Piotr Karasek

RÓŻNORODNOŚĆ MODELI POZYSKIWANIA DOWODÓW CYFROWYCH – PERSPEKTYWA BADAWCZA

The variety of digital forensic investigation models – research perspective

Naturalną konsekwencją dynamicznego rozwoju technologii komputerowej oraz jej upowszechnienia się w społeczeństwie jest wkroczenie także do prawnie relewantnych sfer życia. Niestety, współczesne rozwiązania technologiczne służą – pośrednio lub bezpośrednio – także popełnianiu przestępstw. Z tego powodu w sądach w XXI wieku pojawił się nowy rodzaj materiału dowodowego – dowód cyfrowy. Prawidłowe wykorzystanie cyfrowego materiału dowodowego w postępowaniu sądowym – szczególnie w postępowaniu karnym – wymaga pozyskania[1] takiego materiału dowodowego w sposób merytorycznie prawidłowy, zgodny z zasadami nauki informatyki w tym zakresie. Pomimo że informatyka kryminalistyczna jest bardzo młodą dziedziną, w ciągu ostatnich dwudziestu lat powstało wiele modeli procedur postępowania z dowodami cyfrowymi – żaden jednak nie uzyskał uniwersalnej akceptacji. Żaden też nie został dostosowany do potrzeb polskich organów ścigania i nie ma mocy obowiązującej. Brak formalnej metodyki pozyskiwania dowodów cyfrowych nie sprzyja prawidłowej pracy wymiaru sprawiedliwości. Celem niniejszego artykułu jest więc przybliżenie pojęcia „informatyki kryminalistycznej" jako dziedziny nauki kryminalistyki oraz jej „zasad podstawowych" i zwrócenie uwagi na problem dużej różnorodności proponowanych procedur postępowania z cyfrowym materiałem dowodowym. Jednoczenie autor wskazuje kierunek dalszych działań badawczych, które zamierza podjąć, aby sformułować ujednolicony model postępowania z dowodami cyfrowymi w warunkach polskiego procesu karnego.

Wstępem do dalszych rozważań powinno być jednak krótkie objaśnienie istoty cyfrowego materiału dowodowego oraz związanego z nim pojęcia „przestępczości komputerowej". Obecnie ten ostatni termin wydaje się najbardziej upowszechniony w odniesieniu do przestępstw powiązanych z wykorzystaniem technologii komputerowych, choć w przeszłości wykorzystywano też termin „cyberprzestępczość"

[1] Przez „pozyskanie" dowodu cyfrowego rozumiany będzie całokształt procesu dążącego do jego wykorzystania przez sąd, a więc nie tylko procesowe zabezpieczenie dowodu, lecz także jego analiza przez biegłego czy późniejsza prezentacja w sądzie.

– na ogół na określenie tego samego zjawiska[2]. Omijając jednak historyczne aspekty prób konstruowania definicji przestępstw komputerowych, dla rozważań na gruncie kryminalistyki przydatne i rozsądne wydaje się przywołanie definicji klasyfikacyjnej przygotowanej przez A. Adamskiego. Wyróżnił on przestępczość komputerową w sensie materialnym oraz procesowym[3]. Materialnokarnie rozumiana przestępczość komputerowa obejmuje zarówno przestępstwa *„stricte* komputerowe" (np. włamanie do systemu komputerowego, „ataki hakerskie") jak i przestępstwa, których celem jest naruszenie dóbr tradycyjnie chronionych przez prawo karne, a popełnione z wykorzystaniem komputera (np. oszustwo za pośrednictwem Internetu czy naruszenie praw autorskich). Jeszcze szersze, i najistotniejsze z kryminalistycznego punktu widzenia, jest karnoprocesowe rozumienie przestępczości komputerowej: każde działanie sprawcy przestępstwa, jego pomocnika, czy nawet świadka biorącego mimowolny udział w zdarzeniu, polegające na wykorzystaniu sprzętu komputerowego w związku z przestępstwem, pozostawia w ramach urządzenia komputerowego cyfrowe ślady działalności, mogące stać się dowodami w sprawie. Działanie tych osób może polegać na przechowywaniu nielegalnego pliku, wysłaniu wiadomości elektronicznej o określonej treści czy wyszukiwaniu określonych fraz w Internecie. Wszelkie ślady tych działań mogą być przydatne w postępowaniu karnym w charakterze dowodów.

