Uniwersytet Ekonomiczny w Katowicach

Studia Ekonomiczne. Zeszyty Naukowe
Uniwersytetu Ekonomicznego w Katowicach
ISSN 2083-8611 Nr 355 · 2018

Informatyka i Ekonometria 13

Maciej Szmit

Uniwersytet Łódzki
Wydział Zarządzania
Katedra Informatyki
maciej.szmit@uni.lodz.pl

O STANDARDACH INFORMATYKI ŚLEDCZEJ

Streszczenie: Informatyka śledcza, pomimo znaczącej roli, jaką odgrywa współcześnie, w praktyce wymiaru sprawiedliwości nie doczekała się jeszcze – przynajmniej w Polsce – powszechnie przyjętej metodologii. Artykuł zawiera przegląd najważniejszych norm, narzędzi i dobrych praktyk informatyki śledczej oraz stanowi próbę uporządkowania najważniejszych pojęć z tego zakresu pojawiających się w krajowej literaturze przedmiotu.

Słowa kluczowe: informatyka śledcza, informatyka sądowa.

JEL Classification: K24.

Wprowadzenie

Narzędzia informatyczne odgrywają istotną rolę w kwestiach związanych z naruszeniami prawa zarówno jako „miejsca" popełnienia przestępstw (a mówiąc ściślej: nośniki informacji bądź urządzenia przetwarzające informację, przeciwko ochronie której popełniono przestępstwa), jak i jako narzędzia wspomagające działalność sprzeczną z prawem. Zdecydowana większość danych (tych intencjonalnie wytwarzanych przez ludzi, a także tych gromadzonych na ich temat w różnych systemach automatycznych, stanowiących tzw. cień cyfrowy) ma obecnie postać cyfrową, jest więc rzeczą naturalną, że musiały rozwinąć się techniki i narzędzia pozwalające na takie uzyskiwanie i taką analizę informacji z urządzeń techniki komputerowej, które wspierałyby proces rozpoznania i wykrywania przestępstw oraz ustalania stanów rzeczowych w sytuacjach prawnie relewantnych (na przykład dla potrzeb postępowań karnych, cywilnych czy administracyjnych).

Techniki i metody takie są przedmiotem zainteresowania specjalistów informatyki śledczej, natomiast szerzej ujęte zagadnienia opiniodawczej roli informatyki – informatyki sądowej. Celami niniejszego artykułu są dokonanie przeglądu najważniejszej literatury przedmiotu oraz próba uporządkowania niektórych pojęć związanych z tą rolą.

1. Podstawowe pojęcia i definicje

Informatyka śledcza nie doczekała się jeszcze sformalizowanej pozycji w klasyfikacji dyscyplin naukowych, już zresztą sama jej nazwa budzi wątpliwości: niektórzy wolą mówić o informatyce sądowej [zob. np. Szmit i in., 2011; Szmit, 2014; Kosiński, 2015], kryminalistyce komputerowej albo informatyce kryminalistycznej [por. Gruza, Goc, Moszczyński, 2008, s. 559], a nawet forensyce komputerowej (z ang. *forensic* – sądowy) [Kordylewski, 2017].

Można zaproponować następującą roboczą definicję informatyki sądowej: **Informatyka sądowa jest to dyscyplina pomostowa pomiędzy prawem a informatyką, zajmująca się opiniodawczą rolą informatyki, w szczególności opiniowaniem sądowo-informatycznym. Ma ona charakter interdyscyplinarny, funkcjonując na pograniczu nauk społecznych, tj. prawa, nauk o bezpieczeństwie** (w niektórych krajach, np. w Czechach, wyodrębnione są osobne nauki policyjne – por. np. L.F. Korzeniowski [2012]) **i nauk o zarządzaniu oraz nauk technicznych (informatyki)**.

Na pograniczu prawa i informatyki znajdują się jeszcze dwie dyscypliny niezaliczające się do informatyki sądowej: informatyka prawnicza [zob. np. Wiewiórowski, Wierczyński, 2016] – dyscyplina, przedmiotem której są systemy informacji prawnej oraz prawne aspekty tworzenia i wykorzystywania infrastruktury informacyjnej państwa, a także analiza kryminalna – zajmująca się poszukiwaniem relacji pomiędzy informacjami dotyczącymi zdarzeń o charakterze przestępczym, osób związanych z nimi oraz danymi pochodzącymi z innych źródeł (współcześnie oczywiście przy szerokim wykorzystaniu technik komputerowych).

