Patryk Królikowski

ZARYS PROBLEMATYKI DOWODU ELEKTRONICZNEGO ORAZ JEGO ZABEZPIECZANIA Z PUNKTU WIDZENIA TECHNIKI I TAKTYKI KRYMINALISTYCZNEJ

1. Zamiast wstępu...

W 1972 roku nikomu nie znany elektronik i programista John T. Draper[1] skonstruował urządzenie, które zwróciło uwagę środowiska informatyków na możliwości, jakie kryją raczkujące wówczas systemy komputerowe. Jak większość odkryć, tak i to było dziełem przypadku. Niewidomy przyjaciel Drapera zwrócił mu uwagę na gwizdek, który dodawano jako prezent-zabawkę do płatków śniadaniowych dla dzieci. Dźwięki wydawane przez gwizdek do złudzenia przypominały te emitowane przez aparaty telefoniczne podczas wybierania numerów. Okazało się, że zagwizdanie podczas rozmowy (np. podczas połączenia z bezpłatną infolinią) powodowało przełączenie centralki w tryb oczekiwania na nowe połączenie i prowadzenie rozmów - w tym także międzymiastowych i międzynarodowych - bez żadnych ograniczeń i kosztów. Ten zwyczajny gwizdek podsunął Draperowi pomysł skonstruowania urządzenia, które pozwalało na wykorzystywanie w prosty sposób centralek telefonicznych do nawiązywania dowolnych i bezpłatnych połączeń. Tak narodził się słynny Blue Box (Niebieska Skrzynka), który przez wiele lat służył „wtajemniczonym" do prowadzenia darmowych rozmów. Sam autor dzięki temu urządzeniu zatelefonował do prezydenta Richarda Nixona, a późniejszy współzałożyciel koncernu Apple, informatyk o polskich korzeniach - Steve Wozniak, jako pierwsza osoba „z zewnątrz" zatelefonował bezpośrednio do papieża.

Z biegiem lat proceder wykorzystywania Blue Boxów stał się w USA dość poważnym problemem. Powodem takiego stanu rzeczy była łatwość dostępu do tych urządzeń i tym samym narażanie zarówno koncernów telekomunikacyjnych, jak i państwa na ogromne straty finansowe. Skutkowało to zakrojonymi na szeroką skalę akcjami FBI oraz szeregiem zatrzymań, których ofiarą - w wyniku prowokacji - padł także sam Draper, choć zrezygnował z korzystania z Blue

[1] John Draper (ur. 1944), znany jako Captain Crunch, Crunch oraz Crunchman - jeden z pionierów hackingu.

Boxów wiele miesięcy wcześniej. Stosując rozróżnienie w nazewnictwie stosowane w tzw. środowisku, choć niezrozumiałe dla potocznego odbiorcy, można stwierdzić, że Draper jest przedstawicielem krystalizującego się od połowy lat 60. ubiegłego wieku *hackingu*[2], na którego kanwie powstała niechlubna odmiana nazywana *cracking*. Haking, który sam w sobie nie jest nastawiony na wyrządzanie krzywdy, a ma jedynie stanowić dowód wiedzy, umiejętności i otwartości umysłu, przerodził się w kraking - działalność przestępczą polegającą na pozbawionym zasad i nie zważającym na skutki uzyskiwaniu, niszczeniu i zmienianiu informacji znajdujących się w systemach informatycznych najczęściej w celach zarobkowych. Należy dodać, że przez długi czas przywiązywano dużą wagę do używania tych określeń we właściwym kontekście. Obecnie haking w „czystej" postaci zanika - komercjalizacja dotknęła także i tej gałęzi. Kraking ewoluował i można powiedzieć, że przyjął obecnie formę nieco bardziej złożoną określaną wspólnym mianem cyberprzestępczości.

Pojawienie się nowej grupy przestępstw - przestępstw informatycznych, zrodziło potrzebę znalezienia sposobu skutecznego przeciwdziałania i walki z nimi. Służby policyjne musiały posiąść odpowiednią wiedzę techniczną, a także poznać metody działania charakterystyczne dla komputerowych włamywaczy. Specyfika i złożoność zagadnienia okazywały się nader często niemożliwe do wystarczającego zgłębienia, stąd też tajemnicą poliszynela jest wykorzystywanie umiejętności hakerów i zatrudnianie ich „po właściwej stronie". Klasycznym przykładem jest pościg amerykańskich służb specjalnych za osławionym już Kevinem Mitnickiem[3], w który zaangażował się motywowany osobistymi pobudkami japoński naukowiec i specjalista bezpieczeństwa systemów informatycznych Tsutomu Shimomura. Jego działania nierzadko

[2] Haking (ang. *hacking*) - czynność polegająca na rozpracowaniu i znalezieniu słabych miejsc w systemie, sieci lub programie; to poznawanie systemów i ich zabezpieczeń (w informatyce m. in. analiza algorytmów zabezpieczających, wyszukiwanie (i łatanie) dziur, tworzenie oprogramowania do łamania szyfrów itd.). Zdaniem Kevina Mitnicka haking to filozofia i termin niekoniecznie związany z informatyką, bo hakować można i ludzi, i maszyny rolnicze.

Kraking (ang. *cracking*) to łamanie zabezpieczeń i włamywanie się do systemów dla własnych wymiernych korzyści i popularności.

[3] Kevin David Mitnick (ur. 6 sierpnia 1963 roku w Van Nuys, Kalifornia) - jeden z najbardziej znanych komputerowych włamywaczy. Został oskarżony o włamanie na terenie USA do kilku ważnych systemów komputerowych. Nigdy jednak nie zarzucono mu czerpania korzyści materialnych z crackingu. Po aresztowaniu Mitnick spędził w areszcie cztery lata i 5 miesięcy przed wydaniem wyroku. Przetrzymywano go w całkowitej izolacji, bez dostępu do komputerów. Zakończył odbywanie wyroku w styczniu 2000 roku, ale zakaz korzystania z Internetu obejmował go do 21 stycznia 2003. Więcej informacji w: http://www.kevinmitnick.com/, en.wikipedia.org/wiki/Kevin_Mitnick oraz Littman J.: The Fugitive Game: Online with Kevin Mitnick. Little, Brown and Company, 1996.

wykraczały poza te przewidziane prawem. Na kanwie śledztwa powstał film pt. „Takedown"[4], który co prawda dalece odbiega od rzeczywistego przebiegu zdarzeń, ale rzuca światło na problem i złożoność przestępstw informatycznych.

Oprócz hakerów dużą rolę w ujawnianiu i ściganiu przestępstw informatycznych zaczęły odgrywać również niezależne zespoły eksperckie oraz tworzone w ramach agencji rządowych grupy kryminalistyków wykrywających i zabezpieczających ślady przestępstw informatycznych. W ramach przedmiotu kryminalistyki wykształciła się nowa dyscyplina określana mianem computer forensics, w Polsce znanej jako informatyka śledcza, kryminalistyka informatyczna i informatyka kryminalistyczna.

2. Kryminalistyka informatyczna, informatyka śledcza, *computer forensics*...

Problemy z konstrukcją właściwego odpowiednika *computer forensics* w polskim języku wynikają przede wszystkim z innego pojmowania zakres przedmiotowego. W języku angielskim nie istnieje słowo „informatyka", którego źródłosłowem jest „informacja", a jedynie *computer science*. Stąd też często można spotkać nieuzasadnione, acz zrozumiałe zamienne stosowanie określeń „przestępstwo komputerowe" i „przestępstwo informatyczne", o czym szerzej w dalszej części.

W dosłownym tłumaczeniu *computer forensics* to komputerowa kryminalistyka, choć to określenie nie przyjęło się na gruncie polskim jako zbyt wąskie, bo odnoszące się tylko do komputera. Najczęściej spotykanym jest to, którego autorstwo i promocję przypisuje sobie Sebastian Małycha[5] - „informatyka śledcza". Wydaje się jednak, że z punktu widzenia nauk kryminalistycznych jest to pojęcie z kolei zbyt szerokie, gdyż odnosi się ogólnie do wykorzystania informatyki przy prowadzeniu śledztwa, a więc dotyczy również np. elektronicznych baz danych, wykorzystywanych komputerów i innego sprzętu itp., itd. Najwłaściwsze wydaje się być określenie „kryminalistyka informatyczna", której obszar zainteresowań jest nieco węższy, gdyż kładzie nacisk na zastosowanie metod kryminalistycznych w informatyce. Z tego punktu widzenia również warte rozważenia byłoby używanie nazwy „informatyka kryminalistyczna", którą należałoby wtedy tłumaczyć jako techniki informatyczne wykorzystywane w kryminalistyce.

---

[4] Pełne brzmienie tytułu: „Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw", reżyseria Joe Chappelle, producent Miramax, 2000.

[5] S. Kanikuła, *Informatyczne zbrodnie, wywiad z Sebastianem Małychą*, na http://www.outsourcing.com.pl, cyt: „Ja osobiście preferuję określenie »informatyka śledcza«, jakie zacząłem propagować, i - powiem nieskromnie - uważam się za jego autora (...)." Sebastian Małycha, prezes zarządu, dyrektor handlowy Mediarecovery, inicjator wielu akcji związanych z bezpieczeństwem i sposobami zarządzania infrastrukturą IT.

3. Pojęcia

Przed przystąpieniem do scharakteryzowania dowodów elektronicznych i metod ich zabezpieczania należy wyjaśnić poszczególne pojęcia, które są istotne dla pełnego zrozumienia ich specyfiki.

