій на каналі Інтернет-радіостанції. В результаті дослідження тексту стенограм, які експерт звіряв, прослуховуючи відповідні звукозаписи, було встановлено, що висловлення особи містять спонукання до діяльності, спрямованої на зміну меж території та державного кордону України шляхом від'єднання територій західноукраїнських областей та передачі їх у володіння інших держав [7].

Окрім цього, інформація, отримана з відкритих джерел, активно використовується для проведення слідчих дій. Так, одним з доказів винуватості особи у справі № 569/18865/23, були протоколи пред'явлення особи для впізнання за відеозаписом, розміщеним у відеохостингу YouTube, та за фотознімками, розміщеними у соціальній мережі "Одноклассники", у ході яких свідки впізнали обвинувачену особу [8].

Що ж стосується практики міжнародних судових органів, то варто відмітити декілька справ, що розглядав Міжнародний кримінальний суд (далі - МКС). Вони є прецедентними стосовно практики використання інформації, отриманої з відкритих джерел, як доказів.

"Першим тестом" того, що може бути досягнуто з використанням нетрадиційних технік розслідування, вважається справа Ахмада Аль-Факі Аль-Махді. Обвинуваченому було пред'явлено звинувачення в участі в умисному знищенні дев'яти мавзолеїв та дверей до мечеті в Тімбукту, Малі, в 2012 р. Під час розслідування Офіс прокурора МКС успішно співпрацював із представниками громадянського суспільства та розслідувачами відкритих джерел. Так, дослідницьким агентством Situ було надано інтерактивну цифрову платформу, призначену для сприяння організації, аналізу та презентації доказів, отриманих з відкритих джерел. Інструмент, що поєднував геопросторову інформацію, супутникові знімки, фотографії та відео з відкритих джерел був використаний для ознайомлення суддів та інших учасників з різними подіями, що відбувалися в Тімбукту. На початку судового засідання у серпні 2016 року Аль-Махді визнав свою провину та був засуджений до 9 років позбавлення волі [9, с. 11].

У справі Жан П'єра Бемба Гомбо, окрім злочинів проти людяності та воєнних злочинів, віце-президент Демократичної Республіки Конго підозрювався у підкупі свідка. Представники обвинувачення надали суду докази що свідчили про здійснення сестрою обвинуваченого банківського переказу на рахунок свідка, який згодом передав гроші іншому свідку, що згодом дав неправдиві свідчення. Прокуратура, зокрема, надала фотографії з Фейсбуку, на яких зображено двох підкуплених свідків – важливий доказ зв'язку між ними для сторони обвинувачення. Сторона захисту висунула заперечення, які полягали в тому, що неможливо встановити хто виклав фото, коли, де та ким воно було зроблено, та чи взагалі на ньому зображені особи, на яких вказує прокуратура. Окрім цього, оскільки прокуратура не мала прямого доступ до серверів або даних Фейсбук, вона покладалася на скріншоти Фейсбук сторінок, що містили фотографії. У зв'язку з цим, прокуратура не має доступу до метаданих (наприклад час публікації або IP-адреса користувача,

що опублікував фото), а тому немає можливості встановити особу, яка опублікувала фотографії. В остаточному рішенні всіх п'ятьох обвинувачених було визнано винними, однак суд безпосередньо не розглядав заперечення, висунуті стороною захисту [10, с. 327–329].

У серпні 2017 року, Палата попереднього провадження МКС видала ордер на арешт Махмуда аль-Верфаллі, командира елітного підрозділу армії Лівії. Він звинувачувався у страті тридцяти трьох осіб в серії дій, зафіксованих на відео, завантаженому на Фейсбук. Цей ключовий доказ, отриманий з відкритих джерел зображував 18 осіб, вдягнутих у помаранчеві комбінезони та чорні капюшони, зі зв'язаними за спиною руками, що стояли на колінах на землі в чотири ряди. Після прочитання "Вироку", п'ятеро осіб в камуфляжній уніформі вистрілили в осіб, що стояли на колінах. Юридичні та правозахисні спільноти вітали ордер як нову віху, перший випадок коли МКС використав докази, отримані з відкритих джерел, як основу для ордеру. Вперше Прокуратура поклала інформацію з відкритих джерел в основу розслідування, без відео справи б не було [9, с. 13].

Висновки. Незважаючи на важливу роль цифрової інформації як доказів, отриманих з відкритих джерел у сучасних умовах розслідування та значний обсяг практики їх використання, нормативно-правове регулювання даної проблеми не можна назвати належним. Однією з небагатьох спроб стандартизації процедури розслідування з використанням відкритих даних є Протокол Берклі, який, попри важливе практичне значення, не має обов'язкової юридичної сили. З огляду на суттєву різницю між електронними доказами, якими є переважна більшість доказів, отриманих з відкритих джерел, та іншими видами доказів, вбачається доцільним закріплення в кримінальному процесуальному законодавстві їх визначення, належний спосіб збирання, збереження, тощо.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. De Busser E. Open-Source Data and Criminal Investigations: Anything You Publish Can and Will Be Used Against You. *Groningen Journal of International Law*. 2014. Т. 2, № 2. С. 90. URL: https://doi.org/10.21827/5a86a843e5c9d.
2. Berkeley Protocol on Digital Open-Source Investigations. United Nations, 2022. URL: https://doi.org/10.18356/9789210053433.
3. OSINT при розслідуванні кримінальних правопорушень: підручник / О.О. Торбас. – Одеса: Видавництво «Юридика», 2024. – 180 с.
4. Алєксєєва-Процюк Д.О., Брисковська О.М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. Вип. 2. С. 247–253. URL: http://www.nvppp.in.ua/vip/2018/2/50.pdf.
5. Вирок Юр'ївського районного суду Дніпропетровської області від 19.04.2024, справа № 198/206/23. URL: https://reyestr.court.gov.ua/Review/ 118478551.
6. Вирок Деснянського районного суду м. Чернігова від 25.04.2024, справа № 750/11291/23. URL: https://reyestr.court.gov.ua/Review/118605084.
7. Вирок Галицького районного суду м. Львова від 25.11.2021, справа № 461/1790/19. URL: https://reyestr.court.gov.ua/Review/101378026.
8. Вирок Рівненського міського суду Рівненської області від 19.04.2024, справа № 569/18865/23. URL: https://reyestr.court.gov.ua/ Review/118521528.
9. Trevisan S. Open-source information in criminal proceedings: lessons from the International Criminal Court and the Berkeley Protocol. Giurisprudenza Penale. 2021. С. 1–17. URL: https://www.giurisprudenzapenale.com/wp-content/uploads/2021/04/Trevisan_gp_ 2021_4.pdf.
10. Hiatt K. Open Source Evidence on Trial. THE YALE LAW JOURNAL FORUM. 2016. С. 323–330. URL: https://www.yalelawjournal.org/ pdf/Hiatt_PDF_zxz3ufoz.pdf.