Pojęcie „dowodu cyfrowego" nie zostało formalnie zdefiniowane na gruncie ustawy procesowej (podobnie jak wiele innych rodzajów materiału dowodowego). W świetle przepisów procesu karnego cyfrowy materiał dowodowy należy do otwartego katalogu dowodów „rzeczowych" (pomimo że ma on zarazem zestaw cech odróżniających go od innych rodzajów materiału dowodowego, a jego fizycznie materialna forma jest trudna do uchwycenia)[4]. Zdefiniowanie „dowodu cyfrowego" w literaturze również nie było proste i istnieje przynajmniej kilka propozycji redakcyjnych w tym zakresie. Na potrzeby niniejszego opracowania możliwe jest jednak skonstruowanie następującej, syntetycznej definicji „dowodu cyfrowego": są to informacje o znaczeniu dowodowym, które mają formę danych cyfrowych[5]. Zatem *dowodem* w postępowaniu jest *informacja* uzyskana na podstawie *danych* w *formie*

[2] Niektórzy autorzy postulowali, że pojęcia „cyberprzestępczości" i „przestępczości komputerowej" nie są ze sobą tożsame, gdyż pierwsze z nich jest znacznie szersze od drugiego. Wydaje się jednak, że podział ten nie ma znaczenia w praktyce, a terminy te wykorzystywane są zamiennie. Por.: A. Lach, *Dowody elektroniczne w procesie karnym*, Dom Organizatora, Toruń 2004, s. 12, za: E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*, Academic Press, Amsterdam–London–New York 2000, s. 8–9.

[3] A. Adamski, *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000, s. 30–34.

[4] W ten sposób ujmują to m.in.: M. Niebrzydowska, R. Kotowicz, *Wstęp do informatyki śledczej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 6 (4), s. 61; A. Lach, op. cit., s. 32, P. Krejza, *Najlepsze praktyki w poszukiwaniu i zabezpieczaniu dowodów elektronicznych*, w: M. Szmit (red.), *Elementy informatyki sądowej*, Polskie Towarzystwo Informatyczne, Warszawa 2011, s. 43.

[5] W podobny sposób określają to m.in.: A. Lach, op. cit., s. 28; B. Perrin, M. Remy, R. Rouloaty, *Electronic evidence in Swiss criminal procedure*, „Digital Evidence and Electronic Signature Law Review" 2011, t. 8, s. 72.

cyfrowej (o dowodowym znaczeniu dla postępowania). Niezwykle istotne jest przy tym, aby pamiętać, że informacja znajdująca się w zainteresowaniu organów procesowych, konkretne dane cyfrowe, istnieje zawsze niezależnie od jej mechanicznego nośnika (a więc dysku twardego, SSD, płyty CD/DVD czy też pamięci przenośnej). Te stanowią bowiem jedynie przestrzeń przechowywania materiału dowodowego i same w sobie na ogół nie mają takiego znaczenia – zwłaszcza w kontekście faktu, że dane cyfrowe ze swojej natury pozwalają na ich bezstratne kopiowanie i przenoszenie w niezmienionej formie. Tym samym w ich przypadku zaciera się różnica między „kopią" a „oryginałem" dowodu[6].

Warto pamiętać, że kategoria dowodów cyfrowych jest niezwykle szeroka pod względem treściowym – dowodem mogą być pliki wygenerowane przez człowieka (zdjęcia, SMS-y, dokumenty tekstowe, e-maile itp.), jak i stworzone przez system, bez świadomego udziału człowieka (np. rejestry systemowe, przechowywane czasy dostępu do plików itp.). Współcześnie należy brać pod uwagę cyfrowy materiał dowodowy pochodzący nie tylko z komputerów osobistych, lecz także ze wszelkiego rodzaju innych urządzeń: tabletów, telefonów, bezzałogowych obiektów latających („dronów"). Trzeba też mieć świadomość, że współcześnie prawnie relewantne treści mogą, lecz nie muszą znajdować się bezpośrednio w urządzeniu – mogą być przechowywane także w tzw. chmurze. Niemniej jednak wszystkie informacje znajdujące się w danym urządzeniu elektronicznym mogą, w pewnych okolicznościach, mieć znaczenie dla postępowania karnego. Obecnie dość standardowo przedstawianym w sądach dowodem (także w mniej „poważnych" sprawach karnych, w sprawach cywilnych) są na przykład treści e-maili czy SMS-ów, choć wydaje się, że często nie są one prezentowane w sposób zgodny z wymogami nauki, gwarantującymi wiarygodność i autentyczność takich dowodów[7].

Jednym z najpoważniejszych wyzwań związanych z cyfrowym materiałem dowodowym jest łatwość dokonania zamierzonej lub przypadkowej modyfikacji danych cyfrowych (także przez funkcjonariuszy organów ścigania). Rzeczywiście, dane informatyczne stosunkowo łatwo poddają się zmianom. Możliwe jest też dokonanie tego w taki sposób, ażeby wykrycie wprowadzonych modyfikacji było praktycznie niemożliwe[8]. Nie trzeba zresztą posiadać specjalistycznej wiedzy, by zauważyć, że materiał cyfrowy poddaje się modyfikacji znacznie łatwiej niż materialne źródła

[6] Zob.: P. Karasek, *Gdy dowodem są dane – czyli prawdy i mity związane z pozyskiwaniem dowodów cyfrowych*, „Edukacja Prawnicza" 2015, nr 2, s. x.