Szczególnym rodzajem działalności opiniodawczej jest prowadzenie audytów oraz kontroli systemów teleinformatycznych i projektów informatycznych [por. np. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 10 września 2010 r.]. Kolejne szczególne miejsce – ze względu na doniosłość ekonomiczną – zajmuje opiniowanie dla potrzeb zamówień publicznych [Gawrońska-Baran, 2014]. Innym, wysoce specyficznym rodzajem działalności opi-

niodawczej jest działalność związana z informatyką śledczą, którą można spróbować zdefiniować jako dyscyplinę kryminalistyczną bądź zespół technik kryminalistycznych [Hanausek, 2005; Kozdrowski, 2012], zajmującą się badaniem urządzeń techniki komputerowej i cyfrowych nośników danych, w szczególności na potrzeby postępowania sądowego (ale również na przykład przy odzyskiwaniu przypadkowo skasowanych danych).

2. Przestępczość komputerowa

Szczególnie interesujące z punktu widzenia informatyki sądowej są zagadnienia związane z opiniowaniem w sprawach dotyczących tzw. prawa nowych technologii, w szczególności sprawach karnych dotyczących przestępstw komputerowych. Zawężając rozważania wyłącznie do najpopularniejszych zagadnień, można za Konwencją Rady Europy o Cyberprzestępczości wyróżnić następujące rodzaje „cyberprzestępstw":

1. Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów (tytuł 1):
   - nielegalny dostęp (art. 2),
   - nielegalne przechwytywanie danych (art. 3),
   - naruszenie integralności danych (art. 4),
   - naruszenie integralności systemu (art. 5),
   - niewłaściwe użycie urządzeń (art. 6).
2. Przestępstwa komputerowe (tytuł 2):
   - fałszerstwo komputerowe (art. 7),
   - oszustwo komputerowe (art. 8).
3. Przestępstwa ze względu na charakter zawartych informacji (tytuł 3):
   - przestępstwa związane z pornografią dziecięcą (art. 9).
4. Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych (tytuł 4):
   - przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych (art. 10).

Przestępstwa związane z posiadaniem, przechowywaniem czy przesyłaniem tzw. nielegalnych treści (ze względu na charakter zawartych informacji) nazywa się czasami „kontentowymi" (ang. *content* – treść, zawartość), natomiast przestępstwa odpowiadające wspominanemu powyżej tytułowi 1 Konwencji o Cyberprzestępczości – przestępstwami CIA (ang. *Confidentionality*, *Integrity*, *Availability* – poufność, integralność, dostępność).

W krajowych przepisach przestępstwa nielegalnego dostępu, nielegalnego przechwytywania danych, naruszenia integralności danych, naruszenia integralności systemu, niewłaściwego użycie urządzeń oraz fałszerstwo komputerowe zostały stypizowane w XXXIII rozdziale Kodeksu karnego (art. 267-269b). Oszustwo komputerowe stypizowane jest w art. 287 Kodeksu Karnego, przestępstwa związane z pornografią dziecięcą – w art. 202 Kodeksu Karnego. Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych kryminalizowane są po części Ustawie o prawie autorskim, po części zaś (uzyskiwanie programu komputerowego bez zgody osoby uprawnionej) w art. 278 §2 Kodeksu Karnego. Przestępstwo sharingu (nielegalnego współdzielenia usług, w szczególności sygnału telewizyjnego) – w Ustawie z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym (Dz.U. z 2002 r., nr 126, poz. 1068).

Przestępczość komputerowa w Polsce systematycznie rośnie. W tabeli 1 pokazano statystyki dotyczące liczby przestępstw wykrytych oraz wszczętych postępowań. Należy przy tym zaznaczyć, że nie wszystkie przestępstwa przeciwko ochronie informacji są przestępstwami stricte komputerowymi, na przykład takimi „niekomputerowymi" przestępstwami, które znajdą się w poniższej statystyce, mogą być: zniszczenie fotoradaru czy otwarcie cudzego (papierowego) listu. Niestety w Polsce nie prowadzi się bardziej szczegółowych badań prawometrycznych w tym zakresie.

Tabela 1. Statystyki wybranych przestępstw przeciwko ochronie informacji.

