Kontrola i audyt

Narzędzia wykorzystywane w audycie śledczym

Duże zbiory danych, AI i otwarte źródła informacji

Audyt śledczy to rodzaj audytu przeprowadzanego w celu ustalenia przyczyn lub okoliczności związanych z podejrzeniami oszustwa bądź nadużycia w organizacji o charakterze komercyjnym, publicznym albo non-profit. W artykule zostały zaprezentowane jego najważniejsze cechy. Na początku skupiono się na kilku kluczowych kwestiach, tj. istocie audytu śledczego, podstawowych cechach typowych nadużyć, głównych elementach analizy śledczej. W dalszych częściach pracy zaprezentowano wybrane cechy oraz potencjalne i realne możliwości zastosowania dużych zbiorów danych i sztucznej inteligencji w audycie śledczym. Przedstawiono wybrane techniki pozyskiwania informacji ze źródeł otwartych i zastosowania tej strategii w działalności audytowej.

WOJCIECH GOLEŃSKI, MARCIN BĘDZIESZAK, MACIEJ FOLTA

Istota audytu śledczego – wybrane metody

Audyt śledczy (dochodzeniowy) jest to swego rodzaju połączenie klasycznego audytu z metodami śledczymi, a zwłaszcza z analityką śledczą. Z tego powodu w audycie śledczym kluczowe znaczenie ma proces zbierania informacji oraz ich

właściwa analiza. W tym celu stosuje się różne metody gromadzenia danych i ich przetwarzania. Ta dziedzina podlega ciągłej ewolucji, ponieważ zmieniają się zarówno sposoby pracy audytorów i śledczych, jak i metody stosowane przez osoby dopuszczające się oszustw i nadużyć w organizacjach. Czynnikiem determinującym owe zmiany jest rozwój technologii, który spowodował olbrzymie przemiany w procesie gromadzenia informacji, a to z kolei stworzyło zapotrzebowanie na nowe podejście do analizy i wywiadu[1].

Audyt śledczy ma za zadanie przeciwdziałać różnym przejawom przestępczości gospodarczej, a w szczególności wykrywać oszustwa, korupcję oraz inne nadużycia i przestępstwa finansowe. W tym celu są wykorzystywane nie tylko metody stosowane w rewizji finansowej, lecz również metody kryminalistyczne. Nie zawsze metody rewizyjne są wystarczające, aby wykryć przestępstwa gospodarcze[2], które obejmują wszelkie czynności skierowane przeciwko prawidłowym zasadom funkcjonowania gospodarki. Są nimi zarówno drobne nadużycia, jak i działalność zorganizowanych grup przestępczych. Do najpopularniejszych rodzajów przestępstw gospodarczych zalicza się pranie pieniędzy, oszustwa księgowe, korupcję, zmowy przetargowe i cyberprzestępstwa[3]. Jak podaje M. Kaczmarski*:* „Termin audyt śledczy – w swojej tradycyjnej formie – odnosi się do badania zarzutów nieprawidłowości w przedsiębiorstwie z wykorzystaniem metod pracy audytora wewnętrznego, biegłego rewidenta, zdobyczy nauki kryminalistyki oraz warsztatu pracy śledczych w procesie karnym (…)[4]". Jest to więc rozwiązanie hybrydowe, właściwe do zastosowania, w sytuacji gdy waga zarzutu może mieć istotny i negatywny wpływ na działalność operacyjną przedsiębiorstwa, a jego kontekst sprawia, że nie jest on bezzasadny[5].

Audyt śledczy w największym stopniu nakierowany jest na wykrywanie nadużyć i oszustw[6]. Zrozumienie istoty tych procederów ma niepoślednie znaczenie dla odróżnienia opisywanej formy audytu od innych sposobów dokonywania oceny funkcjonowania organizacji. Oszustwa w najszerszym ujęciu za J. T. Wellsem, można zdefiniować jako każde przestępstwo popełnione w celu osiągnięcia korzyści za pomocą wprowadzenia w błąd, charakteryzujące się:

---

1 UNODC, *Analiza kryminalna. Podręcznik dla analityków*, CBA, Warszawa 2020, s. 5.

2 P. Ostrowska: *Problematyka rachunkowości kreatywnej, agresywnej i audytu śledczego w świetle opinii księgowych*, „Academic Review of Business and Economics" Vol. 2(1)/2022, s. 99.

3 C. Martysz, K. Walczak: *Zarys problematyki przeciwdziałania przestępstwom gospodarczym i ich wykrywania*, [w:] *XXV lat w naukach ekonomicznych: dokonania, wyzwania, perspektywy*, R. Bartkowiak, M. Matusiewicz (red.), Warszawa 2018.

4 M. Kaczmarski: *Czym jest audyt śledczy i kiedy może się przydać*?, <https://www.riskcompliance.pl/news/czym-jest-audyt-sledczy-i-kiedy-moze-sie-przydac/>, (dostęp 21.1.2025).

5 Tamże.

6 Zob. IAASB: *Fraud and going concern in an audit of financial statement: Exploring the Differences Between Public Perceptions About the Role of the Auditor and the Auditor's Responsibilities in a Financial Statement Audit*, Discussion Paper Comments Due: Jan. 12, 2021, s. 16.

1) istotnym zafałszowaniem informacji; 2) świadomością fałszu u sprawcy; 3) poleganiem na fałszywej informacji przez ofiarę; 4) wystąpieniem szkody jako skutku takiego działania[7]. W myśl art. 286 Kodeksu karnego oszustwo polega na działaniu sprawcy w celu osiągnięcia korzyści majątkowej, doprowadzającym inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania[8]. Z kolei nadużycie zostało stypizowane w art. 296 k.k. Sprawcą jest ten, kto będąc obowiązany na podstawie przepisu ustawy, decyzji właściwego organu lub umowy do zajmowania się sprawami majątkowymi lub działalnością gospodarczą osoby fizycznej, prawnej albo jednostki organizacyjnej niemającej osobowości prawnej, przez nadużycie udzielonych mu uprawnień lub niedopełnienie ciążącego na nim obowiązku, wyrządza jej znaczną szkodę majątkową oraz działa w celu osiągnięcia korzyści majątkowej[9]. Nadużycie odróżnia od „zwykłej" nieprawidłowości rozmyślność sprawcy oraz potajemny/skryty charakter aktywności, a także częste zacieranie jej śladów. W tym sensie nadużycie jest tożsame z oszustwem[10]. *De facto* nadużycie i oszustwo są pokrewnymi terminami, ale nadużycie jest węższym pojęciem, gdyż dotyczy świadomego i niewłaściwego wykorzystania zasobów organizacji[11]. Owa „zwykła" nieprawidłowość jest działaniem lub zaniechaniem działania, które nie ma intencjonalnego charakteru, ale w świetle kryteriów oceny jest nielegalne, niegospodarne, niecelowe lub nierzetelne, a także może być nieprzejrzyste lub niejawne[12]. Audyty śledcze umożliwiają zatem identyfikację potencjalnych nadużyć, które mogą negatywnie wpłynąć na reputację i wyniki finansowe firmy. Ich celem jest również zabezpieczenie interesów inwestorów i udziałowców oraz zmniejszenie ryzyka wystąpienia nadużyć gospodarczych w przyszłości[13]. Całkowite wyeliminowanie oszustw i nadużyć jest ze swojej istoty niemożliwe. Audyt śledczy ma ograniczać ich liczbę oraz minimalizować skutki[14]. Zrozumienie metod, za pomocą których najczęściej

[7] J. T. Wells: *Nadużycia w firmach. Vademecum. Zapobieganie i wykrywanie*, LexisNexis, E&Y, Warszawa 2006, s. 2.
[8] Art. 286 ustawy z 6.6.1997 r. – Kodeks karny (Dz.U. z 2024 r. poz. 017), dalej k.k.
[9] Art. 296 ustawy z 6.6.1997 r. – Kodeks karny (Dz.U. z 2024 r. poz. 017), zob. W. Ignatczak, M. Dyjasz: *Audyt śledczy – przetwarzanie informacji z wykorzystaniem metod i technik analizy śledczej*, PIKW, Warszawa 2019, s. 16-17.
[10] W literaturze przedmiotu zwykle rozróżnia się nadużycie od oszustwa oraz od przestępstwa gospodarczego. To ostatnie dotyczy konkretnych sytuacji określonych w prawie karnym. Dlatego też nie każde nadużycie czy oszustwo jest przestępstwem gospodarczym – zob. M. Proczek, P. Szczepańska: *Nadużycia i przestępstwa finansowe a działalność Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" nr 319/2017; M. Kutera: *Rola audytu finansowego w wykrywaniu przestępstw gospodarczych*, Difin, Warszawa 2008.
[11] W. Ignatczak, M. Dyjasz: *Audyt śledczy – przetwarzanie informacji*…, op.cit., s. 16-17.
[12] A. Piaszczyk: *Audyt śledczy*, ECE Prestiż, Lublin 2009, s. 6-7.
[13] Por. raport KPMG <https://kpmg.com/pl/pl/home/services/deal-advisory/zarzadzanie-ryzykiem-naduzyc-i-uslugi-dochodzeniowe/audyty-sledcze.html>, (dostęp 30.1.2025).
[14] A. Piaszczyk: *Audyt śledczy*…, op.cit, s. 5.

wykrywane są nadużycia, ma kluczowe znaczenie dla identyfikowania i przerywania sposobów ich powstawania. Pozwala to zmniejszyć ich wpływ, skutek i czas trwania danego zdarzenia dla zainteresowanego podmiotu, tym samym zwiększając skuteczności działań związanych z wykrywaniem i zapobieganiem oszustwom i nadużyciom w organizacjach[15]. Wyzwaniem jest także wykrywanie przypadków korupcji, która stanowi jedną z największych patologii życia publicznego[16]. Standardowe systemy kontroli wewnętrznej zwykle mają na celu wyeliminowanie nieprawidłowości lub ograniczenie ryzyka ich wystąpienia. Nie służą natomiast wykrywaniu oszustw, będących działaniami celowymi[17].

Przestępstwa gospodarcze, oszustwa, nadużycia mogą przybierać różne formy. Według najnowszego raportu Stowarzyszenia Biegłych do spraw Przestępstw i Nadużyć Gospodarczych – ACFE (ang. *Association of Certified Fraud Examiners*) schematy nadużyć dzielą się na trzy główne kategorie: 1) sprzeniewierzenie majątku, 2) korupcję, 3) fałszowanie sprawozdań finansowych. Sprzeniewierzenia polegają zwykle na kradzieży lub niewłaściwym wykorzystaniu zasobów organizacji przez pracownika. Jest to zdecydowanie najczęstsza kategoria nadużyć, występująca w 89% przypadków. Powodują one relatywnie najniższe straty dla objętych szacunkami organizacji, wynoszące średnio 120 tys. dolarów rocznie. Niemal połowa przypadków nadużyć (48%) obejmuje różne formy korupcji, które generowały straty na poziomie 200 tys. dolarów dla pojedynczych, objętych szacunkami organizacji. Fałszowanie sprawozdań finansowych, polegające na celowym wprowadzeniu istotnych błędów lub pomijaniu danych w sprawozdaniach, było najrzadszą kategorią (5% przypadków), ale powodującą najwyższe jednostkowe straty, średnio 766 tys. dolarów[18]. Szacuje się, że nadużycia pochłaniają około 5% ogólnych przychodów firm[19]. Wszystkie powyżej opisane kategorie (tj. oszustwa i nadużycia) zwykło się żargonowo określać z języka angielskiego mianem *fraudów*.