[7] Treść korespondencji częstokroć dostarczana jest do sądu w formie prostych wydruków, co nie pozwala na weryfikację rzeczywistego pochodzenia plików. Anegdotyczną wartość przedstawiają sytuacje, w których przedstawiane wydruki komputerowe prezentowane są wraz z notarialnym poświadczeniem za zgodność z oryginałem. We wszystkich takich przypadkach dowód przedstawia – z kryminalistycznego punktu widzenia – mierną wartość, jednakże często dowody takie po prostu nie są kontestowane przez drugą stronę procesu, w związku z czym wydruk jest wystarczający.

[8] P. Krejza, op. cit., s. 43, oraz M. Niebrzydowska, R. Kotowicz, op. cit., s. 64.

dowodowe[9]. W głównej mierze to właśnie z tą cechą wiąże się konieczność zachowania ścisłych zasad przy zabezpieczaniu i analizie dowodów cyfrowych. W wypadku nieumiejętnego podjęcia tych czynności może bowiem dojść do kontaminacji materiału dowodowego, co z kolei może poskutkować całkowitą utratą jego wartości. Na znaczenie prawidłowego zabezpieczania, a także prawidłowej analizy dowodów cyfrowych zwrócił już uwagę Sąd Najwyższy w orzeczeniu z dnia 20 czerwca 2013 r. (III KK 12/13), w którym stwierdza, że: „dane informatyczne muszą być analizowane w sposób nadzwyczaj dokładny oraz przy użyciu najaktualniejszej wiedzy”[10]. W praktyce będzie to miało tym większe znaczenie, im bardziej dany materiał jest kwestionowany przez drugą ze stron procesu.

Ustaleniem prawidłowych metod obchodzenia się z dowodami cyfrowymi zajmuje się informatyka kryminalistyczna[11]. Jest to bardzo młoda dziedzina, nawet w porównaniu z samą współczesną nauką kryminalistyki, rozwijaną przecież dopiero od końca XIX i początku XX wieku. Termin „informatyka kryminalistyczna” pierwszy raz pojawił się w piśmiennictwie polskim w 1996 roku[12], a jej historia sięga lat osiemdziesiątych XX wieku[13]. W ciągu ostatnich dwóch dekad nastąpił istotny wzrost jej znaczenia wywołany szybkim rozwojem technologii komputerowych i częstszym występowaniem dowodów cyfrowych w postępowaniu sądowym. W kontekście omawianej problematyki właściwą definicją informatyki kryminalistycznej wydaje się ta przedstawiająca ją jako: „wykorzystanie naukowo wypracowanych metod w dążeniu do zabezpieczenia, uwierzytelnienia, udokumentowania i zaprezentowania dowodów cyfrowych pozyskanych z urządzeń cyfrowych, dla celów umożliwienia lub ułatwienia rekonstrukcji zdarzenia o charakterze kryminalnym”[14].

---

[9] R.L. Kodner, *Manipulated digital evidence: how to spot it?*, „Family Advocate” 2005–2006, t. 28 (16), s. 16.

[10] Wyrok Sądu Najwyższego z dnia 20 czerwca 2013 r., sygn. III KK 12/13, „Biuletyn Prawa Karnego” nr 8/13, s. 11.

[11] Na określenie tej dziedziny kryminalistyki wykorzystywane są naprzemiennie różne terminy. Trudno jest bowiem ustalić jedną, odpowiadającą wszystkim wersję tłumaczenia jej nazwy z języka angielskiego, zwłaszcza że nawet w ramach języka oryginalnego nie ma jednolitości terminologicznej (między innymi wykorzystuje się pojęcia takie jak: *computer forensics*, *digital forensics*, *forensic IT*). Termin „informatyka kryminalistyczna” wydaje się obejmować szersze pole badawcze niż np. „informatyka śledcza”, a jednocześnie lepiej pasować do polskich realiów językowych niż „kryminalistyka komputerowa”. Warto przy tym zwrócić uwagę na propozycję dr. M. Szmita, by posługiwać się terminem „informatyka sądowa”, zob.: M. Szmit, op. cit., s. 25–26.

[12] Termin ten został użyty w książce: Z. Czeczot, T. Tomaszewski, *Kryminalistyka ogólna*, Comer, Toruń 1996, s. 432–438, informacja podana za: E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 556.

[13] A. Agarwal, M. Gupta, S. Gupta, S.C. Gupta, *Systematic digital forensic investigation model*, International „Journal of Computer Science and Security” 2011, t. 5 (1), s. 118.