I. Bezpieczeństwo informatyczne

Bezpieczeństwo sensu *largo* to zespół czynników zewnętrznych i wewnętrznych oraz przedsięwziętych środków tworzących przekonanie o możliwości uchronienia się przed zagrożeniem. **Bezpieczeństwem informatycznym** jest więc zespół czynników, reguł, zasad postępowania oraz środków podjętych w celu uchronienia infrastruktury informatycznej (sprzętu komputerowego oraz przechowywanych za jego pomocą informacji) przed realnymi lub hipotetycznymi zagrożeniami. Omawianie poszczególnych elementów składowych bezpieczeństwa informatycznego leży poza ramami niniejszego opracowania, warto je jednak wymienić:

1. Określenie obszaru i zasobów, jakie podlegać będą ochronie oraz zbudowanie na tej podstawie polityki bezpieczeństwa.
2. Wybranie i wdrożenie odpowiednich do polityki bezpieczeństwa narzędzi (w postaci oprogramowania i sprzętu) mających zapewnić bezpieczeństwo informatyczne.
3. Przeprowadzenie testów i audytu wprowadzonego systemu zabezpieczeń.
4. Szkolenie personelu technicznego i użytkowników systemów informatycznych.
5. Stała obserwacja infrastruktury.
6. Reakcja na naruszenie bezpieczeństwa informatycznego (incydent) oraz wyciągnięcie odpowiednich wniosków.

Nie jest to wyliczenie enumeratywne i ma charakter jedynie ogólnego planu postępowania w celu zapewnienia bezpieczeństwa, który to plan w zależności od zastanych warunków może ulegać modyfikacjom. Inaczej bowiem bezpieczeństwo informatyczne będzie rozumiane w laboratoriach wojskowych, a inaczej w bibliotece publicznej. Z punktu widzenia niniejszego artykułu najistotniejszy jest punkt 6, tj. reakcja na incydent - czyli takie postępowanie, które umożliwi ustalenie przyczyny naruszenia, źródła, sprawcy oraz jego modus operandi.

II. Przestępstwo informatyczne

Pojęciem bezpośrednio związanym z bezpieczeństwem informatycznym, a ściślej z jego naruszeniem, jest przestępstwo informatyczne. Definicja taka w polskim prawie karnym nie istnieje *explicite*. Nie oznacza to jednak, że kodeks karny zupełnie pomija problem przestępstw związanych z wysoką technologią. Świadczą o tym chociażby zmiany przyjęte w październiku 2008 (weszły w życie 18.12.2008) roku, które - choć spotkały się z dość nerwową

reakcją środowisk skupionych wokół bezpieczeństwa informatycznego[6] - świadczą o zauważeniu przez legislatorów problemu. Kodeks karny wymienia kilkanaście typów czynów zabronionych, które wspólnie można określić właśnie mianem przestępstw informatycznych. Należy wspomnieć, że w doktrynie i literaturze przedmiotu spotyka się również termin „przestępstwo komputerowe"[7]. Jeśli zgodnie z definicją słownikową[8] przyjmiemy, że komputer to elektroniczna maszyna cyfrowa, a szerzej - urządzenie elektroniczne służące do automatycznego przetwarzania informacji (danych) przedstawionych cyfrowo (tzn. za pomocą odpowiednio zakodowanych liczb) [9], to przestępstwem komputerowym będzie takie, które zostało popełnione przy użyciu komputera bądź jest wymierzone przeciwko takiemu. W uproszczeniu można więc przyjąć, że przestępstwem komputerowym jest także fizyczne zniszczenie komputera (np. rozbicie młotkiem) lub użycie komputera jako narzędzia w celu okaleczenia człowieka. Jeżeli natomiast przyjmiemy powszechną definicję informatyki określającą ją jako dziedzinę nauki i techniki zajmującą się przetwarzaniem informacji - w tym technologiami przetwarzania informacji oraz technologiami wytwarzania systemów przetwarzających informacje[10], to dojdziemy do wniosku, że działania intruzów (np. hakerów, krakerów itd.) są zawsze skierowane przeciwko samej informacji, jej przepływowi, przetwarzaniu i przechowywaniu - w różnym stopniu, w zależności od rodzaju popełnianego czynu, a komputer jest tylko medium wykonującym te zadania. Włamanie do komputera, sabotaż komputerowy, piractwo komputerowe itp. pociągają za sobą zawsze naruszenie informacji, stąd też uzasadnione wydaje się używanie określenia „przestępstwo informatyczne" zamiast „przestępstwo komputerowe".

III. Dowód elektroniczny

Określenie, czym jest **dowód elektroniczny**, zawiera się w krótkim stwierdzeniu, że jest to przesyłana lub przechowywana informacja w formie elektronicznej, która może mieć znaczenie dowodowe. Jednakże zrozumienie, co jest dowodem

---

[6] Debata na temat zarówno zmiany brzmienia art. 267 jak i art. 269b toczyła się m.in. na łamach portalu prawo.vagla.pl.

[7] por. A. Adamski, *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000 oraz B. Fiszer, *Przestępstwa komputerowe i ochrona informacji*, Zakamycze, Warszawa 2000.

[8] *Słownik wyrazów obcych i zwrotów obcojęzycznych* Władysława Kopalińskiego: http://www.slownik-online.pl/kopalinski, hasło: komputer.

[9] *Nowa encyklopedia powszechna PWN*; www.encyklopedia.pwn.pl, hasło: komputer.

[10] *Słownik wyrazów obcych i zwrotów obcojęzycznych* Władysława Kopalińskiego: http://www.slownik-online.pl/kopalinski, hasło: informatyka - techniki i metody przetwarzania informacji; dyscyplina nauki i techniki zajmująca się org. powstawania i przebiegu informacji, technologią i metodyką jej przekształcania, zwłaszcza za pomocą techniki obliczeniowej.

elektronicznym, a co nim nie jest - na co wskazuje Arkadiusz Lach[11] - wymaga głębszej analizy kluczowych pojęć składających się na definicję. Te pojęcia to: „informacja" oraz „elektroniczny".

III. 1. Informacja

Z punktu widzenia nauk społecznych **informacja** to część procesu komunikacji, który polega na obiegu (nadawaniu, odbieraniu, wymianie) informacji. Przyjmuje się więc, że „informacja" po prostu istnieje niejako zewnętrznie wobec człowieka. Z podobnym traktowaniem informacji można spotkać się u Davida MacKaya, który całą pracę[12] poświęca przetwarzaniu informacji, nigdzie jej jednak nie definiując, przyjmując, że ta po prostu już jest. W próbach zdefiniowania pojęcia „informacja" badacze często posługują się innym pojęciem - „dane", których często niesłusznie używa się zamiennie, o czym w dalszej części niniejszego rozdziału. „Dane" zdaniem Thomasa Davenporta są zestawem abstrakcyjnych, obiektywnych faktów na temat rzeczy, zdarzeń i procesów[13]. Samą informację Davenport zaś definiuje jako te dane, które mają znaczenie z punktu widzenia celu powstania i przekazania informacji. Celem zaś, dla którego nadawca generuje i przesyła informację, jest wywołanie określonej zmiany w zachowaniu lub osądzie odbiorcy informacji.[14] Jak więc widać i jak słusznie zauważa Arkadiusz Lach, pojęcie informacji odnosi się głównie do nauk społecznych, jak: psychologia, socjologia, antropologia kultury, językoznawstwo czy socjolingwistyka, ale rozwijająca się nauka doprowadziła do rozszerzenia tego pojęcia na nauki przyrodnicze czy matematyczne.[15] Współcześnie informację interpretuje się zazwyczaj jako zasób, który pozwala na zwiększenie naszej wiedzy o nas i o otaczającym nas świecie[16], a na potrzeby niniejszego opracowania przyjęto definicję informacji zaproponowaną przez Tadeusza Hanauska, według której informacją są „wszelkie dane o świecie zewnętrznym, które uzyskujemy przez bezpośrednie poznanie zmysłowe, albo przez podawany przez inną osobę opis jakiegoś zjawiska lub rzeczy. "[17]

Obok definicji informacji dla dalszych rozważań wydaje się również istotne wprowadzenie określenia „praktycznej wartości informacji", gdyż nie każda wygenerowana informacja będzie miała taką samą wartość, a mówiąc innymi

[11] A. Lach, *Dowody elektroniczne w procesie karnym*, Dom Organizatora, Toruń 2004, s. 17.

[12] D, MacKay, *Information Theory, Inference and Learning Algorithms*, Cambridge University Press, Cambridge 2003.

[13] T.H. Davenport, L. Prusak, Working Knowledge. How Organizations Manage What They Know, Harvard Business School Press, Boston 1998, s. 2.

[14] Tamże, s. 3.

[15] A. Lach, *Dowody elektroniczne w procesie karnym*, Dom Organizatora, Toruń 2004, s. 18.

[16] J. Kisielnicki, H. Sroka, *Systemy informacyjne Biznesu*, Agencja Wydawnicza Placet, Warszawa 1999.

[17] T. Hanausek, *Kryminalistyka*, Zakamycze, Warszawa 200, s. 44.

słowy - nie każda informacja jest tak samo użyteczna. Zdaniem Romana Krzeszewskiego „praktyczną wartość informacji określają następujące charakterystyki:

1. Dokładność
2. Aktualność
3. Kompletność
4. Odpowiedniość

Ad. 1

Dokładność informacji wyrażona jest stopniem wiarygodności przenoszonego za jej pośrednictwem opisu rzeczywistości.

Ad. 2

Aktualność to dostępność informacji w czasie i miejscu, w których można zrobić z niej odpowiedni użytek.