Wykrywanie *fraudów* w audycie śledczym polega na wykorzystaniu metod z zakresu kryminalistyki, co sprawia, że stanowi on specyficzny rodzaj audytu finansowego. Kryminalistyka wykorzystuje metody służące wykryciu, zidentyfikowaniu oraz zebraniu dowodów w celu rozstrzygnięcia sprawy[20]. Stosuje analizę śledczą (kryminalną) oraz zróżnicowane techniki zbierania informacji śledczych. Informacja w procesie audytu śledczego ma zasadnicze znaczenie. Istotne jest tu nie tylko zbieranie danych, informacji oraz

[15] Por. ACFE: *Occupational Fraud 2024: A Report to the Nations*, s. 21

[16] Istnieje bardzo bogata literatura na temat zagadnienia korupcji. Obszerność tematu wykracza poza możliwości prezentacji w niniejszym artykule. W kontekście audytu śledczego warto wskazać przynajmniej na dwa opracowania dotyczące badanego zjawiska – zob. INTOSAI: *Guideline for the Audit of Corruption Prevention in Public Procurement,* Vienna 2022; OECD: *Anti-Corruption and Integrity Outlook 2024*, Paris 2024.

[17] A. Piaszczyk: *Audyt śledczy*…, op.cit, s. 8.

[18] ACFE, *Occupational Fraud 2024: A Report to the Nations,* Austin 2024.

[19] Tamże.

[20] P. Ostrowska: *Problematyka rachunkowości*…, op.cit., s. 99.

wykorzystanie dostępnej wiedzy na temat istoty danego zjawiska, ale także właściwa analiza oraz interpretacja ustalonych faktów[21]. Proces zbierania danych może obejmować zróżnicowane techniki o ilościowym i jakościowym charakterze[22]. Pozyskiwanie informacji związanych z daną sprawą na potrzeby audytu może dotyczyć zarówno źródeł osobowych (wywiady, obserwacje, przesłuchania, informacje sygnalistów (ang. *Human Intelligence* – HUMINT), jak i dokumentów organizacji, w tym o charakterze finansowym – (ang. *Financial Intelligence* – FININT), czy też danych z sieci komputerowych (ang. *Signals Intelligence* – SIGINT) oraz źródeł zewnętrznych, np. o charakterze otwartym, (ang. O*pen Source Intelligence* – OSINT)[23]. Równie istotna jest właściwa ocena wszystkich zebranych danych pod względem wiarygodności i przydatności w dalszym procesie ich analizy[24]. Analiza uzyskanych informacji jest kluczowym elementem audytu śledczego[25].

M. Dyjasz zauważa, że analiza śledcza jest procesem, w ramach którego wykorzystywane są różnorodne metody i techniki przetwarzania informacji, pozwalające na skuteczne ustalanie oraz domniemywanie związków pomiędzy danymi o działalności przestępczej z innymi, potencjalnie z nimi powiązanymi informacjami, w celu ich wykorzystania przez uprawnione organy. Najważniejszą rolę w procesie analizy odgrywają informacje pochodzące ze wszelkich dostępnych źródeł, które należy rozpatrywać w powiązaniu ze sobą[26]. Jest to analiza „informacji kryminalnych", co kojarzy się z systemami zestawiania informacji wykorzystywanymi do przechowywania i odczytu danych dotyczących przestępczości i przestępców. W miarę jak rosła ilość i różnorodność zbieranych informacji, stopniowo wprowadzano coraz bardziej złożone systemy służące do tego celu[27]. Niemniej podstawą mogą być tu klasyczne techniki analityczne. Przetwarzanie informacji w procesie audytu śledczego powinno obejmować kryminalistyczną regułę tzw. „siedmiu złotych pytań", w założeniu pozwalając rozwiązać problem wykrycia sprawcy, a także określić, jakich należy dokonać ustaleń w konkretnej sprawie. Te pytania to: 1) co? – pozwala na określenie co się właściwie wydarzyło; 2) kto? – pozwala na ustalenie kto właściwie jest sprawcą, a kto ofiarą; 3) gdzie? – pozwala na określenie miejsca zdarzenia, skutku, ukrycia, przygotowania do popełnienia przestępstwa; 4) kiedy? – ustala okres wystąpienia zdarzenia; 5) dlaczego? – pozwala na określenie motywu i pobudek działania sprawcy; 6) w jaki sposób? – pozwala na ustalenie *modus operandi* sprawcy; 7) za pomocą

[21] Zob. W. Ignatczak, M. Dyjasz: *Audyt śledczy…*, op.cit., s. 24-33.
[22] Zob. Z. Dobrowolski, J. Kościelniak: *Audyt śledczy w spółkach Skarbu Państwa i spółkach komunalnych*, ISP UJ, Kraków 2018, s. 35 i nast.
[23] Por. T. Maziriri: *Forensic Auditing: A Guide for Practitioners*, Amazon 2021.
[24] *EY Academy of Business*, <https://www.academyofbusiness.pl/trainings/audyt-sledczy/>, (dostęp 31.1.2025); zob. W. Ignatczak, M. Dyjasz: *Audyt śledczy…*, op.cit., s. 34-50 oraz 86 i nast.
[25] Tamże.
[26] M. Dyjasz: *Analiza śledcza jako technika wsparcia audytu śledczego*, IIA Polska, prezentacja PowerPoint.
[27] UNODC, *Analiza kryminalna…*, op.cit., s. 6.

czego? – pozwala na określenie narzędzia działania sprawcy. Reguła ta wskazuje kierunek ustaleń, wyjaśniających co właściwie w danej sprawie się wydarzyło (lub potencjalnie mogło mieć miejsce). Powyższe pytania sprowadzają się zatem do wskazania: 1) kto wiedział lub mógł wiedzieć o zdarzeniu? (próba ustalenia świadków i współsprawców); 2) kto chciał lub mógł chcieć dokonania przestępstwa? (ustalenie motywu, pobudek – kto mógłby osiągnąć korzyść, komu by się opłacało popełnić czyn); 3) kto uzyskał lub mógł uzyskać korzyść ze zdarzenia? (korzyść jest nie zawsze materialna, może być także bezpośrednia); 4) kto był lub mógł być na miejscu zdarzenia? (ukierunkowane na ustalenie alibi); 5) jaką osobowość miał lub mógł mieć sprawca?[28]. We wskazanym procesie przydatna może okazać się także koncepcja trójkąta oszustwa (ang. *fraud triangle*). Zgodnie z nią na popełnienie przestępstwa mają wpływ trzy czynniki: odczuwanie silnej potrzeby finansowej (presja), dostrzeżenie okazji, racjonalizacja. W koncepcji sformułowanej przez D.R. Cresseya[29] presja, motyw dotyczy potrzeby, na przykład braku możliwości wywiązania się ze spłaty prywatnych długów, niemożności porozumienia się z przełożonym lub chęć podniesienia standardu życia, racjonalizacja odnosi się do postawy sprawcy przestępstwa oraz oznacza łatwość w usprawiedliwianiu własnych zachowań, okazja oznacza faktyczną możliwość popełnienia nadużycia[30].

Biorąc powyższe pod uwagę, warto wskazać kilka kluczowych cech, które odróżniają audyt śledczy od tradycyjnie rozumianego audytu wewnętrznego lub audytu zewnętrznego (kontroli), realizowanego m.in. przez najwyższe organy kontroli. Jak już zostało wskazane, audyt śledczy skoncentrowany jest na wykrywaniu oszust i nadużyć, łącząc metody pracy audytora wewnętrznego, biegłego rewidenta oraz metody analizy śledczej i zdobyczy kryminalistyki[31]. Chodzi raczej o zmianę optyki w podejściu do wykrywania nieprawidłowości, a nie zastosowanie metod operacyjno-rozpoznawczych we wskazanym procesie, gdyż są one domeną organów ścigania[32]. Należy więc zauważyć, że już samo zastosowanie przedstawionych powyżej koncepcji (m.in. trójkąta oszustwa, siedmiu „złotych pytań"), a także m.in. rozbudowanych diagramów powiązań osobowych w celu wykrycia np. konfliktu interesów lub potencjalnych mechanizmów korupcjogennych, przenosi akcenty z działań nastawionych na diagnozę stanu faktycznego, na działania typowo wykrywcze. Audyt śledczy stosowany jest w sytuacji uzasadnionego przypuszczenia wystąpienia poważnego nadużycia. Wskazuje się także, że zlecający ma większy

[28] D. Jagiełło: *Taktyka kryminalistycznych czynności dowodowych*, CH. Beck, Warszawa 2019, s. 6.
[29] D. R. Cressey: Other *People's Money. A study in Social Psychology of Embezzlement*, Free Press, 1953.
[30] A. Nowak: *Identyfikacja przyczyn i sprawców oszustw finansowo-księgowych – ujęcie statystyczne*, „Zeszyty Naukowe Usz" nr 765 Finanse, Rynki Finansowe, Ubezpieczenia nr 61 (2013), s. 139.
[31] M. Kaczmarski: *Czym jest audyt śledczy i kiedy może się przydać*?, <https://www.riskcompliance.pl/news/czym-jest-audyt-sledczy-i-kiedy-moze-sie-przydac/> (dostęp 21.1.2025).
[32] Zob. E. Wójcik: *Czynności operacyjno-rozpoznawcze i ich rola w zwalczaniu przestępczości zorganizowanej*, <http://m.wspia.eu/file/21440/44-WÓJCIK.pdf> (dostęp 3.3.2025).

wpływ na harmonogram i przebieg badania audytowego niż w wypadku standardowego audytu wewnętrznego[33]. Co do zasady, audyt śledczy jest realizowany przez wyspecjalizowanych audytorów z zewnątrz organizacji, tak aby całkowicie wyeliminować pokusę nadużycia oraz zwiększyć wiarygodność prowadzonych badań. Badacze zagadnienia dowodzą, że klasycznego audytu finansowego, przeprowadzanego przez biegłego rewidenta czy audytora wewnętrznego, nie można bezpośrednio wykorzystać do badania przestępczości gospodarczej. Wynika to z ograniczeń formalnych, metodologicznych oraz braku specjalistycznych kwalifikacji, w tym np. znajomości zagadnień prawa karnego i gospodarczego, logiki, podstaw psychologii i kryminalistyki[34]. Należy pamiętać, że statutowym zadaniem biegłego rewidenta nie jest celowe poszukiwanie nadużyć, błędów lub naruszeń prawa, tylko rewizja sprawozdań finansowych[35]. Z kolei audytor wewnętrzny skoncentrowany jest na ocenie procesów, systemów, funkcjonowanie komórek organizacyjnych, zgodności działania z prawem, a w szczególności prawidłowości zarządzania ryzykiem, adekwatności i skuteczności systemu kontroli wewnętrznej oraz sprawowaniu nadzoru korporacyjnego w jednostce. Pomimo potrzeby oceny i komunikowania ryzyka oszustwa, od audytora wewnętrznego nie należy jednak oczekiwać posiadania wiedzy specjalistycznej dotyczącej prowadzenia audytu śledczego[36]. Podobnie jest w wypadku czynności realizowanych przez kontrolerów NIK, przez kontrolę należy bowiem rozumieć badanie stanu faktycznego, jego porównanie ze stanem postulowanym lub wymaganym, a następnie ustalenie zakresu i przyczyn rozbieżności. Immanentnym elementem jest wydanie wniosków i zaleceń pokontrolnych[37]. W trakcie kontroli NIK zwraca się także szczególną uwagę na sposoby funkcjonowania kontroli wewnętrznej (audyt wewnętrzny i kontrola zarządcza)[38]. Można więc zauważyć, że zastosowanie metod analizy śledczej w postępowaniu kontrolnym może okazać się odpowiednie w sytuacji uzasadnionego podejrzenia nadużycia. Właściwa identyfikacja anomalii (potencjalnych nieprawidłowości) będzie tu następować z wykorzystaniem metod analitycznych typowych dla kontroli, a następnie mogą zostać zastosowane metody analizy śledczej. W tym kontekście, warto zauważyć, że kontrolując instytucje publiczne, NIK m.in. zwraca uwagę na nieprawidłowości, które powodują lub zwiększają ryzyko korupcji – mechanizmy