[14] Definicję tę skonstruowano w podczas zorganizowanego w tym celu panelu dyskusyjnego w ramach Digital Forensic Workshop w 2001 r. Zob.: R. Kaur, A. Kaur, *Digital forensics*,

Czynnościami przeprowadzanymi w ramach tej dziedziny rządzi szereg naczelnych reguł, które przedstawiane są najczęściej w formie „zasad podstawowych", „dyrektyw" czy „najlepszych praktyk". Nie istnieje jednak ich uniwersalna redakcja. W zależności od autora danego zestawienia różna jest liczba proponowanych zasad i ich szczegóły. W 1999 r. R. McKimmish wyodrębnił cztery takie zasady. Jego zestawienie obejmowało: po pierwsze, nadrzędny nakaz unikania korzystania w badaniach informatycznych z pierwotnego nośnika danych (np. dysku twardego zabezpieczonego u podejrzanego) w celu uniknięcia modyfikacji materiału. Po drugie, nakaz szczegółowego opisania i uzasadnienia wszystkich zmian wprowadzonych pomimo zasady pierwszej (czasami jest to bowiem niezbędne). Po trzecie, nakaz przestrzegania reguł prawa dowodowego obowiązującego w danym kraju. Ostatnia zasada przewidywała nakaz posiadania odpowiednich kwalifikacji przez osobę zajmującą się zabezpieczeniem i analizą dowodów[15].

Z kolei W.G. Kruse i J.G. Heiser w 2002 r. sformułowali jedynie trzy zasady podstawowe, które określili mianem trzech „A" (od ang. *Acquire*, *Authenticate*, *Analyze)*. Pierwsza z nich nakazuje pozyskanie (*Acquire*) dowodów cyfrowych bez modyfikacji czy uszkodzenia materiału źródłowego. Druga nakazuje uwierzytelnienie (*Authenticate*) pozyskanych kopii danych w taki sposób, by móc wykazać, że pochodzą one z pierwotnego ich nośnika. Trzecia zasada dotyczy analizy (*Analyze*) danych dowodowych, która ma być dokonywana tak, by zawsze dysponować „nienaruszoną" kopią oryginalnego materiału. Autorzy podkreślają przy tym, że to, jakie czynności zostaną przeprowadzone, zawsze będzie zależeć od konkretnych okoliczności i celów danego postępowania, jednakże za każdym razem powinny być one zgodne ze sformułowanymi powyżej zasadami[16].

W polskiej literaturze przedmiotu przywołuje się zazwyczaj „zasady naczelne informatyki śledczej" sformułowane przez A. Lacha. Zredagował on ich aż dwanaście, przy czym w zakresie merytorycznym nie odbiegają one od treści „zasad podstawowych" formułowanych przez pozostałych autorów[17].

Sens podstawowych zasad informatyki kryminalistycznej, pomimo różnic w ich redakcji, w zasadzie się nie zmienia. Poza wspomnianymi powyżej istnieje jeszcze szereg innych propozycji. Różnice dotyczą jednak liczby i brzmienia zasad, a ich treść jest niezwykle do siebie zbliżona: należy dążyć do zabezpieczenia danych

„International Journal of Computer Applications" 2012, t. 50, nr 5, s. 5, za: G.L. Palmer, *A road map for digital forensic research*, Technical Report DTR-T0010-01 for the First Digital Forensic Research Workshop 2001.

[15] Zob.: R. McKimmish, *What is Forensic Computing?*, Australian Institute of Criminology, Canberra 1999, http://aic.gov.au/documents/9/C/A/%7B9CA41AE8-EADB-4BBF--9894-64E0DF87BDF7%7Dti118.pdf (dostęp 28.04.2016), s. 3–4.

[16] Zob.: W.G. Kruse II, J.G. Heiser, *Computer Forensics: Incident Response Essentials*, Addison-Wesley, New York 2002.

[17] Zob. opracowane przez A. Lacha *Zasady Naczelne Informatyki Śledczej*, przedstawione na stronie internetowej: http://www.siis.org.pl/najlepsze-praktyki/zasady-naczelne.html (dostęp 26.04.2016).

materiału cyfrowego w taki sposób, by nie dokonać w nim żadnych modyfikacji, wszelkich czynności analitycznych należy dokonywać na jego uwierzytelnionej kopii oraz prowadzić szczegółową dokumentację wszystkich czynności. To założenie stanowi wspólny grunt dla wszystkich opublikowanych dotychczas procedur pozyskania dowodów cyfrowych dla celów postępowania karnego[18]. W ocenie autora jedną z lepszych propozycji stanowi ta wyżej wskazana, sformułowana przez W.G. Kruse'a i J.G. Heisera – ze względu na jej wyczerpujący, a jednocześnie łatwy do zapamiętania charakter.