Rok	Art. 267 § 1-4		Art. 268 i 268a		Art. 269 § 1-2		Art. 269a		Art. 269b		Art. 287 § 1-2	
	Wszczętych postępowań	Stwierdzonych przestępstw	Wszczętych postępowań	Stwierdzonych przestępstw	Wszczętych postępowań	Stwierdzonych przestępstw	Wszczętych postępowań	Stwierdzonych przestępstw	Wszczętych postępowań	Stwierdzonych przestępstw	Wszczętych postępowań	Stwierdzonych przestępstw
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
2014	2868	1901	743	572	10	6	27	48	47	43	2567	2154
2013	2203	1655	765	589	14	9	37	34	42	28	1768	1573
2012	1657	1513	796	884	9	5	35	30	21	27	1285	1351
2011	1583	948	885	629	3	5	38	30	38	29	1012	1364
2010	1194	1102	690	479	7	0	22	18	35	71	838	623
2009	982	645	555	1115	6	2	34	243	23	18	673	978

cd. tabeli 1

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
2008	694	505	366	249	6	2	13	13	12	12	472	404
2007	616	384	244	168	6	0	11	11	4	4	322	492
2006	538	370	201	136	3	4	19	19	9	9	285	444
2005	430	260	152	98	2	3	1	1	6	6	326	568
2004	378	248	105	89	12	0					229	390
2003	362	232	114	138	2	2					219	168
2002	294	215	89	167	6	12					114	368
2001	259	175	60	118	9	5					59	171
2000	249	240	66	48	7	5					127	247
1999	182	113	59	49	10	1					52	164

Źródło: [Policyjne statystyki przestępczości (br.)].

3. Uwarunkowania prawne

Duża część norm i dobrych praktyk w zakresie postępowania z cyfrowym materiałem dowodowym wywodzi się ze Stanów Zjednoczonych Ameryki Północnej. Należy pamiętać, że – w związku z obowiązywaniem w prawie amerykańskim tzw. zasady owoców zatrutego drzewa, będącej częścią formalnej teorii dowodów – wymagania dotyczące postępowania z dowodami są znacznie bardziej surowe, niż ma to miejsce w przypadku postępowań przed polskimi sądami.

Doktryna owoców zatrutego drzewa (ang. *Fruit of the Poisonous Tree*, FPT), sformułowana w procesie Silverthorne Lumber Co. versus United States, oraz reguła wyłączenia dowodów (ang. *exclusionary rule*) są mechanizmami prawnym wywiedzionymi z 4. Poprawki do Konstytucji USA zabraniającymi wykorzystania przed sądem (przeciwko oskarżonemu) dowodów innych niż te, które są wynikiem legalnych działań organów dochodzeniowo-śledczych. W przeciwieństwie do tego w polskim prawie karnym procesowym obowiązuje zasada swobodnej oceny materiału dowodowego przez organ procesowy oraz – legalizujący użycie bezprawnie uzyskanych dowodów – art. 168a Kodeksu Postępowania Karnego, ponieważ zaś opinia biegłego jest jednym ze środków dowodowych, to nakładane na nią wymagania formalne są z natury rzeczy znacznie mniejsze.

Konsekwencje obowiązującego stanu prawnego są – z punktu widzenia metod opiniodawczych – dość istotne. Na przykład w odniesieniu do wykonywania kopii cyfrowych śladów dowodowych konieczne jest (w realiach amerykańskich) wykonanie podwójnej kopii wraz z obliczeniem sumy kontrolnej pozwalającej na zweryfikowanie poprawności wykonanej kopii. W realiach polskich tego rodzaju czynności nie są w żaden sposób wymagane, zdarza się również, że

opinie biegłych wydawane są na podstawie materiału, którego integralność została naruszona lub badanie prowadzone jest bezpośrednio na oryginalnym – tj. zabezpieczonym w trakcie postępowania – nośniku danych.

Odnośnie do metodologicznych wymogów dowodu z opinii biegłego przed sądem w USA obowiązuje tzw. standard Daubert, zgodnie z którym opinia powinna spełniać szereg kryteriów pozwalających ocenić, czy ekspertyza biegłego (konkluzje i badania) ma charakter naukowy, a także Federalna Reguła Dowodowa 702. Na standard ów składają się orzeczenia:

– w sprawie Daubert versus Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993 r.) oraz w sprawie apelacyjnej Daubert versus Merrell Dow Pharmaceuticals, Inc., 43 F. 3d 1311 – Court of Appeals, 9th Circuit,
– w sprawie General Electric Co. versus Joiner, 522 U.S. 136 (1997 r.) oraz
– w sprawie Kumho Tire Co. versus Carmichael, 526 U.S. 137 (1999 r.).