[33] *Co to jest Audyt śledczy?* [w:] *Słownik szkolenia EITT*, https://eitt.pl/slownik (dostęp 21.1.2025).
[34] E. I, Szczepankiewicz: *Rewizja finansowa, audyt wewnętrzny a audyt śledczy w wykrywaniu oszustw gospodarczych*, „Studia i Prace Kolegium Zarządzania i Finansów / SGH", nr 152/2016.
[35] Por. IAASB: *Proposed International Standard on Auditing 240 (Revised) The Auditor's Responsibilities Relating to Fraud in an Audit of Financial Statements and Proposed Conforming and Consequential Amendments to Other ISAs*, Exposure Draft February 2024, Comments due: June 5, 2024.
[36] Tamże, s. 83-84.
[37] Por. J. Starościak: *Elementy nauki administracji*, Warszawa 1957, s. 187; W. Dawidowicz: *Zagadnienia ustroju administracji państwowej w Polsce*, Warszawa 1970, s. 34; J. Boć: *Pojęcie i zasięg kontroli* [w:] *Prawo administracyjne*. J. Boć (red.), Kolonia Limited 2010, s. 378-380.
[38] E. Jarzęcka-Siwik, B. Skwarka: *Najwyższa izba Kontroli. Komentarz do ustawy o NIK*, Difin, wydanie III zaktualizowane, Warszawa 2017, s. 49.

korupcjogenne[39]. Jak wiadomo, korupcja stanowi jedno z najpoważniejszych nadużyć wykrywanych w trakcie audytów śledczych. Najwyższa Izba Kontroli ma z kolei znaczące osiągnięcia w ujawnianiu systemowych przyczyn tego zagrożenia oraz proponowaniu rozwiązań i działań, które je zmniejszają[40]. Wydaje się zatem, że zastosowanie elementów analizy śledczej, typowej dla opisywanej tu formy audytu w postępowaniu kontrolnym/audytowym ma swoje uzasadnienie, przy zastrzeżeniu, że kontrole NIK, audyty wewnętrzne oraz audyty śledcze posiadają swoiste, odmienne cechy. Bez wątpienia wiedza z zakresu realizacji audytu śledczego może stanowić pożądane uzupełnienie warsztatu: biegłego rewidenta, audytora wewnętrznego oraz kontrolera państwowego.

Proces przygotowania i realizacji audytu śledczego obejmuje wiele elementów[41]. Warto podkreślić, że prezentowane w tym artykule elementy mają jedynie wycinkowy charakter, zarówno w odniesieniu do audytu śledczego, jako działalności wykrywającej nadużycia i oszustwa, jak i sposobów oraz metod zbierania oraz analizy danych wykorzystywanych w audycie.

Duże zbiory danych i AI w audycie śledczym

Ze względu na rosnącą ilość danych generowanych przez organizacje oraz różnorodność źródeł, z których pochodzą, coraz większego znaczenia w audycie śledczym nabiera wykorzystanie analityki danych. Może być ona zdefiniowana jako proces zbierania, przetwarzania i analizowania danych w celu uzyskania użytecznych informacji, które mogą wspierać podejmowanie decyzji w różnych dziedzinach. Analityka danych obejmuje różnorodne metody, które pozwalają na przetwarzanie, analizowanie i interpretowanie danych w celu uzyskania wartościowych informacji. W odniesieniu do audytu śledczego jest to wskazana wcześniej zaawansowana analiza śledcza[42].

Zaawansowane technologie analizy danych mogą być wykorzystane w celu identyfikacji nadużyć, wzorców oszustw, przestępstw gospodarczych oraz ryzyka finansowego. Dzięki możliwości analizy ogromnych zbiorów danych (ang. *big data*)[43] w czasie rzeczywistym, audytorzy mogą wykrywać nietypowe transakcje, które potencjalnie wskazują na oszustwa

[39] A. B. Hussein: *Zagrożenie korupcją w świetle wyników kontroli NIK opublikowanych w latach 2016–2020*, NIK, Warszawa 2021, s. 6.

[40] Tamże.

[41] Zob. Z. Dobrowolski, J. Kościelniak: *Audyt śledczy w spółkach Skarbu Państwa i spółkach komunalnych*, ISP UJ, Kraków 2018, s. 45-48.

[42] Por. W. Ignatczak, M. Dyjasz: *Audyt śledczy…*, op.cit., s. 76-77.

[43] „Big data" definiowane jest przez 3V, tj.: 1) przetwarzanie dużych wolumenów danych (ang. *volume*); 2) dużą zmienność i dynamikę przetwarzanych danych (ang. *velocity*), szczególnie w czasie zbliżonym do rzeczywistego (np. danych sensorycznych, strumieniowych, pochodzących z Internetu); 3) dużą różnorodność danych (ang. *variety*), w szczególności nieustrukturyzowanych. Pozostałe dwa „v" dodawane do klasycznego modelu dotyczą: 4) wartości danych (ang. *value*) na potrzeby podejmowania decyzji w organizacji 5) wiarygodności danych (ang. *veracity*), w tym problemów ich jakości wynikającej z przetwarzania danych pochodzących z różnorodnych źródeł; J. Wieczorkowski: *Wykorzystanie koncepcji big data w administracji publicznej*, „Roczniki Kolegium Analiz Ekonomicznych/SGH" nr 33/2014; *Technologie informatyczne w administracji publicznej*, 2014.

lub nadużycia[44]. Wykorzystanie analityki danych w audycie wymaga dostępu do bogatych i różnorodnych baz, aby zapewnić kompleksową ocenę efektywności i zgodności działań. Kluczowe zasoby danych obejmują systemy informatyczne, w których gromadzone są informacje o działalności jednostki. Mogą to być systemy finansowo-księgowe, systemy kadrowe, systemy zarządzania projektami czy systemy informatyczne obsługujące konkretne usługi publiczne. Dodatkowo korzysta się z zewnętrznych baz danych, takich jak centralne rejestry prowadzone przez instytucje rządowe (np. rejestr podmiotów gospodarczych, rejestr PESEL) czy też bazy danych statystycznych (np. GUS, Eurostat). Kluczowe jest jednak wskazanie, że powinny one być zróżnicowane. Wykorzystanie analityki danych oznacza bowiem łączenie różnych źródeł, dzięki czemu możliwe jest pozyskanie takich informacji, których nie można otrzymać z każdej z baz danych z osobna, a także to, że analiza dotyczy ogromnych ilości danych, a zatem tradycyjne metody audytowe nie byłby w pełni adekwatne. Możliwe jest np. analizowanie danych dotyczących transakcji finansowych, w połączeniu z informacjami z systemów ERP (do planowania zasobów przedsiębiorstwa), CRM (do zarządzania z klientami) a nawet mediów społecznościowych. Dzięki zaawansowanym narzędziom analitycznym, takim jak sztuczna inteligencja (ang. *artificial inteligence*, AI) i uczenie maszynowe (ang. *machine learning*), możliwe jest automatyczne wykrywanie wzorców i anomalii, które mogą wskazywać na oszustwa i nadużycia.

Integracja informacji z różnorodnych źródeł znacząco zwiększa potencjał audytów śledczych. Audytorzy mogą analizować dane z systemów ERP, mediów społecznościowych, a także zewnętrznych baz danych, co pozwala na uzyskanie pełniejszego obrazu sytuacji finansowej i operacyjnej organizacji oraz jej otoczenia zewnętrznego[45]. Dzięki temu możliwa jest lepsza ocena ryzyka i podejmowanie bardziej świadomych decyzji. Wykorzystując technikę analizy predyktywnej, można

[44] Przykładem wykorzystania narzędzi big data w tym obszarze jest Arachne. To narzędzie punktowej oceny ryzyka, opracowane przez Komisję Europejską w celu wspierania instytucji zarządzających odpowiedzialnych za europejskie fundusze strukturalne i inwestycyjne przez zapewnienie im narzędzia punktowej oceny ryzyka, aby mogły skutecznie i wydajnie wykrywać najbardziej ryzykowne projekty, kontrakty, wykonawców i beneficjentów. W wymiarze technicznym Arachne jest narzędziem eksploracji danych/oceny ryzyka, wspierającym instytucje zarządzające w kontrolach administracyjnych za pomocą modeli predykcyjnych wykrywających nadużycia finansowe dla Europejskiego Funduszu Społecznego (EFS) i Europejskiego Funduszu Rozwoju Regionalnego (EFRR). W systemie przetwarza i analizuje się dane dwóch milionów beneficjentów i krzyżuje je z informacjami z zewnętrznych baz danych, które zawierają informacje o ponad 210 milionach firm i 120 milionach osób stojących za tymi firmami. Ma to doprowadzić do sytuacji, w której system monitorowania stanie się bardziej wydajny i zdolny do wykrywania oszustw i niewłaściwego zarządzania środkami publicznymi. *Arachne. Karta dotycząca wprowadzenia i stosowania narzędzia punktowej oceny ryzyka Arachne w kontrolach zarządczych*, Komisja Europejska, <https://ec.europa.eu/social/BlobServlet?docId=14836&langId=pl>, (dostęp 18.2.2024); *Use of big data and AI in fighting corruption and misuse of public funds. Good practice, ways forward and how to integrate new technology into contemporary control framework,* organized by the Policy Department on Budgetary Affairs for the Committee on Budgetary Control, European Parliament 2021.

[45] Zob. Z. Dobrowolski, J. Kościelniak: *Audyt śledczy…*, op.cit., s. 45.

prognozować przyszłe ryzyko nadużyć, co pozwala na wcześniejsze wdrożenie działań zapobiegawczych. Największą przewagą analityki danych nad prostymi procedurami analitycznymi jest jej zdolność do oceny ryzyka, identyfikacji anomalii i wykrywania błędów. W przeciwieństwie do tradycyjnych praktyk audytu, wykorzystanie zaawansowanej technologii zapewnia wyższą jakość dowodów, które pochodzą z wielu nowych źródeł, w tym dużych zbiorów danych, danych egzogenicznych. Tym samym zwiększają się zdolności do łączenia różnych procesów, potwierdzania baz danych i ciągłego monitorowania alertów (tzw. czerwonych flag)[46]. Wskazuje się, że digitalizacja audytu i wykorzystanie w nim zaawansowanych narzędzi analitycznych prowadzi do sześciu kluczowych rezultatów[47]: 1) zwiększenia znaczenia audytu, 2) poszerzenia oferty usług audytowych; 3) poprawy jakość audytu, 4) zintegrowanej analizy wszystkich danych organizacji; 5) zmiany profilu audytora; 6) zwiększenia innowacyjności działalności audytorskiej.