Generalnie sformułowane zasady podstawowe informatyki kryminalistycznej pomimo swojej różnorodności mają raczej niekontrowersyjny charakter. Uzgodnienie szczegółowej i jednolitej metodyki postępowania z dowodem cyfrowym jest już bardziej problematyczne. Ogólnie warto wskazać, że istnienie naukowo „prawidłowej" procedury zabezpieczania i analizy dowodów jest niezwykle korzystne dla szeroko rozumianego dobra wymiaru sprawiedliwości. W Polsce aktualnie nie obowiązują jednak żadne wiążące na gruncie prawnym procedury pozyskiwania dowodów cyfrowych. Sąd oceniając ich wiarygodność, trzeba zdawać się w ich ocenie na wskazania osób o domniemanych kompetencjach. Brak jest jednak rzetelnego wzorca kontroli prawidłowości zabezpieczenia takich dowodów. W dorobku informatyki kryminalistycznej istnieją natomiast rozmaite propozycje procedur i standardów postępowania. Są to modelowe procedury opracowane przez różne (zwłaszcza zagraniczne) instytucje, zespoły badawcze i pojedyncze osoby zajmujące się tą problematyką[19]. W perspektywie międzynarodowej sformułowano dotychczas bardzo wiele modeli szczegółowo opisujących prawidłową organizację i kolejność czynności służących zabezpieczeniu i wykorzystaniu w sądzie dowodów cyfrowych. Żaden spośród nich nie uzyskał jednak powszechnej akceptacji wśród praktyków. Przyczyną takiego stanu rzeczy może być to, że żadna z nich nie jest prawdziwie uniwersalna. Poszczególne są zwykle projektowane z myślą o ich zastosowaniach w konkretnych okolicznościach – na przykład na potrzeby służb policyjnych w danym kraju, z myślą o postępowaniach w sprawie wybranych czynów zabronionych, czy też tworzone są dla celów „prywatnych śledztw" w międzynarodowych korporacjach[20]. Różnice w publikowanych na przestrzeni lat metodykach postępowania mogą wynikać także z potrzeby uwzględnienia w nowszych opracowaniach zmieniających się przyzwyczajeń użytkowników sprzętu elektronicznego, wynikających m.in. z ciągłego rozwoju technologii informatycznej (np. wejścia do powszechnego użytku smartfonów czy tabletów). Niektóre z procedur obejmują szczegółowo tylko niektóre czynności, np. zabezpieczenie lub analizę dowodów cyfrowych, pomijając inne. Niekiedy są to procedury skupiające się na zabezpieczeniu sprzętu komputerowego w całości, a niekiedy w ogóle niebiorące pod uwagę takiego scenariusza. Wreszcie utworzenie jednolitej i uniwersalnej pro-

[18] R. McKemmish, op. cit., s. 3.
[19] P. Olber, *Polskie procedury vs Międzynarodowe standardy zabezpieczania dowodów cyfrowych*, „Magazyn Informatyki Śledczej i Bezpieczeństwa IT" 2010, nr 8, s. 3.
[20] R.B. Adams, *The Advanced Data Acquisition Model (ADAM): A Process Model for Digital Forensic Practice*, Murdoch University, Perth 2012, s. 29–30.

cedury postępowania jest trudne ze względu na ogromną różnorodność potencjalnie przydatnych materiałów cyfrowych.

Co istotne, większość proponowanych modeli procedur była tworzona na podstawie zbliżonych założeń. Od strony merytorycznej techniki kryminalistycznego zabezpieczania dowodów cyfrowych pozostają zwykle takie same, gdyż wynikają one z aktualnych realiów technologicznych. Zasadniczo wszyscy autorzy kierują się tymi samymi założeniami, wynikającymi z naczelnych zasad informatyki kryminalistycznej. Istnieje jednak około kilkudziesięciu różnych „modelowych procedur postępowania" (o różnym stopniu szczegółowości i skomplikowania). Wstępna analiza szeregu z nich wydaje się wskazywać, że większość różnic pomiędzy nimi dotyczy raczej kwestii taktycznych, prawnych lub organizacyjnych. Merytoryczne i techniczne elementy zagadnień informatyczno-kryminalistycznych są oczywiście niezwykle istotne (także badawczo), jednakże w ramach niniejszego opracowania autor pragnie zwrócić uwagę zwłaszcza na taktyczne aspekty różnorodności współistniejących modeli procedur pozyskiwania dowodów cyfrowych.

Najłatwiej dostrzegalnym efektem różnic pomiędzy poszczególnymi wersjami procedur jest ich podział na kolejne taktyczne „etapy" (bądź „fazy") pozyskiwania dowodu. Autorzy niektórych modeli skupiają się jedynie na pewnych wycinkach koniecznych do przeprowadzenia działań, inni zaś starali się opisać kompletny proces pozyskiwania dowodu. Podział na poszczególne etapy oraz nazwy nadawane im w różnych modelach postępowań są zewnętrznym wyrazem ich wewnętrznych różnic.