Ad. 3

Kompletność mówi o tym, czy informacja daje pełny obraz rzeczywistości, której dotyczy. Dlatego cechy te należy rozpatrywać w kontekście ostatniej z nich, odpowiedniości.

Ad. 4

Odpowiedniość to właśnie dostosowanie informacji do celu i miejsca jej wykorzystania (...). "[18]

Niezależnie od swej użyteczności informacja może być - jak twierdzi Lach - przenoszona w czasie (magazynowanie, zapamiętywanie) i przestrzeni (przekaz, komunikowanie)[19]. Służą temu nośniki informacji.

III. 2. Nośniki informacji

Nośniki informacji, to urządzenia służące do zbiorowego składowania oraz odczytu zebranych informacji. Według Marka Pełki nośnikiem informacji może być każdy stabilny przedmiot materialny, na którym zapisywana jest informacja lub materiał, na którym określone zmienne wielkości fizyczne mogą reprezentować dane.[20] Według Paula Beyonon-Daviesa możemy wyróżnić następujące typy tych urządzeń:

- Dyskietki
- Pamięci taśmowe
- Dyski magnetyczne (In. twarde)
- Dyski optyczne
- Pendrive[21]

---

[18] R. Krzeszewski, *Zarządzanie i Marketing w branży IT*, referat dostępny pod adresem: http://krzeszewski.kis.p.lodz.pl/IwZE/Wyklady/ZiMwIT_1.pdf.

[19] A. Lach, *Dowody elektroniczne w procesie karnym*, Dom Organizatora, Toruń 2004, s. 18; za: S. Mynarski, *Elementy teorii systemów i cybernetyki*, PWE, Warszawa 1979.

[20] M. Pełka, *Nośniki informacji*, Computerworld nr 08/1991, wyd. IDG.

Powyższe stanowią jedynie przykłady najpopularniejszych i najbardziej podstawowych nośników informacji. Bezustanny i szybki rozwój technologii skutkuje pojawianiem się coraz to nowszych i bardziej zaawansowanych rozwiązań, co jednak nie wpływa na zmianę samej definicji „nośnika informacji", a co najwyżej rozszerza możliwości ich zastosowania. Należy w tym miejscu wspomnieć, że o ile w informatyce definicja wydaje się jednoznaczna, o tyle jednoznaczne scharakteryzowanie „nośnika informacji" na potrzeby prawa wydaje się niemożliwe - innymi określeniami posługuje się kodeks karny (art. 115 pkt. 14), innymi kodeks karny skarbowy (art. 53 pkt 20), a jeszcze inne pojęcie obowiązuje w prawie bankowym (ustawa o rachunkowości, art. 10 ust. 1 pkt 3)[22].

Nośniki informacji bywają często nazywane „nośnikami danych", co wskazuje, że nie zauważa się różnicy pomiędzy tymi dwoma pojęciami - informacja i dane, chociaż relacja dane - informacja nie jest relacją symetryczną. Dane to surowe liczby i fakty wyrażone w określonej postaci znakowej[23]. Dane traktowane osobno nie posiadają wartości informacyjnej, nabierają one treści dopiero w określonym kontekście.[24] Thomas Davenport w przedstawionym wcześniej rozróżnieniu prezentuje więc podejście infologiczne, gdzie informacja i jej interpretacja są całkowicie subiektywne, uzależnione od odbiorcy, jego wiedzy i potrzeb informacyjnych. Definiuje się więc informację jako znaczenie, jakie nadaje się danym z uwzględnieniem czynników psychosocjologicznych, językowych, semantycznych i innych. Stoi to w opozycji do podejścia datalogicznego, zgodnie z którym informacja istnieje obiektywnie. Przyjęte w artykule podejście infologiczne zakłada, że dane mogą stać się informacją, jeżeli zostaną odpowiednio ustrukturalizowane, czyli zostaną wykorzystane do budowy określonych komunikatów. Dane stanowią zatem poziom niższy w stosunku do informacji.[25] Tym samym tożsame nie są pojęcia „nośniki danych" oraz „nośniki informacji", choć w polskim prawodawstwie spotkać można oba te sformułowania.

---

[21] P. Beynon-Davies, *Systemy baz danych - nowe wydanie zmienione i rozszerzone*, Wydawnictwo Naukowo-Techniczne, Warszawa 2003, s. 31.

[22] Szerzej na ten temat w: A. Lach, *Dowody elektroniczne w procesie karnym*, Dom Organizatora, Toruń 2004, s. 18-19; w: A. Adamski, *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000, s. 67-68.

[23] J. Stoner, R. Freeman, D. Gilbert, *Kierowanie*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2001, s. 589.

[24] W. Grycewicz, *Doskonalenie jakości informacji w jednostkach administracji skarbowej. Podejście infologiczne*, praca doktorska, Akademia Ekonomiczna im. Oskara Langego we Wrocławiu, Wydział Zarządzania i Informatyki, Katedra Inżynierii Systemów Informatycznych Zarządzania, Wrocław 2007, s. 45-46.

[25] Zgodnie z twierdzeniem Bogdana Stefanowicza, na najniższym poziomie znajdują się dane, nad nimi stoi informacja, nad którą dominuje wiedza, która prowadzi do mądrości. Więcej w: B. Stefanowicz, *Informacja*, Szkoła Główna Handlowa, Warszawa 2004. s. 28.

Podsumowując powyższe, można stwierdzić, że dowodem jest zbiór ustrukturalizowanych danych, które tworzą informację mogącą mieć znaczenie procesowe.[26] Aby można było mówić o dowodzie elektronicznym, należy wyjaśnić samo określenie „elektroniczny". Według potocznego rozumienia, jak również według słownika PWN „elektroniczny" oznacza „dotyczący elektroniki; wykorzystujący zasady elektroniki"[27]. Słownik Władysława Kopalińskiego definiuje „elektroniczny" jako złożony z elementów elektronowych[28]. Sam przymiotnik „elektroniczny" nie oddaje - jak widać - istoty sprawy. Nie chodzi tu bowiem o informację dotyczącą elektroniki czy złożoną z elementów elektronowych, ale o informację zapisaną w formie elektronicznej, przy użyciu nośników informacji.

III. 3. Zapis elektroniczny

Zapis elektroniczny występuje w dwóch formach: analogowej i cyfrowej. Zapis analogowy, czyli zapis dokonany w technice analogowej, można wytłumaczyć, posługując się najbardziej powszechnym przykładem utrwalenia dźwięku na kasecie magnetofonowej[29] lub obrazu i dźwięku na kasecie typu VHS: taśma magnetyczna przesuwa się przed głowicą zapisującą, głowica wytwarza zmienne pole magnetyczne dokładnie odwzorowujące przebieg zapisywanego sygnału.[30] Dzięki oddziaływaniu pola na taśmę, sygnał analogowy zostaje w niej odwzorowany w postaci tzw. pozostałości magnetycznej, czyli lokalnych zmian nama-

[26] Istnieje wiele definicji określających „dowód" (por. R. Kmiecik, E. Skrętowicz, *Proces karny. Część ogólna*, Kraków 2002, s. 312, T. Grzegorczyk, J. Tylman, *Polskie postępowanie karne*, Warszawa 1998, s. 414). W tym miejscu należy również odnieść się do relacji informacja - dowód w odpowiedzi na narzucające się pytanie: Czy każda informacja to dowód? Najkrócej rzecz ujmując każda informacja to potencjalny dowód. Jak słusznie twierdzi Tadeusz Hanausek „każdy dowód zawiera treści informacyjne, lecz nie każda informacja ma znaczenie dowodowe." T. Hanausek, *Kryminalistyka*, Zakamycze, Warszawa 2000, s. 44,

[27] *Słownik wyrazów obcych PWN* on-line na: http://swo.pwn.pl/, hasło: elektroniczny.

[28] *Słownik wyrazów obcych i zwrotów obcojęzycznych* Władysława Kopalińskiego on-line na: http://www.slownik-online.pl/kopalinski/, hasło: elektroniczny.

[29] Szczegółowe różnice pomiędzy cyfrowym i analogowym zapisem dźwięku szerzej opisują Anna Jedynak i Jacek Rzeszotarski w: A. Jedynak, J. Rzeszotarski, *Definicja autentyczności zapisu dźwięku*, Problemy Kryminalistyki, Nr 257 (III z 2007 r.).

[30] Zarejestrowany w ten sposób sygnał ma przebieg dokładnie odzwierciedlający przebieg źródła, jednak jest obciążony poważnymi problemami jakościowymi:

- wszelkie szumy, przydźwięki i zakłócenia, jakie powstają w układach elektronicznych toru zapisu oraz w połączeniach kablowych. sumują się z sygnałem użytecznym, zniekształcając jego przebieg i obniżając jakość późniejszego odtwarzania,
- wraz z kolejnymi cyklami odczytu, wskutek bezpośredniego kontaktu głowicy z nośnikiem, stopniowemu zniszczeniu ulega warstwa ferromagnetyczna przechowująca pozostałość magnetyczną, a tym samym spada wierność nagrania, zanikają jego szczegóły, w: J. Kluczewski, *Zapis analogowy i cyfrowy dźwięku*, na: http://jkluczewski.republika.pl/, s. 1

gnesowania nośnika. Technika analogowa oznacza w tym wypadku „obróbkę sygnałów w ich podstawowej niezmienionej (naturalnej), ciągłej postaci, czyli w ich naturalnym widmie częstotliwościowym. Ciągła postać oznacza w praktyce, że jeśli zakres zmienności sygnału wynosi od 0 do 1, to jego wartość (amplituda) może w dowolnej chwili przyjąć dowolną wartość z tego przedziału i jest określona w całym okresie trwania sygnału. Dokładność określenia chwilowej wartości sygnału jest ograniczona w zasadzie jedynie dokładnością stosowanych przyrządów pomiarowych i warunkami pomiaru. Zapis analogowy oznacza, że sygnał jest rejestrowany na nośniku właśnie w naturalnej, ciągłej postaci. Jedyny zabieg, jakiemu sygnał jest poddany, to ewentualnie modulacja, umożliwiająca trwały zapis."[31] To, co przede wszystkim odróżnia zapis analogowy od cyfrowego, to niemożliwe do uzyskania w technikach cyfrowych ciągłe odwzorowanie sygnału, przetwarzanie go w naturalnej postaci.