W Polsce orzecznictwo dotyczące metod badawczych dopuszczalnych w procesie opiniowania jest stosunkowo ubogie. Wyroki Sądu Najwyższego podkreślają rolę powszechnej akceptacji metod badawczych, kryterium aktualnego stanu wiedzy czy obecnego stanu nauki. W praktyce uniemożliwia to stosowanie do celów opiniodawczych metod o nieugruntowanej pozycji naukowej, pionierskich. W praktyce jednak nie poddaje się wątpliwość na przykład zastosowania konkretnych wersji oprogramowania do informatyki śledczej ani nawet wniosków wywiedzionych przez biegłych używających oprogramowania z naruszeniem prawa [zob. np. Kasperska, 2013].

4. Dobre praktyki i standardy

Informatyka śledcza jest dyscypliną rozwijającą się bardzo dynamicznie. Jest to oczywiście warunkowane tempem rozwoju poszczególnych technologii informatycznych. Wraz ze zmianami technologicznymi (na przykład upowszechnienia się dysków SSD w miejsce HD, rozwojem urządzeń mobilnych, upowszechnieniem się przetwarzania danych w chmurze itd.) powstają odpowiednie narzędzia i metody postępowania. Tempo rozwoju jest przy tym tak duże, że nie ma w praktyce szans na powstanie dojrzałych standardów (w sensie standardów przyjętych przez organizacje międzynarodowe, takie jak ITU-T czy ISO) dla poszczególnych grup urządzeń czy technologii. Proces normalizacyjny trwa na tyle długo, że istniejące normy – aby nie zdezaktualizować się jeszcze przed jego końcem – muszą być opracowywane na stosunkowo wysokim poziomie abstrakcji, dotyczyć kwestii ogólnych i dojrzałych technologii. Stąd też dużą rolę odgrywają rozmaite dobre praktyki czy metodyki opracowane przez

grupy badawcze. Przytłaczająca większość z nich powstała i jest rozwijana w USA. W szczególności należy wymienić SWGDE (The Scientific Working Group on Digital Evidence) – grupę badawczą utworzoną przez The Federal Crime Laboratory Directors Group, która opracowuje wytyczne dotyczące szczegółowych aspektów technicznych informatyki śledczej, oraz SWGIT (The Scientific Working Group on Imaging Technology), której dokumenty zawierają najlepsze praktyki odnośnie do analizy i przetwarzania obrazów i wideo.

Standaryzacją sensu stricto w USA zajmuje się ANSI (American National Standards Institute). Wśród standardów ANSI do badania urządzeń komputerowych odnoszą się standardy:

- AIIM TR31/1-1992 Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems – Part 1: Performance Guideline for Admissibility of Records Produced by Information Technology Systems as Evidence,
- ASTM E2678-09(2014) Standard Guide for Education and Training in Computer Forensics,
- ASTM E2825-12 Standard Guide for Forensic Digital Image Processing,
- ASTM E2763-10 Standard Practice for Computer Forensics,
- ASTM E2765-11 Standard Practice for Use of Image Capture and Storage Technology in Forensic Document Examination (standard ten dotyczy analizy dokumentów przy użyciu technik informatycznych, nie jest więc sensu stricto standardem informatyki sądowej).

Amerykański National Institute of Standard and Technology, formalnie będący częścią U.S. Department of Commerce, utrzymuje szereg projektów dotyczących informatyki śledczej. Na przykład program Computer Forensics Tool Testing Program (CFTT) poświęcony jest testowaniu urządzeń i oprogramowania wspierającego badanie śladów cyfrowych. NIST udostępnia również zasoby narzędzi oraz dokumentacji wspierającej prace informatyków śledczych, w szczególności sygnatury plików wchodzących w skład popularnych systemów operacyjnych oprogramowania (biblioteki National Software Reference Library NSRL oraz CFReDS – Computer Forensic Reference Data Sets for Digital Evidence).