Przykładowo więc autorzy procedury nazwanej *Systematic Digital Forensic Investigation Model* (SDRFIM) wyróżnili aż 11 szczegółowych, następujących po sobie faz postępowania: przygotowania, zabezpieczenia miejsca zdarzenia, wstępnej oceny sytuacji, udokumentowania miejsca zdarzenia, odcięcia komunikacji[21], zebrania dowodów cyfrowych, zabezpieczenia ich[22], analizy wstępnej, analizy właściwej, prezentacji i oceny następczej[23].

Nadawanie poszczególnym kolejnym czynnościom koniecznym dla prawidłowego pozyskania dowodu cyfrowego rangi taktycznych „etapów" nie sprzyja jednak przejrzystości procedur. Wielu autorów stara się więc wyróżnić mniejszą ich liczbę, niekiedy kosztem kompletności procedury. W poradniku Departamentu

[21] Autorzy zwracają uwagę, że zwłaszcza urządzenia mogą zostać przejęte przez policję w trakcie przesyłania/odbierania danych (przewodowo lub bezprzewodowo), co może doprowadzić do zajęcia pamięci nośnika nowymi danymi i zarazem zniszczenia części dowodów. Posługują się pojęciem *communication shielding*, zalecając pozbawienie urządzeń możliwości transferu danych (m.in. przez odłączenie urządzeń mobilnych od stacji dokujących – jest to praktyka wysoce kontrowersyjna w świetle innych opracowań). Zob.: A. Agarwal, M. Gupta, S. Gupta, S.C. Gupta, op. cit., s. 125.

[22] Rozróżniono tu zebranie dowodów (*evidence collection*) oraz ich zabezpieczenie (*evidence preservation*), obejmujące przygotowanie zebranego materiału do transportu (m.in. dokumentacja, metryczki, prawidłowe opakowanie nośników). Zob. tamże, s. 126.

[23] Tamże, s. 124–127.

Sprawiedliwości Stanów Zjednoczonych zostały opisane etapy: przygotowania, oceny miejsca zdarzenia, udokumentowania miejsca zdarzenia, zabezpieczania dowodów i oraz ich transportu[24]. W ogóle nie wzięto więc pod uwagę tego, co dzieje się z dowodem cyfrowym po jego zabezpieczeniu. Podobnych, mniej rozbudowanych modeli jest oczywiście więcej. Autor *Advanced Data Acquisition Model* (ADAM) wyróżnił jedynie etapy: planowania wstępnego, ponownego planowania (już na miejscu zdarzenia) i zabezpieczenia danych[25], z kolei W.G. Kruse i J.G. Heiser proponują wyróżnienie etapów: pozyskania, uwierzytelnienia i analizy materiału cyfrowego[26], w zasadzie omijając często opisywany etap planowania czynności.

Możliwe jest przywołanie i streszczenie wielu kolejnych przykładowych procedur pozyskiwania dowodu cyfrowego. W poniższej tabeli zaprezentowano zestawienie kilkunastu modeli, ze wskazaniem liczby „etapów" uwzględnionych w każdym z nich. Zestawienie to ma na celu uwidocznienie mnogości procedur i skali różnic pomiędzy nimi w zakresie proponowanej w nich taktyki działania.

Tab. 1. Modele procedur pozyskiwania dowodu cyfrowego

Lp.	Procedura (akronim/data powstania)	Liczba etapów
1	Computer Forensic Investigative Process[1] (1984)	4
2	DFRWS[2] (2001)	6
3	Systematic Digital Forensic Investigation Model[3] (SRDFIM 2011)	11
4	Abstract Digital Forensic Model[4] (ADFM 2002)	9
5	Integrated Digital Investigation Process[5] (IDIP 2003)	5
7	Enhanced Digital Investigation Process Model[6] (EDIP 2004)	5
8	Computer Forensics Field Triage Process Model[7] (CFFTPM 2006)	6
9	Digital Forensic Model based on Malaysian Investigation Process[8] (DFMMIP 2009)	7
10	Extended Model of Cybercrime Investigation[9] (2004)	13

[24] Podręcznik ten został napisany z myślą o „pierwszych na miejscu zdarzenia" funkcjonariuszach policji. Z tego względu pominięto w nim etapy analizy zebranego materiału czy późniejszej prezentacji dowodu. Por. M.B. Mukasey, J.L. Sedgwick, D.W. Hagy, *Electronic Crime Scene Investigation: A Guide for First Responders*, U.S. Department of Justice, Office of Justice Programs, Washington DC 2008, s. 13, 15, 19, 21, 31.