Tradycyjnie w audycie i kontroli wykonania zadań wykorzystuje się takie analizy ekonometryczne i statystyczne, jak[48]: analizy wskaźnikowe, analizę koszt – korzyść; analizę opłacalności (koszt – efekt); analizę korelacji; analizę regresji; analizę szeregów czasowych; analizę porównawczą (ang. *benchmarking*) czy analizę obwiedni danych (ang. *Data Envelopment Analysis*). W analityce danych, ze względu na wykorzystywane źródła, stosuje się inne metody i techniki. Kluczowym procesem jest tu ETL – ujawnij, przetwórz, załaduj (ang. *Extract, Transform, Load*). Umożliwia on integrację i przetwarzanie danych z różnych źródeł, takich jak bazy danych, pliki API (ang. *application programming interface*), czyli interfejs programowania aplikacji czy systemy zewnętrzne, i ich dalsze przekształcenie (co może obejmować: czyszczenie danych, normalizację, agregację) oraz załadowanie przekształconych danych do docelowego systemu, takiego jak hurtownia danych lub inny system analityczny. To pozwala na dalszą analizę i raportowanie. Wśród innych metod, które wydają się być przydatne w audycie śledczym można wskazać: uczenie maszynowe, analizę skupień czy klastrowanie. Uczenie maszynowe jest jedną z najpowszechniej stosowanych metod analityki danych. Polega ona na automatyzacji tworzenia modeli analitycznych (uczenie odbywa się na podstawie danych, a ulepszenia następują bez potrzeby bezpośrednich instrukcji). Wyróżnia się uczenie nadzorowane (model jest trenowany na oznaczonych danych, co oznacza, że dane wejściowe są połączone z odpowiednimi wynikami), uczenie nienadzorowane (model pracuje z danymi, które nie mają oznaczeń, i stara się znaleźć ukryte wzorce lub grupy) oraz uczenie

[46] Por. W.R. Titera: *Updating Audit Standard-Enabling Audit Data Analysis*, „Journal of Information Systems" nr 1/2013.
[47] M. Boersma: *(Data) science in financial audits*, „Compact Transparency of Information" nr 4/2018.
[48] W. Karliński, Webinarium: Analiza danych w audycie cz. 2: Podstawowe metody analizy danych (23 marca 2023 r.), https://www.gov.pl/web/finanse/webinarium-analiza-danych-w-audycie-cz-2-podstawowe-metody-analizy-danych-23-marca-2023-r, dostęp 17.03.2025.

przez wzmocnienie (model uczy się dzięki interakcji z otoczeniem, otrzymując nagrody lub kary w zależności od swoich działań). Z kolei analiza skupień (klastrów, klasteryzacja) to metoda nienadzorowanej klasyfikacji, która dzieli zbiór obiektów na podgrupy (klastry) na podstawie ich cech. Jej głównym celem jest grupowanie obiektów w taki sposób, aby obiekty w tych samych grupach były do siebie bardziej podobne niż obiekty w różnych grupach. Z kolei eksploracja reguł asocjacyjnych to proces, który polega na odkrywaniu zależności między różnymi elementami w dużych zbiorach. Jest to kluczowy aspekt analizy danych, szczególnie w kontekście danych transakcyjnych.

Wraz z pojawieniem się zaawansowanej analityki danych i AI audyt śledczy zyskał dodatkowe możliwości wykrywania nieprawidłowości. Jednocześnie musi on podołać coraz trudniejszym zadaniom. Nieuczciwe działania finansowe stały się bardziej złożone, wymagają innowacyjnych technik wykrywania i zapobiegania. Rozwój big data, uczenia maszynowego i analityki predykcyjnej przekształcił audyt śledczy, umożliwiając profesjonalistom wydajną i dokładną analizę ogromnych zestawów informacji. Tradycyjne metody audytu śledczego w dużej mierze polegały na przeglądach opartych na próbkach, które były czasochłonne i miały ograniczony zakres. Jednak wraz z rozwojem cyfrowych narzędzi śledczych, audytorzy mogą teraz przeprowadzać kompleksowe analizy[49], ujawniając nieuczciwe wzorce, które dotychczas mogły pozostawać niezauważone. Ponieważ transakcje finansowe są coraz częściej przeprowadzane za pośrednictwem platform cyfrowych, audytorzy śledczy muszą wyprzedzać wyrafinowane taktyki oszustw, które wykorzystują luki technologiczne. Wykorzystanie technologii *blockchain* (umożliwia wybranej grupie uczestników dzielenie się danymi umieszczanymi w zewnętrznym rejestrze, np. w chmurze), monitorowania transakcji w czasie rzeczywistym i narzędzi do oceny ryzyka opartych na AI rewolucjonizuje dochodzenia finansowe. Ponadto organy regulacyjne na całym świecie przyjmują bardziej rygorystyczne środki zgodności, co wymaga od urzędników dostosowania swoich praktyk do norm prawnych i etycznych.

Analiza big data i AI oferuje znaczne korzyści, stwarza również wyzwania etyczne, w tym związane z prywatnością danych, ale także bezpieczeństwem i stronniczością w procesie analizy. Zapewnienie dokładności i niezawodności uzyskanych informacji ma kluczowe znaczenie, jeśli chce się uniknąć błędnych wniosków[50]. Potencjał algorytmów uczenia maszynowego do dziedziczenia stronniczości z historycznych danych o oszustwach jest poważnym problemem, ponieważ stronnicze modele mogą niesłusznie wskazywać na określone grupy lub nie wykrywać pojawiających się schematów oszustw. Ponadto zbytnie poleganie na cyfrowych technikach kryminalistycznych wymaga od audytorów

[49] W. Karliński: *Metody analityczne w procesie kontrolnym*, „Kontrola Państwowa" nr 1/2024.
[50] F. Amalina, I.A.T. Hashem, Z.H. Azizul, A.T. Fong, A. Firdaus, M. Imran, N.B. Anuar: *Blending big data analytics: Review on challenges and a recent study*, „Ieee Access" nr 8/2019.

śledczych rozwijania wiedzy specjalistycznej w zakresie zaawansowanych technologii i środków cyberbezpieczeństwa[51]. Organizacje powinny wdrażać rygorystyczne zasady zarządzania danymi, aby chronić poufne informacje finansowe i zapewnić zgodność z wymogami regulacyjnymi (ang. *compliance*). Rozważania etyczne obejmują również odpowiedzialne korzystanie z AI, zapewniając, że zautomatyzowane procesy podejmowania decyzji pozostaną przejrzyste i rozliczalne. Tym bardziej, że w miarę rozwoju technologii pożądane jest, aby audyt śledczy integrował bardziej zaawansowane algorytmy AI, technologię blockchain i analizę big data. Blockchain zapewnia przejrzysty i odporny na manipulacje rejestr transakcji finansowych, zwiększając tym samym możliwości wykrywcze[52]. Wykorzystanie automatycznego wykonywania określonych procedur badania (np. tzw. inteligentnych kontraktów) i monitorowanie transakcji w czasie rzeczywistym za pośrednictwem tych technologii minimalizuje ryzyko manipulacji i zapewnia rozliczalność w operacjach biznesowych. Są one zatem przydatne zarówno przy analizie ryzyka w czasie audytu, jak i w działaniach wykrywczych.

Analityka wykorzystująca zbiory big data w pewien sposób zrewolucjonizowała audyt śledczy, dostarczając narzędzi do wykrywania wzorców, anomalii w odniesieniu do profilaktyki i detekcji nadużyć w dużych zestawach danych. Eksploracja danych, klastrowanie, klasyfikacja i eksploracja reguł asocjacyjnych pozwalają analizować m.in. podejrzane transakcje[53]. Ogromna liczba przypadków poddawanych analizie pozwala na identyfikację nietypowych zachowań, np. częstotliwości transakcji, wysokości kwot lub nieregularny czas transakcji[54]. Wykorzystując modele statystyczne, audytorzy śledczy mogą odkryć rozbieżności, które wskazują na manipulację finansową. W procesie analizy śledczej istotne są także sposoby prezentacji informacji śledczych, jak narzędzia do wizualizacji danych, w tym wykresy punktowe, mapy cieplne i wykresy słupkowe, dodatkowo usprawniające wykrywanie oszustw, dzięki temu że przedstawiają złożone dane finansowe w sposób możliwy do zinterpretowania przez audytora/analityka[55]. Zaawansowane rozwiązania pulpitu nawigacyjnego zapewniają audytorom śledczym aktualizacje uzyskiwanych informacji w czasie rzeczywistym i alerty wizualne w wypadku wykrycia anomalii. Ponadto zautomatyzowane skrypty i automatyzacja procesów robotycznych (RPA) usprawniają identyfikację podejrzanych transakcji, zmniejszając obciążenie ręczną pracą i zwiększając wydajność. Możliwość automatyzacji dochodzeń finansowych

[51] V. Chang: *An ethical framework for big data and smart cities*, „Technological Forecasting and Social Change" nr 165/2021.
[52] M.T. Oladejo, L. Jack: *Fraud prevention and detection in a blockchain technology environment: challenges posed to forensic accountants*, „International Journal of Economics and Accounting" nr 4/2020.
[53] Por. Y. Liu, R. Jia, J. Ye, X. Qu: *How machine learning informs ride-hailing services: A survey*, „Communications in Transportation Research" nr 2/2022.
[54] A. Wygodny: *Sztuczna inteligencja w audycie i zarządzaniu ryzykiem*, „Kontrola Państwowa" nr 6/2024.
[55] T. Fawcett, F. Provost: *Adaptive fraud detection*, „Data mining and knowledge discovery" nr 1/1997.

za pomocą analiz opartych na AI zmniejsza liczbę błędów i pozwala audytorom śledczym skupić się na przypadkach wysokiego ryzyka, które wymagają szczegółowej analizy.

Techniki uczenia maszynowego, w tym uczenie nadzorowane i nienadzorowane mogą być z powodzeniem wykorzystywane w audycie śledczym. Nadzorowane modele uczenia, takie jak drzewa decyzyjne, regresja logistyczna i maszyny wektorów nośnych, umożliwiają przewidywanie oszukańczych transakcji na podstawie danych historycznych[56]. Modele te wykorzystują oznaczone zestawy danych do trenowania algorytmów w rozpoznawaniu oszukańczych zachowań, co pozwala na zwiększoną dokładność w identyfikowaniu potencjalnych nadużyć finansowych. Techniki uczenia nienadzorowanego, takie jak algorytmy klastrowania, ujawniają z kolei podejrzane transakcje dzięki grupowaniu danych o podobnych cechach[57]. Anomalie w tych klastrach często oznaczają nieprawidłowości finansowe, co skłania do dalszych badań. Ponadto modele głębokiego uczenia, w szczególności sieci neuronowe, okazują się przydatne w wykrywaniu wzorców oszustw przez analizę złożonych relacji w danych transakcyjnych. Zastosowanie uczenia się przez wzmacnianie, które z czasem dostosowuje się do nowych schematów oszustw, dodatkowo zwiększa możliwości wykrywcze, zapewniając ciągłe udoskonalenia w zakresie identyfikacji podejrzanych działań finansowych. Należy podkreślić, że schematy uczenia maszynowego daleko wykraczają poza analizę transakcji.