Normy międzynarodowe ISO/IEC z rodziny ISO/IEC 27x zawierają kilka norm związanych z informatyką śledczą, jedna z nich – ISO/IEC 27037:2012 doczekała się już edycji polskiej (PN-EN ISO/IEC 27037:2016-12 (wersja polska), Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dotyczące identyfikowania, gromadzenia, przejmowania i przechowywania cyfrowego materiału dowodowego). Pozostałe normy to: ISO/IEC 27041:2015, Information

Technology – Security Techniques – Guidance on Assuring Suitability and Adequacy of Incident Investigative Method oraz ISO/IEC 27043:2015, Information Technology – Security Techniques – Incident Investigation Principles and Processes, a także norma dotyczącą analizy i interpretacji cyfrowych śladów dowodowych: ISO/IEC 27042:2015, Information Technology – Security Techniques – Guidelines for the Analysis and Interpretation of Digital Evidence.

Na tym tle krajowa literatura przedmiotu wygląda bardzo skromnie. Spośród dobrych praktyk i zaleceń na uwagę zasługuje dokument opracowany przez Sekcję Informatyki Sądowej Polskiego Towarzystwa Informatycznego, rekomendowany przez Pracownię Badań Komputerów Laboratorium Kryminalistycznego Komendy Wojewódzkiej Policji w Łodzi w 2009 r., zatytułowany *Dobre praktyki – badanie dysku twardego* oraz dobre praktyki związane z zabezpieczaniem dowodów elektronicznych opracowane przez Stowarzyszenie Instytut Informatyki Śledczej. Obie pozycje mają jednak znaczenie głównie historyczne.

Śladom cyfrowym poświęcona jest jedna monografia [Kasprzak, 2015], zagadnienia ich dotyczące poruszane są również w publikacjach J. Kosińskiego [2015] oraz monografii M. Szmita [2014].

Podsumowanie

Informatyka śledcza intensywnie się rozwija zarówno od strony metodologicznej, jak i narzędziowej, przy czym rozwój ten ma miejsce przede wszystkim w USA. Na tym tle informatyka śledcza w Polsce wygląda bardzo skromnie. W Polsce rozwijane są raczej systemy służące do analizy kryminalnej bądź narzędzia informatyczne znajdujące zastosowanie w innych dziedzinach kryminalistyki. Kwestią bardzo istotną jest dostosowanie istniejących standardów informatyki śledczej do warunków polskiego systemu prawnego oraz upowszechnianie fachowej wiedzy oraz znajomości norm i narzędzi wśród biegłych oraz specjalistów zajmujących się informatyką sądową i śledczą.

Literatura

AIIM TR31/1-1992 Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems – Part 1: Performance Guideline for Admissibility of Records Produced by Information Technology Systems as Evidence.

American National Standards Institute, https://www.ansi.org (dostęp: 28.11.2017).

ASTM E2678-09(2014) Standard Guide for Education and Training in Computer Forensics.

ASTM E2763-10 Standard Practice for Computer Forensics.

ASTM E2765-11 Standard Practice for Use of Image Capture and Storage Technology in Forensic Document Examination.

ASTM E2825-12 Standard Guide for Forensic Digital Image Processing.

Computer Forensic Reference Data Sets for Digital Evidence, https://www.cfreds.nist.gov (dostęp: 28.11.2017).

Federalna Reguła Dowodowa 702 (Sąd Najwyższy USA, 2011 r.), http://www.law.cornell.edu/rules/fre/rule_702 (dostęp: 28.11.2017).

Gawrońska-Baran A. (2014), *Zamówienia publiczne w zakresie informatyki*, C.H. Beck, Warszawa.

Gruza E., Goc M., Moszczyński J. (2008), *Kryminalistyka – czyli rzecz o metodach śledczych*, WAiP, Warszawa.

Hanausek T. (2005), *Kryminalistyka – zarys wykładu*, Zakamycze, Kraków.

ISO/IEC 27041:2015, Information Technology – Security Techniques – Guidance on Assuring Suitability and Adequacy of Incident Investigative Method.

ISO/IEC 27042:2015, Information Technology – Security Techniques – Guidelines for the Analysis and Interpretation of Digital Evidence.

ISO/IEC 27043:2015, Information Technology – Security Techniques – Incident Investigation Principles and Processes.

Kasperska A. (2013), *Sąd Okręgowy w Lublinie: Biegli pracowali na pirackim oprogramowaniu?* „Kurier Lubelski", 25 czerwca, http://www.kurierlubelski.pl/artykul/929564,sad-okregowy-w-lublinie-biegli-pracowali-na-pirackim-oprogramowaniu,id,t.html (dostęp: 31.08.2018).