[25] Również w tym wypadku proponowany model procedur nie obejmuje tego, co dzieje się z materiałem dowodowym po jego zabezpieczeniu (tj. etapów związanych z jego analizą i prezentacją). Zob.: R.B. Adams, op. cit., s. 229–231.

[26] Zob.: S. Perumal, *Digital forensic model based on Malaysian investigation proces*s, „International Journal of Computer Science and Network Security" 2009, t. 9, nr 8, s. 38.

11	Dual Data Analysis Proces[10] (2007)	4
12	Advanced Data Acquisition Model[11] (ADAM 2012)	3
13	A Control Framework for Digital Evidence[12] (2006)	4
14	Good Practice Guide for Digital Evidence[13] (2012)	4
15	Framework For a Digital Forensic Investigation[14]	3
16	U.S. DoJ Guidelines[15] (2008)	5

1. M.M. Pollitt, *Computer Forensics: An Approach to Evidence in Cyberspace*, „Proceeding of the National Information Systems Security Conference, Baltimore, MD" 1995, t. II, s. 487–491.
2. G. Palmer, DTR-T001-01 Technical Report. A Road Map for Digital Forensic Research, Digital Forensics Workshop (DFRWS), Utica New York 2001.
3. A. Agarwal, M. Gupta, S. Gupta, S.C. Gupta, op. cit., s. 118.
4. M. Reith, C. Carr, G. Gunsh, *An examination of digital forensics models*, „International Journal of Digital Evidence" 2002, t. 1, nr 3.
5. B. Carrier, E.H. Spafford, *Getting physical with the digital investigation process*, „International Journal of Digital Evidence" 2003, t. 2.
6. V. Baryamereeba, F. Tushabe, *The Enhanced Digital Investigation Process Model*, Proceeding of Digital Forensic Research Workshop, Baltimore 2004.
7. M.K. Rogers, J. Goldman, R. Mislan, T. Wedge, S. Debrota, *Computer Forensic Field Triage Process Model*, Conference on Digital Forensics, Security and Law 2006, s. 27–40.
8. P. Sundresan, *Digital forensic model based on Malaysian investigation process*, „International Journal of Computer Science and Network Security" 2009, t. 9, nr 8.
9. S. Ciardhuain, *An extended model of cybercrime investigation*, „International Journal of Digital Evidence" 2009, t. 3, nr 1, s. 1–22.
10. D. Bem, E. Huebner, *Computer forensic analysis in a virtual environment*, „International Journal of Digital Evidence" 2007, t. 6, nr 2, s. 1–13.
11. R.B. Adams, op. cit.
12. S. von Solms, C. Louwrens, C. Reekie, T. Grobler, *A control framework for digital forensics,* w: M.S. Olivier, S. Shenoi (red.), *Advances in Digital Forensics II,* „IFIP Advances in Information and Communication Technology" 2006, t. 222, s. 345.
13. J. Williams, *ACPO Good practice guide for digital evidence*, Association of Chief Police Officers, March 2012, s. 7–12.
14. M. Kohn, J.H.P. Eloff, M.S. Olivier, *Framework for a digital forensic investigation*, Information and Computer Security Architectures Research Group (ICSA), Department of Computer Science, University of Pretoria, http://mo.co.za/open/dfframe.pdf (dostęp 07.05.2016).
15. M.B. Mukasey, J.L. Sedgwick, D.W. Hagy, op. cit., s. ix.

Źródło: opracowanie własne.

W ocenie autora najbardziej czytelne, szczególnie dla mniej wykwalifikowanego odbiorcy (a takimi często są na przykład policjanci, którzy muszą znać odpowiednie procedury, nawet nie będąc informatykami), są modele przewidujące zrealizowanie całego procesu pozyskiwania dowodu cyfrowego w mniejszej liczbie taktycznych faz. Przykładem uniwersalnej, a zarazem nie rozwlekłej procedury może być model powstały pod redakcją S. von Solmsa, przewidujący cztery etapy: planowania i przygotowania (gotowości), pierwszych czynności (wstępnego zabezpieczenia dowodów), śledztwa (wyodrębnienia dowodów, ich uwierzytelnienia i analizy) oraz etap sądowo-dowodowy (rekonstrukcja zdarzeń i prezentacja dowodu)[27]. Jednym z najbardziej przejrzystych i kompletnych zestawień etapów procedury uzyskania dowodu cyfrowego jest to zaproponowane przez Stowarzyszenie Komendantów Policji Anglii, Walii i Irlandii Północnej (ACPO), które zaleca realizowanie całego procesu w czterech zasadniczych fazach: planowania, zabezpieczania, analizy i prezentacji[28]. Identyczny podział wydaje się najczęściej proponowany w dotychczasowym piśmiennictwie polskim.