W przeciwieństwie do zapisu analogowego zapis cyfrowy, czyli zapis wyrażony za pomocą cyfr, przy użyciu techniki cyfrowej oznacza, że sygnał przetwarzany jest z postaci naturalnej, ciągłej, do reprezentacji numerycznej, czyli ciągu dyskretnych wartości liczbowych.[32] Najbardziej rozpowszechnioną reprezentacją numeryczną jest tzw. system zero-jedynkowy, inaczej binarny lub dwójkowy. Dwójkowy system liczbowy to pozycyjny system liczbowy[33], w którym podstawą jest liczba 2, co oznacza, że do zapisu liczb potrzebne są tylko dwie cyfry: 0 i 1. Znak dwójkowy (0 lub 1) nazywany jest bitem. System ten jest powszechnie używany w informatyce, gdyż minimalizacja liczby stanów do dwóch pozwala zminimalizować przekłamywanie danych. System binarny w jasny sposób opisuje Lach stwierdzając, że „aby możliwe stało się przedstawienie informacji za pomocą dwóch jednostek, należy za ich pomocą niejako opisać potrzebne do przetwarzania informacji symbole, czyli zbiór tych symboli, nazywany inaczej alfabetem, przedstawić go w postaci cyfr 0 i 1. W tym celu bity grupuje się w zbiory znaków zawierające zazwyczaj 8 bitów, które nazywamy bajtami. Pozwala to na stworzenie 256 kombinacji (2 do potęgi 8) mających postać od 00000000 do 11111111, co wystarczy do oznaczenia wszystkich klawiszy na klawiaturze komputerowej (...). Przy użyciu takiej liczby znaków można scharakteryzować każdą wielkość (tekst obraz, dźwięk), a tym samym zakodować [przyporządkować wybrany ciąg zero-jedynkowy obiektom, które mają one reprezentować] dowolne dane wprowadzone do komputera (...)."[34]

---

[31] J. Kluczewski, *Zapis analogowy i cyfrowy dźwięku*, na: http://jkluczewski.republika.pl/, s. 1.

[32] Tamże, s. 2.

[33] System liczbowy to zbiór reguł jednolitego zapisu i nazewnictwa liczb.

[34] A. Lach, *Dowody elektroniczne w procesie karnym*, Dom Organizatora, Toruń 2004, s. 25.

Informacja w formie elektronicznej może być przetwarzana, a więc generowana, modyfikowana, rozpowszechniania itd. w systemach informatycznych i tam zwykle się znajduje.

III. 4. System informatyczny

Przez **system informatyczny** rozumiemy „ (...) formalny, komputerowy system mający za zadanie udostępnienie, wybór i integrację danych pochodzących z różnych źródeł, w celu dostarczenia we właściwym czasie informacji (...) ".[35] Pojęcie to definiuje również cyberkonwencja, gdzie w myśl art. 1 pkt a przez system informatyczny rozumie się „każde urządzeniu lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych.", a także ustawa o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926 ze zmianami), gdzie system informatyczny to „zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych." Pomimo swej ogólności i neutralności dającej swobodę w interpretacji tego, czy określony system jest systemem informatycznym[36], czy nie, definicje te mogą stanowić problem w sytuacji przechowywania informacji na nośnikach typu pendrive, płyta CD, DVD itd., czyli wtedy, kiedy wg Lacha „informacja jest przechowywana na nośniku niestanowiącym części żadnego urządzenia (...).[37] Wydaje się jednak oczywiste, że nośniki te nie będąc bezpośrednią częścią urządzenia przykładowo na skutek odłączenia przez obsługującego je człowieka[38], w dalszym ciągu zawierają określone informacje w formie elektronicznej, które uzyskać można jedynie po podłączeniu tego nośnika do systemu informatycznego. Są więc niejako mobilnym

[35] E. Turban, *Decision Support and Expert Systems. Management Support Systems*, Macmillan Publishing Company, New York, 1993, s. 29.

[36] Według zacytowanych definicji systemem informatycznym może być właściwie każdy elektroniczny system przetwarzania danych.

[37] A. Lach, *Dowody elektroniczne w procesie karnym*, Dom Organizatora, Toruń 2004, s. 27.

[38] W wielu definicjach „systemu informatycznego" jako istotny jego element pojawia się tzw. czynnik ludzki, nazywany też czynnikiem osobowym lub zasobami ludzkimi, a ponadto:

- sprzęt - głównie komputery, oraz
  - urządzenia służące do przechowywania danych,
  - urządzenia służące do komunikacji między sprzętowymi elementami systemu,
  - urządzenia służące do komunikacji między ludźmi a komputerami,
  - urządzenia służące do odbierania danych ze świata zewnętrznego,
  - urządzenia służące do wpływania systemów informatycznych na świat zewnętrzny, urządzenia służące do przetwarzania danych niebędące komputerami;
- oprogramowanie,
- elementy organizacyjne - czyli procedury,
- elementy informacyjne.

i niekoniecznym w każdym systemie, ale jednak elementem systemu informatycznego i jako takie podlegają procedurom dla niego przewidzianym.

Podsumowując powyższe rozważania, należy stwierdzić, że **dowodem elektronicznym** jest informacja w postaci zapisu elektronicznego (analogowego, cyfrowego[39]) przechowywania i/ lub przetwarzana w systemie informatycznym, która posiada znaczenie dowodowe.

4. Charakterystyka i klasyfikacja dowodów elektronicznych

Dowody elektroniczne nie stanowią odrębnej kategorii dowodów, i choć często procedury dla nich przewidziane muszą być modyfikowane, to w dalszym ciągu pozostają takie same dla tych, jak i każdych innych rodzajów dowodów. To, co wyróżnia dowody elektroniczne na tle innych, to ich specyficzne cechy, wśród których wymienia się:

1. łatwość modyfikacji,
2. wymóg szczególnych środków technicznych do jego zabezpieczenia,
3. poszlakowy charakter,
4. kopia (binarna) równa jest oryginałowi.

Dowód elektroniczny można dość łatwo spreparować, zmodyfikować, a nawet zniszczyć, co oznacza, że aby mógł nosić wartość dowodową, musi być odpowiednio zabezpieczony, uwierzytelniony, a następnie przeanalizowany przez specjalistów wg przyjętych procedur, tzw. dobrych praktyk, zebranych np. w Good Practice Guide przez Association of Chief Police Officers czy Foreign Corrupt Practices Act. Dowód elektroniczny posiada cechy poszlaki, co oznacza, że „dopiero w zestawieniu z innymi faktami, może wskazywać na sprawcę przestępstwa. Należy mieć na uwadze, iż cyberprzestrzeń daje możliwości łatwego podszywania się pod inną osobę. Analiza zgromadzonego materiału wykaże jedynie przykładowo numery IP czy MAC, które będą wskazywały na użytkownika, a nie na rzeczywistego sprawcę. Dopiero w zestawieniu z przykładowo

[39] Zważywszy na postęp technologiczny obecnie jedynie nieznaczna część dowodów to dowody zapisane w technice analogowej, stąd też należy spodziewać się, że wkrótce dowód elektroniczny i dowód cyfrowy będą jednoznaczne, choć obecnie spotkać można jeszcze rozróżnienie traktujące dowód cyfrowy jako jeden z typów dowodu elektronicznego. W literaturze spotkać można również określenie „dowód komputerowy" sugerujący jego pochodzenie i przetwarzanie na urządzeniach określonych jako „komputer", co jednak zbytnio zawęża zakres pojęcia „dowód elektroniczny", dlatego też w niniejszym tekście przyjmuje się „dowód elektroniczny" za taki, na który składają się zarówno dowody cyfrowe, dowody komputerowe, dowody wygenerowane komputerowo, dowody utworzone na skutek działania komputera, dowody pochodzące z komputera, dowody pochodzące z komputera, dowód IT, jak i wiadomość elektroniczna (za A. Lach, *Dowody elektroniczne w procesie karnym*, Dom Organizatora, Toruń 2004, s. 28-29).

przesłuchaniami, monitoringiem, można określić sprawcę."[40] Poszlakowość dowodu elektronicznego to cecha znakomitej większości tego rodzaju dowodów. Jak wcześniej wspomniano - aby dowód elektroniczny mógł zostać poddany analizie lub być zaprezentowany, musi zostać zapisany na nośniku. To sprawia, że wynikowy dowód elektroniczny ujmowany jest w kategorii dowodów rzeczowych.

Szczególną cechą ułatwiającą pracę organom ścigania i biegłym jest możliwość tworzenia nieskończonej ilości kopii dowodu, który jest identyczny z zebranym - bez obawy o pomyłki. Niewątpliwą zaletą dowodów elektronicznych jest również łatwość ich przechowywania z uwagi na niewielką ilość miejsca, jakie zajmują np. dokumenty w formie elektronicznej zgromadzone na twardym dysku.