Kasprzak W.A. (2015), *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Difin, Warszawa.

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., Dz.U. z 2015 r., poz. 728.

Kordylewski L. (2017), *Forensyka*, Forensic Science Center, Chicago IL, USA, http://kordynet.com/forensyka.html (dostęp: 25.09.2018).

Korzeniowski L.F. (2012), *Podstawy nauk o bezpieczeństwie*, Difin, Warszawa.

Kosiński J. (2015), *Paradygmaty cyberprzestępczości*, Difin, Warszawa.

Kozdrowski S. (2012), *Kryminalistyka. Wybrane zagadnienia*, NWSP, Białystok.

National Software Reference Library, https://www.nist.gov/software-quality-group/national-software-reference-library-nsrl (dostęp: 28.11.2017).

NIST CCFT Computer Forensics Tool Testing (CFTT), https://www.cftt.nist.gov (dostęp: 28.11.2017).

Orzeczenie Sądu Najwyższego USA w sprawie Daubert versus Merrell Dow Pharmaceuticals, 509 U.S. 579 (1993 r.), http://supreme.justia.com/cases/federal/us/509/579/case.html (dostęp: 28.11.2017).

Orzeczenie Sądu Najwyższego USA w sprawie Daubert versus Merrell Dow Pharmaceuticals, Inc., 43 F. 3d 1311 – Court of Appeals, 9th Circuit 1995, http://law.justia.com/cases/federal/appellate-courts/F3/43/1311/552448 (dostęp: 28.11.2017).

Orzeczenie Sądu Najwyższego USA w sprawie General Electric Co. versus Joiner, 522 U.S. 136 (1997 r.), http://supreme.justia.com/cases/federal/us/522/136/case.html (dostęp: 28.11.2017).

Orzeczenie Sądu Najwyższego USA w sprawie Kumho Tire Co. versus Carmichael, 526 U.S. 137 (1999 r.), http://supreme.justia.com/cases/federal/us/526/137/case.html (dostęp: 28.11.2017).

Orzeczenie Sądu Najwyższego USA w sprawie Silverthorne Lumber Co. versus United States, https://supreme.justia.com/cases/federal/us/251/385/case.html (dostęp: 31.08.2018).

Policyjne statystyki przestępczości (br.), http://statystyka.policja.pl (dostęp: 28.11.2017).

PN-EN ISO/IEC 27037:2016-12 – wersja polska – Technika informatyczna – Techniki bezpieczeństwa – Wytyczne dotyczące identyfikowania, gromadzenia, przejmowania i przechowywania cyfrowego materiału dowodowego.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 10 września 2010 r. w sprawie wykazu certyfikatów uprawniających do prowadzenia kontroli projektów informatycznych i systemów teleinformatycznych, Dz.U. z 2010 r., nr 177, poz. 1195.

Scientific Working Group on Digital Evidence, https://www.swgde.org (dostęp: 28.11.2017).

Scientific Working Group on Imaging Technology, https://www.swgit.org (dostęp: 28.11.2017).

Stowarzyszenie Instytut Informatyki Śledczej, http://www.siis.org.pl (dostęp: 28.11.2017).

Szmit M. (2014), *Wybrane zagadnienia opiniowania sądowo-informatycznego*, Polskie Towarzystwo Informatyczne, Warszawa.

Szmit M., Baworowski A., Kmieciak A., Krejza P., Niemiec A. (2011), *Elementy Informatyki Sądowej*, Polskie Towarzystwo Informatyczne, Warszawa.

Ustawa z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, tekst jednolity, Dz.U. z 1994 r., nr 90, poz. 631.

Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, Dz.U. z 1997 r., nr 88, poz. 553 z późn. zm.

Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego, Dz.U. z 2017 r., nr 0.1904.

Ustawa z dnia 5 lipca 2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym, Dz.U. z 2002 r., nr 126, poz. 1068.

Wiewiórowski W.R., Wierczyński G. (2016), *Informatyka prawnicza*, Wolters Kluwer, Warszawa.

A FEW WORDS ABOUT COMPUTER FORENSICS STANDARDS

Summary: Computer forensic, despite its significant role in the practice of justice, has not yet – at least in Poland – widely accepted methodology. The article contains review of computer forensics' standards, frameworks, tools and best practices and includes an attempt to describe and systematize the most important terms and definitions appearing in the scientific and professional literature of the subject.

Keywords: Computer forensics.