Wobec mnogości i różnorodności istniejących procedur pozyskiwania dowodu cyfrowego wybór odpowiedniej metodyki jest niezwykle trudny. Wszystkie modele należałoby poddać szczegółowej analizie i dokonać ich porównania, aby ustalić, która z nich mogłaby być odpowiednia dla polskich realiów procesowych. Brak powszechnej zgody co do tego, który z modeli należy stosować, powoduje, że na tak zadane pytanie nie istnieje prosta odpowiedź. W założeniach „prawidłowa" procedura powinna we względnie kompletny sposób obejmować czynności związane z pozyskiwaniem dowodu cyfrowego. Powinna być to procedura uniwersalna pod względem jej zastosowań w kontekście różnych czynów zabronionych; musi ona uwzględnić alternatywną możliwość fizycznego zabezpieczenia nośników danych cyfrowych lub wyłącznie zabezpieczenia danych dowodowych. Kompletna, uniwersalna procedura powinna być oczywiście zgodna z zasadami podstawowymi informatyki kryminalistycznej. W ocenie autora możliwe jest stworzenie „teoretycznie prawidłowej", uniwersalnej procedury postępowania z dowodem cyfrowym na gruncie literatury, a następnie dostosowanie jej – o ile okaże się to konieczne – do polskich wymogów postępowania karnego.

Na zakończenie należy ponownie podkreślić, że zabezpieczając, analizując czy też prezentując treść cyfrowego materiału dowodowego, polscy funkcjonariusze organów ścigania powinni zawsze kierować się zasadami podpartymi wskazaniami nauki informatyki kryminalistycznej – na co zresztą wskazał Sąd Najwyższy we wspomnianym wcześniej wyroku z 20 czerwca 2013 r. Najkorzystniejsze byłoby natomiast wdrożenie jednolitej i rzetelnie przygotowanej procedury pozyskiwania takich dowodów, co ułatwiłoby pracę zarówno funkcjonariuszy, jak i sądów oceniających prawidłowość zabezpieczenia dowodów. Jednak wobec rozdrobnienia różnych proponowanych modeli i procedur pozyskiwania dowodów cyfrowych wybór jednej z nich może być trudny. Istnieje bardzo wiele „gotowych do użycia" procedur stosowanych

[27] S. von Solms, C. Louwrens, C. Reekie, T. Grobler, op. cit., s. 345.
[28] J. Williams, op. cit., s. 7–12.

za granicą. W Polsce nie brak zaś ekspertów (także biegłych sądowych) krajowych dobrze zaznajomionych z tą tematyką – również takich, którzy przygotowują w tym zakresie publikacje merytoryczne. Pomimo to, w obliczu mnogości propozycji, wartościowe będzie dokonanie rzetelnego i pogłębionego zestawienia i analizy różnych proponowanych procedur. Może to pozwolić na odnalezienie pomiędzy nimi różnic i wyjaśnienie ich przyczyn, a w konsekwencji prowadzić do opracowania jednolitej procedury pozyskiwania dowodów cyfrowych odpowiedniej wobec polskich realiów procesowych – w dalszej perspektywie zmierzającej także do zweryfikowania dotychczas już zakończonych postępowań pod kątem poprawności wykorzystania w nich dowodów cyfrowych. Może to pozwolić na dokonanie faktycznej, realnej oceny prawidłowości czynności organów ścigania w zakresie posługiwania się takim materiałem dowodowym.

Streszczenie

Wykorzystanie cyfrowego materiału dowodowego w sądzie jest jednym z wyzwań współczesności dla wymiaru sprawiedliwości. Aby prezentowane dowody miały rzeczywistą wartość, konieczne jest zapewnienie im autentyczności i wiarygodności poprzez stosowanie naukowo uzasadnionych metod zabezpieczania czy analizy dowodów. Zagadnienia te leżą w zainteresowaniu informatyki kryminalistycznej – istnieje jednak bardzo wiele wersji „modelowych procedur postępowania" z dowodami cyfrowymi, co jest niekorzystne zarówno ze szkoleniowego, jak i procesowego punktu widzenia. W zakresie przyszłych badań wartościowe będzie więc opracowanie jednolitej, odpowiedniej dla polskich realiów procesowych metodyki postępowania z dowodami cyfrowymi.

Słowa kluczowe: dowód cyfrowy, dowód elektroniczny, informatyka kryminalistyczna, przestępczość komputerowa

Summary

Digital evidence is becoming more and more ubiquitous in courts, which presents a new challenge for the justice system. For digital data to be credible evidence at court, its authenticity and reliability must be ensured in accordance with rules designed within the field of forensic computer science. Unfortunately, there is a vast number of different „model procedures" in digital forensics. In terms of future research it is worth creating a uniform digital forensics procedure, suitable for polish criminal procedure.

Keywords: digital evidence, digital forensics, computer crime