W audycie wykorzystuje się także lingwistykę śledczą opartą na AI do analizy danych tekstowych, w tym wiadomości e-mail, treści umów i sprawozdań finansowych. Techniki programowania neurolingwistycznego (NLP) pozwalają ujawniać intencje oszustwa w schematach komunikacji, co może okazać się przydatne w analizie ryzyka popełnienia nadużyć i oszustw. Z kolei techniki modelowania predykcyjnego, w tym analiza szeregów czasowych, analiza regresji i sieci bayesowskie[58] mogą informować organizacje o potencjalnych ryzykach oszustw, zanim się one zmaterializują, umożliwiając proaktywne strategie[59]. Proaktywność uwzględnia czynniki, takie jak zachowania finansowe, normy branżowe i wykorzystanie historycznych danych dotyczących oszustw, aby ocenić prawdopodobieństwo wystąpienia *fraudu* w określonym środowisku biznesowym. Organizacje, które integrują analitykę predykcyjną ze swoimi procesami audytu śledczego, korzystają ze zwiększonej dokładności wykrywania oszustw i zmniejszonych strat

[56] C.W. Cai, M.K. Linnenluecke, M. Marrone, A.K. Singh: *Machine learning and expert judgement: analyzing emerging topics in accounting and finance research in the Asia–Pacific*, „Abacus" nr 4/2019.

[57] Y. Liu, R. Jia, J. Ye, X. Qu: *How machine learning informs ride-hailing services: A survey*, „Communications in Transportation Research" nr 2/2022.

[58] M. Kuhn, K. Johnson: *Applied predictive modeling,* New York: Springer, 2013, s. 13.

[59] M. Soltani, A. Kythreotis, A. Roshanpoor: *Two decades of financial statement fraud detection literature review; combination of bibliometric analysis and topic modelling approach*, „Journal of Financial Crime" 2023.

finansowych. Integracja analityki predykcyjnej opartej na AI z ramami zarządzania ryzykiem zwiększa bezpieczeństwo finansowe, czyniąc organizacje bardziej odpornymi na zagrożenia związane z wystąpieniem oszustw.

Sztuczna inteligencja, a w szczególności uczenie maszynowe i programowanie neurolingwistyczne (NLP), wzmacniają tradycyjne działania audytu śledczego głównie przez automatyzację dotychczasowych procesów. Narzędzia oparte na AI analizują ogromne zbiory danych, wykrywają anomalie i dostosowują się do zmieniających się wzorców oszustw, zmniejszając zależność od wstępnie zdefiniowanych reguł[60]. Narzędzia te nieustannie uczą się na podstawie nowych przypadków, zwiększając potencjał wykrywczy audytu. Techniki NLP umożliwiają z kolei analizę niestrukturalnych danych, takich jak wiadomości e-mail i raporty finansowe[61]. Narzędzia te skanują duże ilości danych tekstowych w celu wykrycia podejrzanych wzorców językowych, zmian nastrojów lub zmów wśród pracowników. Ponadto narzędzia do oceny ryzyka oparte na AI zapewniają dostęp do danych w czasie rzeczywistym, a w konsekwencji umożliwiają organizacjom ustalanie priorytetów dla przypadków wysokiego ryzyka i skuteczniejsze dysponowanie zasobami, aby zapobiec nadużyciom.

Badanie informacji ze źródeł otwartych

Jedną z technik wykorzystywanych w zbieraniu informacji w audycie śledczym jest wywiad oparty na źródłach otwartych OSINT[62]. Nazywano go także „białym wywiadem". Polega nazbieraniu i analizie informacji ze źródeł powszechnie i legalnie dostępnych[63]. OSINT nie wymaga, co do zasady, zaawansowanego sprzętu technicznego i fachowej wiedzy na temat jego obsługi[64] w celu identyfikacji, gromadzenia i interpretacji informacji wywiadowczych[65]. Informacja wywiadowcza to: „(k)ażda informacja (...) uzyskana bądź wytworzona w wyniku celowych i kierunkowych działań, zmierzających do zaspokojenia (...) potrzeb informacyjnych w prowadzonej sprawie/postępowaniu[66]". W omawianym wypadku to przede wszystkim pozyskiwanie takich informacji, a nie ich tworzenie. Szukane informacje

[60] W. Hilal, S.A. Gadsden, J. Yawney: *Financial fraud: a review of anomaly detection techniques and recent advances*, „Expert Systems with Applications" nr 193/2022.

[61] A. Naqvi: *Artificial intelligence for audit, forensic accounting, and valuation: a strategic perspective*. John Wiley & Sons, 2020.

[62] Przede wszystkim szeroko rozumianych mediów, a zwłaszcza zasobów internetowych.

[63] W przeciwieństwie do informacji ze źródeł zamkniętych, czyli oznaczających „informacje, które gromadzi się w określonym celu i których dostępność dla ogółu społeczeństwa jest ograniczona", oraz informacji ze źródeł niejawnych oznaczających „informacje zgromadzone operacyjnie przez specjalnie do tego celu przeznaczone niejawne środki, w tym z wykorzystaniem osobowych źródeł informacji oraz techniki operacyjnej". Por. UNODC, *Analiza kryminalna…*, op.cit., s. 12.

[64] *OSINT, czyli biały wywiad – co to jest?*, „Biznes Netia" 2024, <https://www.netia.pl/pl/srednie-i-duze-firmy/youtro-strefa-wiedzy/osint-czyli-bialy-wywiad-jak-mozna-go-wykorzystac-w-biznesie> (dostęp 3.2.2025.

[65] Zob. W. Ignaczak, M. Dyjasz, *Audyt śledczy…*, op.cit., s. 34-50.

[66] ibid.

mogą dotyczyć ludzi, instytucji i rzeczy, a także miejsc i czasu. Ludzie popełniają przestępstwa, a instytucje są ich narzędziami[67]. OSINT umożliwia zgromadzenie poszlak i faktów dotyczących osób i ich powiązań, co pozwala na uprawdopodobnienie popełnienia oszustw[68] dzięki ujawnieniu przesłanek przemawiających za popełnieniem danego czynu.

OSINT może być cennym uzupełnieniem opisanej wyżej analizy big data. O ile ta pierwsza skupia się zwykle na szukaniu trendów i prawidłowości, przyjmując perspektywę „z lotu ptaka", to OSINT poszukuje informacji o poszczególnych osobach na podstawie detali. Aby opisać specyfikę tej formy zbierania informacji, należy zacząć od podstawowych pojęć. Pozwoli to przedstawić proces pozyskiwania i interpretacji danych. Należy pamiętać, że mowa tu o działaniach wywiadowczych wspierających działania śledcze, stąd też pojęcia użyte w dalszej części tekstu mają właśnie rodowód wywiadowczy. W nomenklaturze OSINT funkcjonują pojęcia „figuranta", „selektora" i „transformacji"[69]. Figurant to osoba, na temat której poszukuje się informacji. Jest to pojęcie o tyle istotne, że przestępstwa popełniają osoby fizyczne, a instytucje służą im do działań przestępczych. Instytucje tworzone są przez ludzi, czyli właśnie figurantów. Pojęcie „figurant" będzie używane w dalszej części tekstu w odniesieniu do osoby, wobec której prowadzone są działania wywiadowcze. Przez selektor rozumie się podstawową informację na temat figuranta[70]; może być to zdjęcie, nazwisko, numer PESEL, profil na portalu społecznościowym itp. Transformacją jest natomiast powiązanie prowadzące do kolejnego selektora. Ilustrując to pojęcie, posłużyć się można znanym przykładem tablicy korkowej – tablica to prowadzone śledztwo, przybite do niej pinezkami zdjęcia, wycinki prasowe i inne informacje o figurancie to selektory, natomiast łączące je nitki włóczki to transformacje[71].

W dzisiejszych czasach OSINT to poszukiwanie informacji głównie w Internecie. Zakłada się, że każda jest istotna dla prowadzonego postępowania do momentu

---

[67] W klasycznym materiale śledczym „Anatomia zabijania" (ang. *Anatomy of a Killing*), dziennikarze BBC zidentyfikowali kameruńskich żołnierzy jako sprawców masowego morderstwa. Audytor śledczy nie spotka się raczej z tak dramatyczną sprawą, jednak przytaczany materiał jest treściwą ilustracją pracy białym wywiadzie. Por. BBC *Cameroon: Anatomy of a Killing – BBC Africa Eye Documentary*, 2018; BBC *Anatomy of a Killing: What Happened Next? – BBC Africa Eye Documentary,* (29.1.2025).

[68] Por. Z. Dobrowolski, J. Kościelniak: *Audyt śledczy w spółkach Skarbu Państwa i spółkach komunalnych*, Instytut Spraw Publicznych UJ, Kraków 2018, s. 6.

[69] Zob. *Cyber Academy, OSINT – biały wywiad,* Piotr Konieczny, Niebezpiecznik.pl, 2020, <https://www.youtube.com/watch?v=JHSHUXlkeTg> [dostęp 4.2.2025].

[70] Czyli osoby, której dotyczy analiza. W odniesieniu do audytu śledczego, będzie to osoba, która mogła popełnić nadużycie. Por. przyp. 67.

[71] H. Lengyel: *From Clues to Connections: The Power of Crime Boards in Investigations - Community Learning Training*, <https://blog.commlearning.com/from-clues-to-connections-the-power-of-crime-boards-in-investigations/>, (dostęp 3.3.2025). Warto nadmienić istnienie specjalistycznego oprogramowania do prowadzenia działań śledczych działających na zasadzie tablicy korkowej, np. Maltego <https://www.maltego.com> czy LinkScope <https://accentusoft.com>. Por. także <https://alternativeto.net/software/maltego/>.

jego zakończenia. Do prowadzenia białego wywiadu nie jest wymagane bycie informatykiem, często bywa jednak przydatna znajomość zaawansowanych technik wyszukiwania[72], narzędzi ułatwiających pozyskiwanie informacji[73] oraz „cyfrowego BHP"[74]. Ważne są dociekliwość, erudycja i umiejętność nieszablonowego myślenia oraz odporność na frustrację – o ile techniki OSINT mogą być przydatne także w audycie śledczym, to nie gwarantują one sukcesu poszukiwań[75].

Aktywność w Internecie zostawia ślady, dlatego należy postępować tak, aby w miarę możliwości je zacierać[76]. Zasada ta, paradoksalnie, dotyczy zarówno audytora, jak i potencjalnego sprawcy nadużycia. Prowadzenie poszukiwań z własnego bądź służbowego konta może dać osobie podejrzewanej o oszustwo sygnał, że znalazła się w obszarze zainteresowania audytora śledczego lub organów ścigania i może ją to skłonić do usunięcia potencjalnych śladów i dowodów. W wypadku informacji publicznej łatwiejsze może być jej uzyskanie na wniosek wysłany z domeny komercyjnej niż publicznej lub kojarzonej z organizacją prowadząca audyty, kontrole czy dochodzenia.

Przeszukiwane zasoby internetowe można podzielić na trzy warstwy: 1) sieć otwartą, 2) głęboką sieć (ang. *deep web*), 3) ciemną sieć (ang. *dark web*), która nie będzie w tym artykule szerzej omawiana[77]. Sieć otwarta to w zasadzie wszystko, co rozumie się potocznie pod pojęciem Internetu: strony i serwisy. *Deep web* to także sieć otwarta, jednak jej zasoby są trudniejsze do wyszukania i przeglądania. Nie wynika to z braku ich nielegalności, lecz zazwyczaj specjalistycznego charakteru lub niechęci bądź niezdolności do zindeksowania zawartości strony. Ponadto nie wszystkie strony internetowe pozwalają na indeksowanie[78]

---

[72] Zob. poniżej.

[73] Jak np. skrypty w języku Python: holehe pozwalający sprawdzić, w jakich domenach zarejestrowany jest dany adres email bądź skrypt Sherlock do wyszukiwania nazw użytkownika w mediach społecznościowych. Zob. *10 Python OSINT Tools for Investigating Disinformation and Extremism*, 2024, <https://medium.com/@thecyberhuntress/10-python-osint-tools-for-investigating-disinformation-and-extremism-c83b2f33fee6> (dostęp 31.1.2025); także *Python OSINT scripts,* 2024, <www.reddit.com/r/OSINT/comments/17x0qkl/python_osint_scripts/> (dostęp 31.1.2025).