Dowody elektroniczne można podzielić ze względu na różne kryteria. Nie podlega dyskusji podział zastosowany przez Lacha ze względu na:

1. rodzaj danych
   1.1 zawierające tekst,
   1.2 zawierające zapisy obrazu,
   1.3 zawierające zapisy dźwięku,
   1.4 inne;
2. ze względu na źródło dowodowe
   2.1 właściwe dowody rzeczowe,
   2.2 dokumenty;
3. ze względu na sposób ich wykorzystania
   3.1 samoistne,
   3.2 niesamoistne.[41]

Wydaje się jednak, że bezzasadne jest dzielenie dowodów elektronicznych ze względu na sposób ich uzyskania na pochodzące z podsłuchu i przechowywane w systemie lub na elektronicznych nośnikach. Zgodnie z wcześniejszym wyjaśnieniem nośniki elektroniczne są częścią systemu informatycznego, a podsłuch, którego rezultatem jest zaproponowana przez Andrzeja Adamskiego[42] a) treść przesyłanej informacji lub b) dane adresowe jej nadawcy i odbiorcy - również stanowi element systemu informatycznego, jeśli przyjmujemy definicję pochodzącą np. z Cyberkonwencji.

---

[40] http://kryminalistyka.fr.pl/

[41] A. Lach, *Dowody elektroniczne w procesie karnym*, Dom Organizatora, Toruń 2004, s. 37-38.

[42] A. Adamski, *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000, s. 192-197.

Wydaje się również zbyteczne wprowadzanie podziału dowodów elektronicznych ze względu na rodzaj zapisu i sposób powstania zapisu w dowodach cyfrowych[43], gdyż poniższa propozycja wyróżnia te dwie cechy jednocześnie:

4. ze względu na rodzaj zapisu
   4.1 analogowe,
   4.2 cyfrowe,
      4.2.1 zdigitalizowane (pierwotnie analogowe przekonwertowane na cyfrowe).

Z punktu widzenia techniki kryminalistycznej ważne jest wprowadzenie także podziału odnoszącego się do woli i intencji sprawcy:

5. ze względu na czynnik wolicjonalny. Mogą to być dowody:
   5.1 pozostawione przez intruza świadomie (np. rootkity, tylne furtki, skrypty zamazujące pozostawione ślady),
   5.2 pozostawione przez intruza nieświadomie (np. nieusunięcie historii wykonywanych poleceń, zwykłe skasowanie plików).

Rozróżnienie to ma poważne konsekwencje praktyczne. Sprawca może bowiem celowo pozostawić dowody np. w postaci sfałszowanych zapisów prowadzonych przez siebie działań czy dodatkowych plików, których jedynym celem jest wprowadzenie analityka w błąd. Możliwość istnienia dowodów pozostawionych celowo musi być brana pod uwagę już na etapie wstępnej analizy danych. W innym wypadku zachodzi wysokie prawdopodobieństwo przeprowadzenia błędnego wnioskowania.

Dowody elektroniczne można również podzielić, czy też pogrupować ze względu na:

6a. miejsce ich przechowywania i przetwarzania w systemie informatycznym na pochodzące z:
   6a. 1 pamięci masowych,
   6a. 2 pamięci operacyjnej,
   6a. 3 telefonów komórkowych,
   6a. 4 multimedialnych urządzeń przenośnych,
   6a. 5 ruchu sieciowego.

[43] Propozycja Arkadiusza Lacha:
Podział dowodów elektronicznych ze względu na:
- rodzaj zapisu, na analogowe i cyfrowe
- sposób powstania zapisu w dowodach cyfrowych, na: cyfrowe *sensu stricto* i zdigitalizowane (za A. Lach, *Dowody elektroniczne w procesie karnym*, Dom Organizatora, Toruń 2004, s. 37).

Można również zaproponować inną wersją powyższego - z podziałem ze względu na

6b. źródło pochodzenia na:

6b. 1 pochodzące bezpośrednio z systemu informatycznego na miejscu zdarzenia,

6b. 2 pochodzące z systemów informatycznych poza miejscem zdarzenia [np. na komputerze sprawcy pomiędzy napastnikiem a systemem docelowym; na routerach, będące rezultatem działania aplikacji ostrzegających - wpisy w logach systemów wykrywania włamań IDS, IPS, ścian ogniowych (firewalls) itp.],

6b. 3 pochodzące niebezpośrednio z systemu informatycznego (np. dyskietka leżąca w pobliżu komputera, zewnętrzny napęd dysków, palmtop itp.)

oraz ze względu na:

7. ich trwałość na:

7.1. trwałe (np. dyski twarde, dyskietki, pamięci USB),

7.2. nietrwałe (np. pamięć operacyjna, bufor procesora, zawartość plików wymiany).

5. Podstawowe zasady i sposoby zabezpieczania dowodów elektronicznych i ich nośników

Zgodnie z zasadą Locarda[44] każdy, kto pojawia się na miejscu przestępstwa, pozostawia jakiś ślad, informację mogącą być dowodem, ale jednocześnie zabiera ze sobą inny. Zadaniem kryminalistyka badającego informacje w postaci elektronicznej jest niepozostawienie odcisków swojej działalności z jednej strony, a z drugiej zebranie możliwie największej liczby oznak bytności sprawcy. W kryminalistyce informatycznej zadanie to komplikuje fakt, że większość użytecznego materiału badawczego nie ma postaci materialnej. Bez względu na to, czy badana jest zawartość serwisu internetowego czy informacje zgromadzone w komputerze, kryminalistyk porusza się w świecie binarnym, tworzącym systemy operacyjne, programy, dokumenty, gdzie zmiana jednego tylko spośród setek tysięcy zer czy jedynek może skutecznie uniemożliwić zebranie wiarygodnych informacji. Tak więc przystępując do czynności zmierzających do uzyskania przyszłego materiału dowodowego trzeba zachować szczególną ostrożność, działać zgodnie z ustalonymi standardami i bardzo skrupulatnie dokumentować każdy z poczynionych kroków. Znane są bowiem przypadki - także na gruncie polskiego orzecznictwa - że zbierane i analizowane przez wiele tygodni informacje

[44] Edmond Locard (1877-1966), pionier kryminalistyki, autor jednej z jej podstawowych zasad: „Every contact leaves a trace". Por. E. Gruza E., M. Goc, J. Moszczyński, *Kryminalistyka - czyli rzecz o metodach śledczych*, WAIP, Warszawa 2008, s. 18.

zostały odrzucone jako materiał dowodowy ze względu na nieścisłości w dokumentacji lub, co częstsze, ze względu na nieprawidłową metodologię zabezpieczenia oraz analizy. Niezmiernie ważne jest więc, aby pamiętać, że dowód elektroniczny, aby mógl być przydatny z punktu widzenia procesu karnego, musi odznaczać się następującymi cechami:

- Wierność i autentyczność - musi istnieć możliwość powiązania dowodu ze zdarzeniem. Należy mieć pewność, że dowód elektroniczny nie został zniekształcony w trakcie zabezpieczania lub analizy.
- Obiektywność - bez względu na osobę biegłego lub specjalisty analiza powinna zawsze dawać ten sam wynik.
- Kompletność - na dowód elektroniczny winna składać się odpowiednia ilość śladów elektronicznych umożliwiających wyprowadzenie określonej tezy.
- Przystępność - prezentacja dowodu elektronicznego w postępowaniu powinna być dokonywana w taki sposób, aby uczestnicy procesu nie posiadający wiedzy specjalnej z zakresu informatyki mogły zrozumieć istotę przedstawianych informacji. Uwaga ta ma zastosowanie w szczególności do wniosków zawartych w opinii biegłego.

Ponadto, przed przystąpieniem do faktycznego zbierania potencjalnych dowodów elektronicznych należy opracować szczegółowy plan działania. W zarysie powinien on określać przynajmniej następujące elementy:

1. Wyznaczenie ekspertów i określenie ich roli w zespole kryminalistycznym.
2. Przygotowanie i sprawdzenie wyposażenia technicznego laboratorium.
3. Przygotowanie narzędzi (zarówno sprzętu, jak i oprogramowania) oraz akcesoriów niezbędnych ekspertom w prowadzeniu działań na miejscu zdarzenia.
4. Zapoznanie się z dostępnymi informacjami przed przybyciem na miejsce zdarzenia.
5. Zebranie potrzebnych dokumentów przewidzianych wymogami prawa.
6. Wykonanie szczegółowej dokumentacji zastanej sytuacji bezpośrednio po przybyciu na miejsce zdarzenia (m. in. wykonanie zdjęć pomieszczenia, nośników danych, wydruków komputerowych, opisanie przewodów podłączonych do komputera (ów) itp.)
7. Zabezpieczenie i udokumentowanie nośników potencjalnych śladów elektronicznych - w formie protokołu oględzin.
8. Zadbanie o właściwy ich transport do laboratorium.
9. Analiza zgromadzonego materiału oraz przygotowanie do celów procesowych.

Przystępując do zabezpieczania śladów elektronicznych należy przestrzegać kilku kardynalnych zasad, których ignorowanie może doprowadzić do naruszenia

integralności danych lub ich zniszczenia, a w konsekwencji do skutecznego podważenia dowodu:

1. Nie wolno działać w pośpiechu, ale też nie można zbytnio zwlekać z podjęciem działań - wszystko zależy od charakteru zdarzenia. Niestety zachowanie równowagi pomiędzy szybkim działaniem a precyzją jest niezwykle trudne. Z jednej strony efektów nieprzemyślanych czynności w przestrzeni komputerowej bardzo często nie można odwrócić, ale z drugiej może się zdarzyć, że przestępca jest w dalszym ciągu podłączony do systemu i szybkie działanie może pomóc zarówno w schwytaniu go na gorącym uczynku, jak i w zebraniu wiarygodnego materiału dowodowego.
2. Ponadto, konieczne jest dość szybkie oszacowanie potencjalnych źródeł informacji. Jak wspomniano wcześniej, część z nich może mieć charakter nietrwały - przede wszystkim zawartość pamięci operacyjnej. Dlatego trzeba ocenić, które ślady najłatwiej utracić, a w związku z tym, które należy zebrać w pierwszej kolejności. Rozstrzygając o kolejności zabezpieczania śladów, można posiłkować się informacjami zawartymi w dokumencie RFC 3227 - Guidelines for Evidence Collection and Archiving[45].
3. Nigdy nie należy bezpośrednio używać ani systemu operacyjnego komputera, którego oględziny będą dokonywane, ani znajdującego się w nim oprogramowania. Zalecane jest korzystanie z wcześniej przygotowanych narzędzi, których użycie zastępuje te udostępnione przez system operacyjny. Narzędzia te powinny zostać skompilowane statycznie, tj. z wszelkimi bibliotekami niezbędnymi do prawidłowej pracy narzędzia. Na przykład kompilacja statyczna narzędzia `dcfldd`[46] pod systemem z rodziny Linux powinna zostać przeprowadzona z wykorzystaniem polecenia `make CC="gcc -static"`. Specjalizowane dystrybucje budowane na potrzeby analizy kryminalistycznej, oparte na systemie Linux, które nie wymagają instalacji na dysku twardym komputera (można je uruchomić bezpośrednio, np. z dyskietki, płyty CD lub pendriveía) tzw. LiveCD, skonstruowane są tak, aby nie ingerować w integralność analizowanego systemu. Wybierając taką dystrybucję, należy szczególną uwagę zwrócić na to, czy nie montuje ona

[45] RFC - ang. *Request for Comments*. RFC 3227 to zespół wytycznych dla osób przeprowadzających powłamaniową analizę systemów komputerowych i próbę sformalizowania związanych z tym procedur. (Rozdział 2.1 „Order of volatality".) To protokoły, procedury, specyfikacje, opinie oraz dokumentacja standardów Internetu tworzonych przez IETF - *Internet Engineering Task Force*, nieformalne, międzynarodowe stowarzyszenie osób zainteresowanych ustanawianiem standardów technicznych i organizacyjnych w Internecie.

[46] DCFLDD - narzędzie do wykonywania kopii binarnych dysków z możliwością jednoczesnego wykonywania sum kontrolnych.
Do pobrania z http://sourceforge.net/projects/dcfldd/.

automatycznie wszystkich podłączonych do badanego komputera dysków. Weryfikacja tego faktu w najprostszej postaci polega na uruchomieniu dystrybucji LiveCD na komputerze testowym (nie stanowiącym przedmiotu postępowania) oraz wydaniu polecenia `mount`. W wynikach nie powinny być widoczne żadne dyski podłączone do komputera testowego[47]:

```
ubuntu@ubuntu:~$ mount -l
tmpfs on /lib/modules/2.6.24-19-generic/volatile type tmpfs (rw,mode=0755)
proc on /proc type proc (rw,noexec,nosuid,nodev)
/sys on /sys type sysfs (rw,noexec,nosuid,nodev)
varrun on /var/run type tmpfs (rw,noexec,nosuid,nodev,mode=0755)
varlock on /var/lock type tmpfs (rw,noexec,nosuid,nodev,mode=1777)
udev on /dev type tmpfs (rw,mode=0755)
devshm on /dev/shm type tmpfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
gvfs-fuse-daemon on /home/ubuntu/.gvfs type fuse.gvfs-fuse-daemon (rw,nosuid,nodev,user=ubuntu)
```

Rysunek 1. Wyniki polecenia mount -l w systemie uruchomionym z dystrybucji LiveCD - Helix2008R1

Do specjalizowanych dystrybucji LiveCD można zaliczyć m.in. F.I.R.E[48], FCCU[49], czy Helix[50].

4. Niezależnie od presji czasu konieczne jest rzetelne dokumentowanie wszelkich dokonywanych czynności. Po przybyciu na miejsce zdarzenia należy sfotografować wyświetlony na monitorze obraz, podłączone do komputera kable, nośniki znajdujące się w pobliżu, samo otoczenie, zanotować czas przybycia. Jeżeli konieczne okaże się zabranie znalezionych przedmiotów, np. dyskietek, dysków twardych, palmtopów itp., należy zadbać o właściwe oznakowanie i bezpieczne zapakowanie (np. użycie antystatycznych torebek chroniących przed polem magnetycznym). Ta zasada, mimo iż powszechnie znana, powinna być traktowana ze szczególną uwagą, ponieważ znać przebieg zdarzenia - to jedno, a umieć je udowodnić - to już zupełnie co innego. Dlatego w postępowaniu sądowym poprawnie udokumentowane i zabezpieczone dowody mają znaczenie kluczowe. Z tego względu warto w tym miejscu wskazać na specyficzne z punktu widzenia dowodów elektronicznych elementy, które powinny znaleźć się w protokole:
   - Oznaczenie sprzętu komputerowego, w tym:
     - opis wyglądu zewnętrznego - rodzaj obudowy, zasilania, stan fizyczny ze szczególnym uwzględnieniem uszkodzeń,

[47] Dyski reprezentowane są w systemie Linux w następujący sposób /dev/[rodzaj interfesju][pozycja] np. /dev/sda to pierwszy dysk Serial ATA lub SCSI; /dev/hdb to drugi dysk IDE/EIDE. Brak takich wpisów w wynikach komendy *mount* pozwala przyjąć założenie, że dyski nie zostały zamontowane.

[48] Szczegółowe informacje na: http://fire.dmzs.com

[49] Szczegółowe informacje na: http://www.linux-forensics.com/

[50] Szczegółowe informacje na: http://www.e-fense.com/helix/.

- opis podłączonego okablowania,
- opis sposobu połączenia z siecią komputerową, np. karta Ethernet, moduł wireless LAN,
- opis podłączonych napędów dyskowych - zarówno wbudowanych, jak i zewnętrznych. W przypadku napędów zewnętrznych oznaczenie jednostkowe każdego z nich, tj.: typ, producent, numer seryjny, pojemność, struktura fizyczna (jeżeli informacje tego typu są dostępne),
- identyfikacja konfiguracji fizycznej sprzętu komputerowego, tj.: rodzaj procesora, typ/wielkość pamięci operacyjnej, opis kart rozszerzeń, typy kontrolerów dysków (np. S-ATA, SCSI, IDE).

- Zaprotokołowanie sum kontrolnych wykonanych zarówno na zabezpieczanych nośnikach, jak i sporządzonych z nich kopiach binarnych. Ewentualnie wykonanie sum kontrolnych zabezpieczonych plików oraz ich kopii.
- Oznaczenie oprogramowania w tym:
  - rozpoznanie systemu lub systemów operacyjnych zainstalowanych na nośnikach rozruchowych,
  - o ile to możliwe - zaprotokołowanie czasu pochodzącego z BIOS[51] zabezpieczanego systemu oraz czasu rzeczywistego z chwili dokonania zabezpieczenia,
  - sporządzenie wykazu plików znajdujących się na zabezpieczanych nośnikach zewnętrznych bądź wbudowanych w sprzęt komputerowy,
  - ustalenie posiadanego oprogramowania (np. nazwa, wersja, numery seryjne, instrukcje, opisy, dowody legalności).

Z chwilą zabezpieczenia sprzętu komputerowego powinna zostać sporządzona karta ewidencyjna, za pomocą której dokumentowany będzie w układzie chronologicznym każdy etap postępowania z materiałem dowodowym. Takie działanie pozwoli na spełnienie postulatu zachowania ciągłości łańcucha dowodowego (ang. *chain of custody*[52]).

---

[51] BIOS - *(Basic Input Output System)* - zbiór procedur zapisanych w pamięci stałej komputera (osadzonej na płycie głównej), którego zadaniem jest identyfikacja urządzeń systemowych oraz udostępnianie ich systemowi operacyjnemu komputera.

[52] Łańcuch dowodowy (ang. *chain of custody*) jest pojęciem odnoszącym się do sposobu postępowania z dowodem oraz utrzymania go w niezmienionej postaci. Odnosi się również do dokumentu opisującego sposób zabezpieczenia materiału, jego przechowywanie, nadzór, przenoszenie, jego analizę oraz rozporządzanie - więcej na ten temat w: A.J. Marcella, R.S. Greenfield, Cyber Forensics. *A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes*, Second Edition, Aurebach Publications, New York, London 2008, s. 12.

Przedmiotem oględzin oraz głównym źródłem dowodów na miejscu zdarzenia są najczęściej stacje robocze lub serwery - ich zawartość oraz konfiguracja. Trzeba pamiętać, że miejsce zdarzenia może być początkiem w całym łańcuchu źródeł, z których mogą pochodzić dowody. Z reguły właśnie tutaj znajdować się będzie ich znaczna część, ale równie często dodatkowych informacji będzie trzeba szukać u dostawców internetu, operatorów telekomunikacyjnych, w lokalizacjach, na które wskazują ślady z miejsca zdarzenia. W ramach jednostki centralnej (komputera) z punktu widzenia kryminalistyka można wyróżnić cztery podstawowe komponenty:

a) pamięć operacyjną,
b) interfejs sieciowy,
c) pamięć masową,
d) zewnętrze nośniki danych.