[74] Warto korzystać z VPN. W wypadku adresów internetowych lepiej posługiwać się osobnymi adresami mailowymi tylko do tego, a *social mediów* – kilka profili, których będzie można używać do ich przeszukiwana bądź pytania o informację publiczną. Profile takie powinny być traktowane jako „robocze". Powinny być także odpowiednio „zalegendowane", tzn. powinna mieć na nich miejsce w miarę normalna aktywność, powinny funkcjonować w sieciach społecznych. Innymi słowy – być prowadzone w taki sposób, aby nie wzbudzać podejrzeń. Zob. R. Baker, M. Hoffman: *Prawdziwa głębia*…, op.cit., s. 108.

[75] W wymienionym wyżej reportażu *Anatomy of a Killing* dziennikarze sprawdzali ręcznie ukształtowanie geograficzne strefy Sahelu. Możliwe, że nie zidentyfikowaliby miejsca, gdyby nie wskazówka informatora, by sprawdzić okolice miejscowości Zelevet. Por. *Cameroon: Anatomy of a Killing*.

[76] R. Baker, M. Hoffman: *Prawdziwa głębia*…, op.cit., rozdz. 4.3.

[77] W odróżnieniu od poprzednich dwóch, dark web zawiera często dane nielegalne, zazwyczaj niedostępne bez użycia wyspecjalizowanych usług (np. sieci TOR). Autorzy wyrażają wątpliwość, czy w wypadku audytu śledczego zagłębianie się w dark web jest konieczne, a w każdym razie zalecają bardzo daleko idącą ostrożność.

[78] Rejestracji przez mechanizmy wyszukiwarek internetowych.

swojej zawartości[79]. Innym przykładem głębokiego Internetu jest „zaplecze" strony, czyli katalogi serwera, gdzie przechowywane są jej pliki czy usługa ftp[80] do internetowego przesyłania plików. W tej samej kategorii zawierają się także sieci P2P (ang. *peer-to-peer*)[81], w których wszystkie urządzenia są równe w hierarchii, archiwum *Usenet*[82], służące horyzontalnemu dzieleniu się plikami między użytkownikami czy usługa *Wayback Machine*[83] umożliwiająca poszukiwanie archiwalnych stron internetowych (o ile zostały zindeksowane), co może np. pozwolić na znalezienie archiwalnej wersji strony z ogłoszeniem o badanym przetargu i sprawdzenie, czy i jak było ono zmieniane. *Deep web* może być przydatne dla audytora śledczego na kilka sposobów. W folderze ftp mogą znajdować się dokumenty, które nie byłyby dostępne w innym miejscu. Także zawartość wielu z opisanych niżej rejestrów i ewidencji nie jest indeksowana przez wyszukiwarki. Wyszukiwarki są podstawowym narzędziem OSINT. Nazwa *Google* stała się synonimem wyszukiwarki, ale warto pamiętać o istnieniu innych systemów: *Bing, DuckDuckGo, Yandex, Baidu* i innych[84]. Mają one różne mechanizmy działania[85] (np. *Yandex* jako przeglądarka rosyjska lepiej indeksuje treści wschodnioeuropejskie i lepiej rozpoznaje twarze o słowiańskich rysach), dlatego w audycie śledczym warto korzystać z nich symultanicznie. Przeglądarki mają także szereg zaawansowanych ustawień pozwalających na precyzowanie wyników wyszukiwania[86]. Dzięki zawężeniu poszukiwania do konkretnej domeny i typu plików do doc i pdf można znaleźć umieszczone na serwerze przydatne dokumenty.

Audyt śledczy opiera się jednakże przede wszystkim na dostępie do informacji publicznej dotyczącej osób i instytucji[87]. Dlatego też poszukiwania audytora śledczego korzystającego z OSINT będą odbywać się w głównie, o ile nie wyłącznie, na dwóch pierwszych poziomach sieci. Dotyczy to przeze wszystkim publicznych rejestrów i ewidencji. Mogą mieć one charakter

[79] Przykładowo wpisując w okno wyszukiwarki Google hasło „osobowość autorytarna adorno buw", nie otrzyma się linku kierującego do pozycji katalogowej „Osobowości autorytarnej" Theodora Adorno w Bibliotece Uniwersytetu Warszawskiego, mimo że posiada ona tę pozycję w swoich zbiorach; książkę można odnaleźć przez katalog BUW na jej stronie.

[80] Ang. file transfer protocol. Zob. „Pomoc home.pl" *Co to jest FTP?*, 2024, <https://pomoc.home.pl/baza-wiedzy/co-to-jest-ftp> (dostęp 3.2.2025).

[81] Por. Blog Netia.pl „Sieć peer to peer (P2P) – co to jest?", 2021, <https://www.netia.pl/pl/blog/siec-peer-to-peer-p2p-co-to-jest> (dostęp 3.2.2025).

[82] Ogólnoświatowy system grup dyskusyjnych, z którego można korzystać przez Internet. por. <http://www.usenet.pl>.

[83] *Wayback Machine*, <https://web.archive.org/> (dostęp 31.1.2025).

[84] Np. Brave czy Presearch.

[85] R. Baker, M. Hoffman: *Prawdziwa głębia*…, op.cit., s. 115.

[86] Zob. ZPE MEN, *Advanced methods of searching information*, <https://zpe.gov.pl/a/advanced-methods-of-searching-information/DqvCEevlo> (dostęp 31.1.2025); J. Hardwick: *Google Search Operators: The Complete List (44 Advanced Operators)*, 2024, <https://ahrefs.com/blog/google-advanced-search-operators/> (dostęp 31.1.2025).

[87] R. Baker, M. Hoffman: *Prawdziwa głębia*…, op.cit., rozdz. 5.6.

otwarty bądź częściowo otwarty. Rejestry otwarte opierają się w przeważającej części na zasadzie dostępu do informacji publicznej, publikowanej m.in. w Biuletynie Informacji Publicznej oraz w portalach danych[88]. Przykładem rejestru półotwartego jest Centralna Ewidencja Pojazdów i Kierowców, z której dane dotyczące pojazdu dostępne są osobie nieuprawnionej na uzasadniony wniosek po wniesieniu stosownej opłaty[89]. W kontekście prowadzenia audytu śledczego interesujące są przede wszystkim rejestry dotyczące obrotu gospodarczego. W pierwszej kolejności jest to Krajowy Rejestr Urzędowy Podmiotów Gospodarki Narodowej (REGON), prowadzony przez Główny Urząd Statystyczny, gromadzący dane podmiotów zajmujących się działalnością gospodarczą. Poza tym, użytecznym źródłem danych w audycie śledczym są Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG), prowadzona przez ministra właściwego do spraw gospodarki oraz Krajowy Rejestr Sądowy (KRS), prowadzony przez sądy gospodarcze. W CEIDG rejestrowani są przedsiębiorcy będący osobami fizycznymi[90]. Pozwala ona np. na określenie numeru identyfikacji podatkowej (NIP) figuranta, a to – na sprawdzenie, który Urząd Skarbowy nadał mu ów numer; wówczas można szukać jego miejsca zamieszkania. Krajowy Rejestr Sądowy zawiera wykazy: 1) przedsiębiorców (niebędących osobami fizycznymi); 2) stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej oraz 3) dłużników niewypłacalnych. Na Portalu Rejestrów Sądowych można znaleźć także przeglądarkę dokumentów finansowych oraz Repozytorium Akt Rejestrowych[91]. To ostatnie jest szczególnie ciekawe, gdyż może pozwolić wyodrębnić np. selektor w postaci listy obecności na walnym zebraniu członków stowarzyszenia, do którego należy figurant, a na jego podstawie dotrzeć do innych osób, z którymi jest związany. Monitor Sądowy i Gospodarczy zawiera ogłoszenia wynikające z ustawy: wszystkie wpisy do KRS, ogłoszenia wymagane przez Kodeks spółek handlowych i przewidziane przepisami Kodeks postępowania cywilnego, a także inne obwieszczenia i ogłoszenia.

Elektroniczne Księgi Wieczyste[92] pozwalają uzyskać informacje na temat nieruchomości (w szczególności własności i obciążeń), podczas gdy rejestr zastawów[93] sprawdzić obciążenia rzeczy ruchomych. W wypadku pojazdów interesującym źródłem jest także Ubezpieczeniowy Fundusz

[88] Zob. Art. 7 ustawy z 6.9.2001 o dostępie do informacji publicznej (Dz.U. 2001 nr 112 poz. 1198).
[89] Zob. *Wniosek o dostęp do cepik*, <http://www.cepik.gov.pl/dla-obywateli/wniosek-o-dostep-do-cepik> (dostęp 31.1. 2025).
[90] W tym przedsiębiorstw w spadku pod firmą zmarłego przedsiębiorcy; zawiera też ona adnotacje o ewentualnym uczestnictwie w spółce cywilnej.
[91] Zob. <https://rar.ms.gov.pl> (dostęp 31.1.2025).
[92] Zob. <https://ekw.ms.gov.pl/eukw_ogol/menu.do> (dostęp 31.1.2025).
[93] Dostępny poprzez Elektroniczny dostęp do Sądów Rejestrowych/Centralnej Informacji/MSIG, <https://pdi.ms.gov.pl>.

Gwarancyjny. Innymi mniej znanymi źródłami są E-justice Europa.eu[94], agregujący dane dotyczące nieruchomości i prawników w Unii Europejskiej, rejestry prowadzone przez Urząd Ochrony Konkurencji i Konsumentów[95], rejestry Urzędu Patentowego[96], Głównego Urzędu Nadzoru Budowlanego[97], Portal Orzeczeń Sądów Powszechnych[98]. Istnieją także rejestry prowadzone przez podmioty niepaństwowe, jak Jawne Partie i Opencorporates.com, zbierający dane na temat spółek z całego świata czy Import Yeti[99], który pozwala sprawdzić zagranicznych kontrahentów przedsiębiorców. Mniej oczywistymi źródłami informacji są giełdy długów i ogłoszenia licytacji komorniczych, umożliwiające gromadzić selektory dotyczące nieruchomości i ruchomości.

W procesie audytu śledczego użyteczny jest także dostęp do zamkniętych rejestrów administracji państwowej, takich jak baza systemu ewidencji ludności PESEL, rejestr zgonów, dostęp do baz Krajowej Administracji Skarbowej (część z nich przez API) czy do danych systemu Trezor 3.0, rejestrującego wykonanie budżetu państwa (także częściowo dostępnego via API[100]). Możliwość korzystania z nich daje ogromną przewagę w stosunku do wywiadowcy, który nie ma takich uprawnień, gdyż pozwala na dostęp do selektorów pozwalających na precyzyjne lokalizowanie figurantów. Niemniej należy pamiętać o możliwości zwrócenia się bezpośrednio z wnioskiem o udzielenie informacji publicznej.

Źródłami mniej konwencjonalnymi w kontekście audytu śledczego są także Repozytorium Standardów Informacyjnych GUS, będące rodzajem rejestru rejestrów prowadzonych przez podmioty publiczne wraz z adnotacjami o ich zawartości i sposobie dostępu. Dane te charakteryzują się różnym stopniem kompletności, jednakże wciąż możliwe jest, że znajdą się w nich informacje przydatne w audycie śledczym. Jako ciekawy przykład wykorzystania źródeł nieoczywistych, pozornie nieznajdujących zastosowania w procesie audytu, może posłużyć np. wyszukiwarka grobów (przydatna, gdy „słupem"[101] jest osoba zmarła). Warto w tym miejscu wskazać różnice między wyszukiwarkami grobów, a wcześniej wspomnianą bazą zgonów. Pomimo pozornego podobieństwa dotyczą one trochę innych zakresów informacji. Baza zgonów pozwala na potwierdzenie, że dana osoba nie żyje, oraz to gdzie, kiedy i z jakich przyczyn nastąpił

[94] Zob. <https://e-justice.europa.eu/home?action=home&plang=pl> (dostęp 31.1.2025).
[95] Np. rejestr decyzji, rejestr produktów niebezpiecznych, rejestr ostrzeżeń i System Udostępniania Danych o Pomocy Publicznej; por. <https://uokik.gov.pl/bip/rejestry-i-raporty> (dostęp 31.1.2025).
[96] Zob. <https://uprp.gov.pl/pl/wyszukiwarki> (dostęp 31.1.2025). Jest on szczególnie istotny w wypadku znaków towarowych.
[97] Zob. <https://www.gunb.gov.pl/strona/rejestry-spisy-ewidencje> (dostęp 31.1.2025).
[98] Zob. <https://orzeczenia.ms.gov.pl> (dostęp 31.1.2025).
[99] Zob. <https://www.importyeti.com>, (dostęp 31.1.2025).
[100] Zob. <https://dane.gov.pl/pl/knowledgebase/useful-materials/trezor-api-interfejs-programistyczny-dla-systemu-trezor?lang=pl>, (dostęp 31.1.2025).
[101] Osoba fizyczna lub jej tożsamość użyta przez przestępców podczas dokonywania oszustw gospodarczych.

zgon. Wydawać by się mogło, iż korzystanie z wyszukiwarki grobów jest mało przydatne lub wręcz niecelowe, skoro na umieszczonej w wyszukiwarce fotografii nagrobka znajduje się część tych samych danych, co wyszukiwarce zgonów. Jednak ten drugi selektor oferuje wywiadowcy szereg informacji, których nie znajdzie on w wymienionej bazie: miejsce pochówku, informacje o innych osobach złożonych w tej samej mogile (z datami zgonów) czy nazwiska panieńskie. Mogą one pozwolić ustalić np. powinowactwo między figurantami bądź ich pochodzenie z jednej miejscowości. Zdjęcie nagrobka może także pozwolić na transformację i np. wyszukiwanie obrazem[102]. Analogicznie można postąpić w wypadku konfrontacji informacji np. z CEPiK z forami internetowymi miłośników tablic rejestracyjnych, gdy próbuje się odnaleźć selektor w postaci pojazdu

Osobną kategorią jest poszukiwanie informacji w mediach społecznościowych[103]. Wiele takich mediów domyślnie ustawia prywatność kont jako „publiczne", dlatego jeśli figurant nie zmieni tej opcji, będzie można go w nich znaleźć – z pomocą wyszukiwarki wewnętrznej bądź zewnętrznej[104]. Być może pozwoli to np. zidentyfikować figurantów i ustalić powiązania między nimi lub określić, że w momencie, gdy figurant przebywał na zwolnieniu lekarskim, odbywał zagraniczną wycieczkę. Bardziej zaawansowaną techniką jest wyszukiwanie obrazem na podstawie zdjęć figuranta umieszczonych w mediach społecznościowych: od prostej identyfikacji, gdzie dane zdjęcie zostało opublikowane[105], po wykorzystanie rozpoznawania twarzy do znalezienia innej fotografii tej osoby w Internecie[106]. Dzięki temu można natrafić np. na wspólne zdjęcie organizatora przetargu i jego zwycięzcy (np. na rybach, nartach itp.) co wskazuje, że znają się także prywatnie (co może mieć duże znaczenie w wypadku podejrzenia konfliktu interesów lub występowania zjawisk korupcjogennych).

Warto śledzić zwłaszcza narzędzia oparte na opisanych już algorytmach AI. Potrafią one rozpoznawać twarze i w niektórych sytuacjach rozpoznać nawet osobę znajdującą się na drugim planie fotografii. Jeśli chodzi o wyszukiwanie zdjęć, warto nadmienić, że – o ile osoba publikująca daną fotografię ich nie usunęła – zdjęcia cyfrowe opatrzone są metadanymi: informacjami o czasie wykonania fotografii, czasami miejscu, ale także numerze seryjnym aparatu. Dzięki nim, za pośrednictwem wyszukiwarki *Stolen Camera Finder*[107] – można próbować znaleźć inne zdjęcia wykonane tym aparatem.

---

[102] Por. wyżej.

[103] Wg niektórych źródeł poszukiwanie w nich informacji jest osobną kategorią wywiadu. Por. T. Turba: *SOCMINT – czyli OSINT mediów społecznościowych*, <https://sekurak.pl/socmint-czyli-osint-mediow-spolecznosciowych/>, (dostęp 31.1.2025).

[104] Warto wiedzieć, że np. portal LinkedIn jest indeksowany przez Google, a przeglądarka wewnątrz Facebooka ukrywa wpisy o negatywnym sentymencie (lepiej szukać takich w wyszukiwarkach zewnętrznych).

[105] Wyszukiwarki Google Image Search, TineEye i inne.

[106] Np. za pomocą narzędzia PimEyes.

[107] <https://www.stolencamerafinder.com>, (dostęp 31.1.2025).

OSINT jest dynamicznie rozwijającą się dziedziną ze względu na relatywnie niskie bariery wejścia i dużą ilość dostępnych potencjalnych źródeł informacji. Jednak, podobnie jak każda inna metoda pozyskiwania informacji, nie gwarantuje on uzyskania satysfakcjonujących rezultatów. Przedstawione wyżej rejestry danych (zwłaszcza te opisane jako mniej konwencjonalne) nie zawsze są kompletne. Celem tej części artykułu nie było wymienienie wszystkich istniejących i przydatnych w OSINT rejestrów, a potraktowanie ich jako ciekawych przykładów i tym samym wskazanie, że przydatna informacja może znajdować się w źródle nieoczywistym. Nie mniej ważne było również wskazanie, jak jeden selektor może prowadzić do kolejnego. Zobrazowano tu wykorzystanie poszczególnych typów źródeł informacji w tworzeniu łańcuchów selektorów i transformacji. Jak wskazano wyżej, OSINT jest zajęciem często trudnym i żmudnym, a poszukiwania mogą prowadzić (i nierzadko prowadzą) w ślepe zaułki. Jednakże świadomość, że istnieje wiele nieoczywistych źródeł informacji może pomóc znaleźć taką, która akurat jest istotna dla tego konkretnego postępowania albo wskaże nowy kierunek poszukiwań.

Dla audytora śledczego istotna jest zatem integracja danych, będąca pierwszym etapem procesu analitycznego, na którym zestawia się zróżnicowane rodzaje informacji pochodzących z różnych źródeł w celu ustalenia braków informacyjnych. Staranna integracja danych pozwala wskazać na luki w informacjach i słabe punkty w postępowaniu, gwarantując tym samym, że audytor będzie konsekwentnie gromadził informacje wywiadowcze, nawet w najwcześniejszym stadium analizy[108]. Umiejętne korzystanie ze źródeł otwartych pozwala na względnie tanie (aczkolwiek wymagające często znacznego nakładu czasu i pracy), gromadzenie informacji, a tym samym poszerzanie zasobu wiedzy przydatnej w wykrywaniu nadużyć.

Podsumowanie

Audyt śledczy jest procesem wymierzonym przeciwko różnym przejawom przestępczości gospodarczej, w tym oszustwom, korupcji oraz innym nadużyciom i przestępstwom finansowym. Jest niejako połączeniem metod pracy audytora wewnętrznego, biegłego rewidenta, zdobyczy kryminalistyki oraz warsztatu pracy śledczych. Taki audyt, jako działalność wykrywcza, wykorzystuje analizę śledczą, która łączy różnorodne metody i techniki przetwarzania, analizowania i interpretowania informacji dążąc do ustalania związków pomiędzy danymi o działalności przestępczej z innymi informacjami. Wykorzystywane są tu dane z wielu różnych źródeł. Powszechne obecnie rejestry elektroniczne, duże zbiory danych służące organizacjom do prowadzenia bieżącej działalności oraz algorytmy AI, stanowią ogromne wyzwanie w detekcji oszustw. Analityka wykorzystująca zbiory

[108] UNODC, *Analiza kryminalna*…, op.cit., s. 30.

big data „uzbroiła" audyt śledczy w narzędzia do wykrywania wzorców, anomalii w dużych zestawach danych. W artykule zaakcentowano, iż w opisywanym procesie, wybór źródeł pozyskiwania informacji[109] ma trudne do przecenienia znaczenie. Audytor śledczy powinien umieć korzystać ze wszystkich możliwych źródeł, tj. dobierać je raczej ze względu na ich przydatność w danym projekcie niż z uwagi na łatwość w uzyskaniu do nich dostępu.

W kontekście opisanego powyżej OSINT, warto jednak pamiętać, że z punktu widzenia skuteczności i przede wszystkim efektywności audytu śledczego, wykorzystanie źródeł otwartych zamiast uruchomienia kosztownych np. niejawnych aktywów, może znacząco zmniejszyć koszty gromadzenia materiału dowodowego. To z kolei pozwala uzyskać więcej informacji i zmieścić się w ustalonym budżecie. Wykorzystanie źródeł otwartych pomaga również chronić lub zachowywać źródła zamknięte bądź niejawne. Jednocześnie penetrowanie źródeł otwartych może oznaczać konieczność zmierzenia się z niezwykle dużymi wolumenami danych[110]. I w tym kontekście ujawnia się wzajemna zależność OSINT oraz zaprezentowanej w artykule zaawansowanej analizy dużych zbiorów danych z wykorzystaniem AI.

dr **WOJCIECH GOLEŃSKI**
doradca ekonomiczny,
Wydział Analiz Strategicznych
Departamentu Strategii NIK,
Instytut Ekonomii i Finansów
Uniwersytetu Opolskiego
ORCID: 0000-0001-8936-4510
dr **MARCIN BĘDZIESZAK**
główny specjalista k.p.,
Wydział Analiz Strategicznych
Departamentu Strategii NIK,
Instytut Ekonomii Politycznej,
Prawa i Polityki Gospodarczej
Szkoły Głównej Handlowej w Warszawie
ORCID: 0000-0003-3167-6356
dr **MACIEJ FOLTA**
specjalista k.p.,
Wydział Analiz Strategicznych
Departamentu Strategii NIK
ORCID: 0000-0002-1424-1580

Autorzy wyrazili w artykule własne poglądy, a nie instytucji, z którymi są związani.

[109] Zwykle wskazuje się, iż są to informacje: 1) ze źródeł otwartych; 2) ze źródeł zamkniętych; 3) ze źródeł niejawnych. Biorąc pod uwagę specyfikę pracy audytora śledczego, zwykle będzie on korzystać z dwóch pierwszych rodzajów źródeł. Źródła niejawne to dane zgromadzone operacyjnie przez specjalnie do tego celu przeznaczone niejawne środki, w tym tez wykorzystaniem osobowych źródeł informacji oraz techniki operacyjnej. Audytorzy śledczy w przeciwieństwie do funkcjonariuszy organów ścigania i służb specjalnych nie wykorzystują techniki operacyjnej w procesie zbierania i analizy informacji – zob. UNODC: *Analiza kryminalna*…, op.cit., s. 12.

[110] Tamże, s. 12.

Słowa kluczowe: audyt śledczy, zbiory danych, AI, podejrzenie oszustwa, przestępstwa gospodarcze, analiza danych

Bibliografia:

1. ACFE, *Occupational Fraud 2024: A Report to the Nations,* Austin 2024.
2. Amalina F., Hashem I.A.T., Azizul Z.H., Fong A.T., Firdaus A., Imran M., Anuar N.B.: *Blending big data analytics: Review on challenges and a recent study.* Ieee Access, 8/2019.
3. *Advanced methods of searching information*.
4. Baker R., Hoffman M.: *Prawdziwa głębia OSINT: odkryj wartość danych: open source intelligence*, Helion, Gliwice 2024.
5. Boersma M.: *(Data) science in financial audits*, „Compact Transparency of Information" nr 4/2018.
6. Cai C.W., Linnenluecke M.K., Marrone M., Singh A.K.: *Machine learning and expert judgement: analyzing emerging topics in accounting and finance research in the Asia–Pacific*, „Abacus" nr 4/2019.
7. Cressey D. R.: *Other People's Money. A study in Social Psychology of Embezzlement*, Free Press 1953.
8. Chang V.: *An ethical framework for big data and smart cities.* "Technological Forecasting and Social Change", 165/2021.
9. *Co to jest FTP?*, Pomoc home.pl, https://pomoc.home.pl/baza-wiedzy/co-to-jest-ftp.
10. *10 Python OSINT Tools for Investigating Disinformation and Extremism*, „Medium.com".
11. Dobrowolski Z., Kościelniak J.: *Audyt śledczy w spółkach Skarbu Państwa i spółkach komunalnych*, ISP UJ, Kraków 2018.
12. Dyjasz M.: *Analiza śledcza jako technika wsparcia audytu śledczego*, IIA Polska, prezentacja PowerPoint.
13. EY Academy of Business, *Audyt Śledczy*.
14. Fawcett T., Provost F.: *Adaptive fraud detection*, „Data mining and knowledge discovery" nr 1/1997.
15. Hardwick J., *Google Search Operators: The Complete List (44 Advanced Operators)*, „ahrefs.com".
16. Hilal W., Gadsden S.A., Yawney J.: *Financial fraud: a review of anomaly detection techniques and recent advances*, „Expert Systems with Applications" nr 193/2022.
17. Ignatczak W., Dyjasz M.: *Audyt śledczy – przetwarzanie informacji z wykorzystaniem metod i technik analizy śledczej*, PIKW, Warszawa 2019.
18. INTOSAI, *Guideline for the Audit of Corruption Prevention in Public Procurement,* Vienna 2022.
19. Jagiełło D.: *Taktyka kryminalistycznych czynności dowodowych*, CH. Beck, Warszawa 2019.
20. Kaczmarski M.: *Czym jest audyt śledczy i kiedy może się przydać?*
21. Karliński W.: *Metody i narzędzia wspomagania informatycznego kontroli stosowane w NIK* [w:] *Zastosowanie narzędzi wspomagania informatycznego kontroli (CAATs) w działalności kontrolnej i audytorskiej instytucji sektora publicznego w Polsce. Materiały z Konferencji*. Przegląd Metodyczny – numer specjalny, NIK, Warszawa, kwiecień 2016.
22. Karliński W.: *Metody analityczne w procesie kontrolnym,* „Kontrola Państwowa" nr 1/2024.
23. Kuhn M., Johnson K.: *Applied predictive modelling,* New York: Springer, Vol. 26/2013.

24. Kutera M.: *Rola audytu finansowego w wykrywaniu przestępstw gospodarczych*, Difin, Warszawa 2008.
25. Liu Y., Jia R., Ye J., Qu X.: *How machine learning informs ride-hailing services: A survey*. „Communications in Transportation Research" nr 2/2022.
26. Łużak T., „OSINT, czyli biały wywiad – co to jest?", Biznes Netia.pl, 16 maja 2024.
27. Maltego, *Understanding the Different Types of Intelligence Collection Disciplines*, Maltego Blog, 27 października 2022.
28. Martysz C., Walczak K.: *Zarys problematyki przeciwdziałania przestępstwom gospodarczym i ich wykrywania*, [w:] *XXV lat w naukach ekonomicznych: dokonania, wyzwania, perspektywy*. R. Bartkowiak, M. Matusiewicz (red.), Warszawa 2018.
29. Mazririri T.: *Forensic Auditing: A Guide for Practitioners*, Amazon 2021.
30. Munne R. (2016), *Big Data in the Public Sector* [w:] *New Horizons for a Data-Driven Economy A Roadmap for Usage and Exploitation of Big Data in Europe*, ed. J.M. Cavanillas, E. Curry, W. Wahlster, Springer.
31. Naqvi A.: *Artificial intelligence for audit, forensic accounting, and valuation: a strategic perspective*. John Wiley & Sons 2020.
32. NoBookkeeper194, "Python OSINT scripts" [w:] *Reddit*, r/OSINT, 2023, www.reddit.com/r/OSINT/comments/17x0qkl/python_osint_scripts/. [dostęp: 31.01.2025].
33. Nowak A.: *Identyfikacja przyczyn i sprawców oszustw finansowo-księgowych – ujęcie statystyczne*, Zeszyty Naukowe UŚ, nr 765 Finanse, Rynki Finansowe, Ubezpieczenia nr 61 (2013).
34. OECD: *Anti-Corruption and Integrity Outlook 2024*, Paris 2024.
35. Oladejo M.T., Jack L.: *Fraud prevention and detection in a blockchain technology environment: challenges posed to forensic accountants*. "International Journal of Economics and Accounting", 9(4)2020.
36. Ostrowska P.: *Problematyka rachunkowości kreatywnej, agresywnej i audytu śledczego w świetle opinii księgowych*, *„Academic Review of Business and Economics"* Vol. 2(1)2022.
37. Piaszczyk A.: Audyt śledczy, ECE Prestiż, Lublin 2009.
38. Proczek M., Szczepańska P.: *Nadużycia i przestępstwa finansowe a działalność Europejskiego Urzędu ds. Zwalczania Nadużyć Finansowych*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach" 319/2017.
39. *Sieć peer to peer (P2P) – co to jest?*, blog Netia.pl, 08 lipca 2021, https://www.netia.pl/pl/blog/siec-peer-to-peer-p2p-co-to-jest [dostęp: 31.01.2025].
40. SJP: *Indeksowanie*, https://sjp.pwn.pl/slowniki/indeksowanie.html [dostęp 3 lutego 2025 r.].
41. Soltani M., Kythreotis A., Roshanpoor A.: *Two decades of financial statement fraud detection literature review; combination of bibliometric analysis and topic modelling approach*. "Journal of Financial Crime" 2022.
42. Tiron-Tudor A., Donțu A.N., Bresfelean V.P.: *Emerging technologies' contribution to the digital transformation in accountancy firms*. Electronics, 11(22)/2022.
43. Titera W.R.: *Updating Audit Standard-Enabling Audit Data Analysis*. „Journal of Information Systems", vol. 27, no. 1, Spring 2013.

44. Turba T., *SOCMINT - czyli OSINT mediów społecznościowych*, *„Sekurak.pl"*, 14 września 2022, https://sekurak.pl/socmint-czyli-osint-mediow-spolecznosciowych/.
45. UNODC: *Analiza kryminalna. Podręcznik dla analityków*, CBA, Warszawa 2020.
46. *Use of big data and AI in fighting corruption and misuse of public funds. Good practice, ways forward and how to integrate new technology into contemporary control framework*, organized by the Policy Department on Budgetary Affairs for the Committee on Budgetary Control, European Parliament 2021 https://ec.europa.eu/social/BlobServlet?docId=14836&langId=pl.
47. van Veenstra A.F., Grommé F., Djafari S.: *The use of public sector data analytics in the Netherlands*, Transforming Government: People, Process and Policy, Vol. 15 No. 4/2021.
48. Wells J. T.: *Nadużycia w firmach. Vademecum. Zapobieganie i wykrywanie*, LexisNexis, E&Y, Warszawa 2006
49. Wieczorkowski J.: *Wykorzystanie koncepcji big data w administracji publicznej*. „Roczniki Kolegium Analiz Ekonomicznych/SGH", Technologie informatyczne w administracji publicznej, nr 33/2014.

Netografia rejestrów:

1. Repozytorium Akt Rejestrowych Krajowego Rejestru Sądowego, https://rar.ms.gov.pl.
2. Elektroniczne Księgi Wieczyste, https://ekw.ms.gov.pl/eukw_ogol/menu.do.
3. E-uropean Justice, https://e-justice.europa.eu/home?action=home&plang=pl.
4. Strona Urzędu Ochrony Konkurencji i Konsumenta, https://uokik.gov.pl/bip/rejestry-i-raporty.
5. Strona Urzędu Patentowego RP, https://uprp.gov.pl/pl/wyszukiwarki.
6. Strona Głównego Urzędu Nadzoru Budowlanego, https://www.gunb.gov.pl/strona/rejestry-spisy-ewidencje.
7. Portal Orzeczeń Sądów Powszechnych, https://orzeczenia.ms.gov.pl.
8. Import Yeti, https://www.importyeti.com.
9. https://dane.gov.pl/pl/knowledgebase/useful-materials/trezor-api-interfejs-programistyczny-dla-systemu-trezor?lang=pl.
10. https://www.stolencamerafinder.com.

ABSTRACT

Big Data, AI and Open Data Sources – Tools Used in Forensic Audit

The purpose of forensic (investigation) audit is to counteract various types of economic crime, especially to identify fraud and corruption, as well as misappropriation and other financial crime. To this end, not only financial audit methods are used, but forensic ones as well, since financial audit methods do not always identify economic fraud, which comprises all activities against the rules of the economy. These include

both misappropriation and activities of organised crime groups. Most common economic fraud types comprise money laundering, accounting fraud, corruption, bid rigging and cybercrime. Forensic audit is mainly focused on identification of misappropriation and fraud. An understanding of the nature of these processes is very important for distinguishing forensic audit from other ways of evaluation of an organisation's functioning. In accordance with Article 286 of the Criminal Code, a fraud is activity aimed at obtaining material benefits by making another person mismanage their or other people's property, or by making use of another person's mistake, or their inability to properly understand their activities. While misappropriation is defined in Article 296 of the Criminal Code, and the perpetrator is a person that – on the basis of legal provisions, decisions by competent authorities, or an agreement to deal with assets of a natural or legal person, or of an organisational entity – deliberately acts to obtain material benefits by abusing their rights, or by neglecting their responsibilities. In their article, the authors present the most important features of forensic audit. At the beginning, they focus on several key issues, e.g. the nature of forensic audit, the basic features of misappropriation, and the main elements of forensic analysis. Later, they discuss selected features of big data, as well as their potential and actual application in forensic audit, next to potential use of artificial intelligence. Several techniques of obtaining information from open data sources and of using this strategy in auditing have been presented.

Wojciech Goleński, PhD, economic advisor, Unit of Strategic Analyses, Department of Strategy of NIK, Institute of Economy and Finance of the University in Opole, ORCID: 0000-0001-8936-4510,
Marcin Będzieszak, PhD, senior public audit expert, Unit of Strategic Analyses, Department of Strategy of NIK, Warsaw School of Economics, Institute of Political Economy, Law and Economic Policy, ORCID: 0000-0003-3167-6356
Maciej Folta, PhD, public audit expert, Unit of Strategic Analyses, Department of Strategy of NIK, ORCID: 0000-0002-1424-1580

Key words: forensic audit, big data, AI, suspected fraud, economic fraud, data analysis