Pierwsze dwa elementy zawierają ślady nietrwałe i to właśnie na nie trzeba zwrócić uwagę w pierwszej kolejności. Pozostałe mogą być poddane analizie w późniejszym czasie.

Istnieją dwa podejścia do zbierania materiału dowodowego z systemów komputerowych.

1. Praca na tzw. **żywym organizmie** (ang. *live system*), tj. pracującym systemie, bez jego wyłączania. To podejście wymaga szczególnej ostrożności i niesie za sobą niebezpieczeństwo zniszczenia lub zmodyfikowania cennych informacji, ale prawidłowo przeprowadzone zapewnia uzyskanie największej ilości informacji. W związku z dynamicznym rozwojem technik oraz narzędzi jest to zalecana forma analizy, jeżeli badany system w chwili zabezpieczenia jest uruchomiony.
2. Tak zwana **analiza *post mortem***. Polega na badaniu elementów systemu informatycznego (najczęściej nośników) po przewiezieniu do laboratorium. Podejście to zapewnia najbardziej komfortowe warunki pracy ekspertom, ale ogranicza ilość informacji możliwych do zebrania. Analiza *post mortem* przeprowadzana jest z reguły w dwóch sytuacjach:
   a) w przypadku braku odpowiednich kompetencji osoby zabezpieczającej pracujący system operacyjny (wówczas jest on wyłączany),
   b) w przypadku gdy po przybyciu na miejsce zdarzenie okazuje się, że system będący przedmiotem zabezpieczenia został wcześniej wyłączony.

Ad. 1

Jeżeli została podjęta decyzja o zebraniu dowodów elektronicznych z pracującego systemu komputerowego, należy najpierw przygotować narzędzia, które posłużą do zebrania dalszych informacji (np. płytę CD z dystrybucją F.I.R.E). Po zgromadzeniu odpowiednich narzędzi należy zebrać przede wszystkim następujące dane:

- aktualną datę i czas wg badanego systemu - niezmiernie ważny i dość często pomijany element. Zdarza się, że data albo czas systemowy znacznie odbiegają od rzeczywistości. Ich zanotowanie pozwala na dostrzeżenie ewentualnych różnic i ustalenie faktycznego czasu działania sprawcy;
- zawartość tablicy *routingu* - pozwala na uzyskanie obrazu dróg, jakimi podróżują pakiety w komunikacji sieciowej. Może okazać się, że włamywacz zmienił ustawienia tablicy *routingu* i dzięki temu skierował ruch sieciowy w niepożądanym kierunku, co z kolei dostarcza informacji o dodatkowych źródłach materiału badawczego;
- zawartość tablicy ARP *(Address Resolution Protocol)* - zebranie tych informacji pozwoli na ustalenie powiązania adresów fizycznych komputerów (MAC) z adresami sieciowymi (IP) i być może także na zidentyfikowanie komputera sprawcy;
- aktualnie nawiązane i oczekujące połączenia, otwarte porty - pozwolą na ustalenie, czy intruz jest w dalszym ciągu podłączony do systemu i jakie są potencjalne drogi, którymi mogło nastąpić wtargnięcie;
- zawartość pamięci operacyjnej - niezwykle cenne źródło informacji. Wszelka aktywność, w tym także czynności podejmowane przez sprawcę, odzwierciedlone są zapisami w pamięci operacyjnej. Mogą tam znajdować się ostatnio wykonane polecenia, skasowane pliki (np. logi), nawiązane połączenia, identyfikatory, hasła czy klucze potrzebne do odszyfrowania danych itp. Każde działanie podejmowane na badanym komputerze powoduje zmianę zawartości pamięci, dlatego podczas zapisywania obrazu pamięci operacyjnej należy szczególnie zadbać o właściwe udokumentowanie tego procesu. Można sporządzić sumę kontrolną pobranego obrazu, ale jest to działanie raczej mało skuteczne, gdyż nigdy nie będzie możliwości porównania jej z oryginałem. Obecnie istnieją odpowiednie narzędzia umożliwiające prawidłowe zabezpieczenie i analizę zawartości pamięci operacyjnej. Czynności te mogą zostać przeprowadzone np. przy pomocy oprogramowania Memoryze (Mandiant), które pozwala na zapis zarówno całej przestrzeni pamięci operacyjnej, jak i pamięci zaalokowanej przez określony proces czy sterownik[53];
- uruchomione procesy i moduły - w każdym systemie operacyjnym uruchomione są różne składniki, które dodają funkcjonalność, pozwalają użytkownikowi na wykonywanie szeregu zadań czy dostarczają określonych informacji. Wiedza o tym, jakie programy są

[53] Szczegółowe informacje na: http://www.mandiant.com. Innym popularnym narzędziem analizy obrazów pamięci operacyjnej jest Volatality *(Volatile System)*. Szczegółowe informacje na: https://www.volatilesystems.com

w danym momencie uruchomione, pozwala na uzyskanie dodatkowych informacji na temat działań włamywacza. Może okazać się, że bez wiedzy użytkownika zostały uruchomione konie trojańskie, tylne furtki itp. Dostrzeżenie takich programów jest często utrudnione, ponieważ doświadczony sprawca potrafi skutecznie je ukryć. Ujawnienie uruchomionych procesów i aplikacji może posłużyć jako punkt wyjścia do dalszej analizy sposobu ich działania metodą inżynierii odwrotnej (ang. *reverse engineering*)[54].

W przypadku pobierania informacji z pracującego systemu pojawia się dodatkowy problem. Zdarza się bowiem, że każda minuta pracy systemu to nie tylko źródło cennych informacji dla kryminalistka, ale także dawanie sprawcy czasu na zamazanie śladów swojej bytności. Rodzi się więc pytanie, w jaki sposób uniemożliwić sprawcy dalsze działania i jednocześnie pozwolić ekspertowi na w miarę komfortowe zebranie potrzebnych dowodów. W pierwszej kolejności należy odciąć drogę dostępu do systemu. Operację tę można przeprowadzić na kilka sposobów. Pozornie najbardziej oczywistym jest wyciągnięcie kabla łączącego komputer z siecią komputerową. Choć rozwiązanie to wydaje się bezpieczne, należy pamiętać, że sprawca mógł pozostawić program, który w momencie wykrycia odłączenia kabla sieciowego uruchamia np. proces formatowania dysku, kasowania wybranych plików, zmiany informacji w plikach itp. Dlatego też zalecane jest odcięcie systemu od dostępu do sieci zewnętrznej poprzez dokonanie modyfikacji w innych punktach infrastruktury, np. na routerze, firewallu lub zarządzalnym przełączniku.

Ad. 2

Analiza *post mortem* może być poprzedzona analizą pracującego systemu bądź być przeprowadzona niezależnie od niej. W przeciwieństwie do analizy pracującego systemu, przygotowanie do analizy *post mortem* skupia się na właściwym przeprowadzeniu procedury wyłączenia systemów i zabezpieczeniu nośników danych albo w szczególnych przypadkach całego komputera. Każdy nowoczesny system operacyjny zawiera w sobie odpowiednie mechanizmy wyłączające. Niestety, dla kryminalistyka zatrzymanie systemu zgodnie z zaleceniami producentów grozi utratą wielu istotnych danych.

[54] Inżynieria odwrotna (w informatyce) - metoda analizy sposobu funkcjonowania gotowego programu czy aplikacji komputerowej bez dostępu do jej kodu źródłowego. Inżynieria odwrotna budzi kontrowersje natury etycznej. Jest bowiem niekiedy stosowana w celach przestępczych, np. ominięcia zabezpieczeń programu komputerowego, odblokowania określonej funkcjonalności (wymagającej w normalnych warunkach wykupienia odpowiedniej licencji). Inżynieria odwrotna jest jedną z podstawowych metod analizy kodu złośliwego, np. wirusów komputerowych czy koni trojańskich.

Niezależnie od tego, jakiego rodzaju jest to system (Linux, Windows, MacOS, Solaris etc.), zalecana przez producenta procedura zatrzymania ma na celu bezpieczne zamknięcie wszystkich pracujących programów, uporządkowanie danych tak, żeby podczas następnego uruchomienia można było podjąć dalszą pracę, odłączenie urządzeń itp. W systemach Windows nowej generacji wszystkie te kroki powodują zmianę wartości rejestru, modyfikację wielu plików konfiguracyjnych - słowem zamazywanie lub niszczenie śladów, które mogłyby potwierdzać lub negować działania sprawcy. W skrajnych przypadkach dobrze wyszkolony intruz może pozostawić w systemie ukryty program usuwający ślady bytności sprawcy lub wręcz uszkadzający system plików uaktywniający się wtedy, kiedy zostaje wykonane tzw. prawidłowe zamknięcie systemu. Z punktu widzenia zachowania jak największej ilości danych procedura poprawnego wyłączenia systemu jest podobna, w zasadzie bez względu na rodzaj systemu operacyjnego, i sprowadza się do odłączenia przewodu zasilającego komputer (po wcześniejszym sfotografowaniu zawartości monitora). Najcenniejszym źródłem informacji jest zawartość twardego dysku lub innych pamięci masowych znajdujących się w badanym komputerze. Przygotowując je do dalszej analizy, należy pamiętać, że:

1. Nigdy nie należy ponownie włączać komputera, gdyż spowoduje to zniszczenie istotnych informacji.
2. Po wyłączeniu komputera konieczne jest wykonanie kopii nośników danych. Wskazane jest wykonanie przynajmniej dwóch kopii każdego z nich. Kopia powinna być wykonana za pomocą specjalnego oprogramowania lub urządzenia *write blocker* pozwalającego na sporządzenie wiernego duplikatu, tzw. kopii bitowej, czyli odwzorowania każdego bitu nośnika bez względu na jego strukturę logiczną (tzn. partycje, katalogi, pliki itp.). W ten sposób zachowane zostaną wszystkie informacje, także o usuniętych lub ukrytych plikach oraz zawartości przestrzeni niezaalokowanej (nie objętej systemem plików) czy *slack space*.[55]
3. Po wykonaniu kopii należy je uwiarygodnić - to znaczy upewnić się, że są one w rzeczywistości lustrzaną kopią oryginałów. Najpopularniejszą i najbardziej skuteczną metodą służącą do uwiarygodnienia

[55] *Slack space* (ang.) - luźna przestrzeń. W systemach plików do przechowywania danych wykorzystywane są przestrzenie o określonej pojemności nazywane kontenerami, klastrami lub blokami. Wielkość bloku odpowiada najmniejszej ilości danych, z których może skorzystać system plików, aby przechować informację. Podczas zapisywania informacji kontener może zostać wypełniony w całości lub tylko częściowo. Termin *slack space* odnosi się do sytuacji, w której kontener został wypełniony częściowo i oznacza przestrzeń niewypełnioną w ramach bloku danych - szerzej na ten temat w portalu wikistc.org.

plików, katalogów lub całych dysków jest posłużenie się funkcją skrótu (np. MD5, SHA-1, SHA-2), która jest odpowiednikiem sprawdzania zgodności kodu DNA. Ideą algorytmu jest zapewnienie unikalności wyników w taki sposób, aby nie było możliwe uzyskanie tej samej wartości dla dwóch różnych zbiorów. W chwili obecnej najbardziej rozpowszechniony jest algorytm MD5, choć ujawniono, że możliwe jest jego złamanie w dość krótkim czasie. Powoli wypiera go znacznie silniejszy SHA, będący standardem w amerykańskiej Agencji Bezpieczeństwa Narodowego NSA.

4. Zarówno oryginał, jak i kopie należy przechowywać z dala od pola magnetycznego.
5. Wszelkie dalsze prace powinny być prowadzone wyłącznie na kopii bezpieczeństwa.

Jeżeli zachodzi konieczność zabezpieczenia nie tylko nośników danych, ale także całego sprzętu komputerowego, ważne jest opisanie stanu, w jakim on się znajduje przed przewiezieniem do laboratorium. W szczególności należy udokumentować sposób, w jaki sprzęt był podłączony do sieci komputerowej, jakie urządzenia były do niego przyłączone i w jaki sposób oraz zebrać wszystkie nośniki znajdujące się w pobliżu komputera, które mogły być w nim wykorzystane.

Jak zostało powiedziane wyżej, *gros* użytecznych dowodów może znajdować się nie tylko bezpośrednio na badanej maszynie, ale także na prowadzącym do niej elektronicznym szlaku. Takie wiadomości mogą zawierać routery brzegowe, bardziej zaawansowane przełączniki, firewalle, systemy ochrony IDS lub IPS, serwery poczty elektronicznej itp. Zapisy w logach powyższych produktów mogą pomóc w określeniu drogi, jaką przemierzył sprawca. Tutaj także należy działać bez zbędnej zwłoki, gdyż część logów jest systematycznie kasowana, co może uniemożliwić zebranie kluczowych informacji. Nader często szybkie uzyskanie potrzebnych danych staje się utrudnione ze względów proceduralnych - niejednokrotnie konieczna jest pomoc dostawców internetu spoza kraju.

Podczas gromadzenia dowodów nie można zapominać o ich pozornie oczywistych źródłach - urządzeniach, które w ostatnich latach weszły do powszechnego użytku i stały się nieodłącznym elementem życia, które dzięki nim stało się łatwiejsze. Mowa tutaj o elektronicznych asystentach PDA, telefonach komórkowych, smartphoneach czy nawet urządzeniach GPS. W dobie elektronicznej bankowości, poczty elektronicznej, stron www i związanych z nimi haseł, PIN-ów, tokenów, kluczy i innych zabezpieczeń coraz trudniej wszystkie te informacje zapamiętać. Dlatego też zapisywane są one właśnie na tych urządzeniach (numery PIN kart kredytowych na tych kartach, hasła dostępu do konta

w telefonach itd. itp.). Dodatkowo przechowują one szereg dokumentów, notatek i innych danych, które są wyjątkowym źródłem wiadomości także dla eksperta kryminalistyki. Jeżeli w otoczeniu miejsca zdarzenia znajdują się takie urządzenia, można mieć pewność, że zawierają chociaż jedną informację mogącą znacząco przyczynić się do ustalenia zarówno okoliczności przestępstwa, jak i sposobu jego popełnienia. Podobnie, jak w przypadku pamięci operacyjnej, także w dziedzinie analizy urządzeń mobilnych nastąpił prawdziwy przełom. Pojawiły się specjalizowane urządzenia, np. XRY. Jednak szczegółowe opisanie metod wydobywania i analizy informacji z tych urządzeń to temat na obszerne opracowanie, które wykracza poza ramy niniejszego artykułu.

Podsumowanie

Środowisko przestępcze coraz częściej wykorzystuje nowoczesne technologie informatyczne do osiągnięcia swoich celów. Obecnie oszustwa podatkowe, matrymonialne, działania nieuczciwej konkurencji, szpiegostwo przemysłowe, napady na banki czy nawet zamachy terrorystyczne często nie są możliwe bez wykorzystania informatyki i komputerów. Internet sprawia złudne wrażenie anonimowości i bezkarności, dlatego też nazbyt chętnie wykorzystywany jest do popełniania wszelkiego rodzaju przestępstw.[56] Sprzęt komputerowy daje dostęp do informacji, których uzyskanie kilka lat temu wymagało żmudnego planowania i rozległych koneksji. Wraz z przenoszeniem coraz większej liczby przestępstw do świata elektronicznego rośnie też rola kryminalistyki informatycznej w wykrywaniu i ściganiu sprawców. Jest to dziedzina rozwijająca się bardzo dynamicznie w wielu kierunkach. Wyczerpujące opisanie wszystkich metod gromadzenia i analizy śladów elektronicznych wydaje się niemożliwe - dziedzinę tę charakteryzuje duża zmienność i wymaga ona od ekspertów bezustannego kształcenia. Wiele zagadnień aktualnych dzisiaj traci na znaczeniu w przeciągu kilku miesięcy i odwrotnie - te, które wydają się nieistotne w chwili obecnej, z czasem stają się kluczowe. Działanie na polu kryminalistyki informatycznej utrudnia też brak jednolitych standardów i przepisów prawa, które regulowałyby zasady prowadzenia postępowania w oparciu o dowody elektroniczne. Są co prawda wytyczne formułowane przez agencje zajmujące się prowadzeniem takich postępowań, ale nie wiążą one z punktu widzenia procesu sądowego, a wyznaczają jedynie kierunek, w którym należy podążać. Nie jest to jednak powód do narzekań, lecz oznaka tego, że należy podejmować wszelkie działania zmierzające do unormowania na drodze prawnej i proceduralnej tej raczkującej dopiero dziedziny.

[56] Na przykład siatka Al-Kaidy porozumiewała się poprzez specjalnie przygotowany system poczty elektronicznej, a udaremniony dzięki wysiłkom policyjnej grupy do walki z przestępstwami wysokiej technologii (NHTCU) napad na bank (na kwotę ok. 220 mln funtów) został przeprowadzony zza pulpitu komputera.

BIBLIOGRAFIA:

1. Adamski A., *Prawo karne komputerowe*, C. H. Beck, Warszawa 2000.
2. Barczak A., Sydoruk T., *Bezpieczeństwo systemów informatycznych*, Dom Wydawniczy Bellona, Warszawa 2003.
3. Beynon-Davies P., *Systemy baz danych - nowe wydanie zmienione i rozszerzone*, Wydawnictwo Naukowo-Techniczne, Warszawa 2003.
4. Burdach M., *Forensic Analysis of a Live Linux System*: www.securityfocus.com
5. Carvey H., *Windows Forensics and Incident Recovery*, Addison Wesley, 2004.
6. Casey E., *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, Second Edition, Academic Press, 2004.
7. Davenport T. H., Prusak L., *Working Knowledge. How Organizations Manage What They Know*, Harvard Business School Press, Boston 1998.
8. Fiszer B., *Przestępstwa komputerowe i ochrona informacji*, Zakamycze, Warszawa 2000.
9. Gruza E., Goc M., Moszczyński J., *Kryminalistyka - czyli rzecz o metodach śledczych*, WAIP, Warszawa 2008.
10. Grycewicz W., *Doskonalenie jakości informacji w jednostkach administracji skarbowej. Podejście infologiczne*, praca doktorska, Akademia Ekonomiczna im. Oskara Langego we Wrocławiu, Wydział Zarządzania i Informatyki, Katedra Inżynierii Systemów Informatycznych Zarządzania, Wrocław 2007.
11. Grzegorczyk T., Tylman J., *Polskie postępowanie karne*, Lexis Nexis, Warszawa 1998.
12. Hanausek T., *Kryminalistyka*, Zakamycze, Warszawa 2000.
13. Jedynak A., Rzeszotarski J., *Definicja autentyczności zapisu dźwięku*, Problemy Kryminalistyki Nr 257 (III z 2007 r.).
14. Kisielnicki J., Sroka H., *Systemy informacyjne biznesu*, Agencja Wydawnicza Placet, Warszawa 1999.
15. Kluczewski J., *Zapis analogowy i cyfrowy dźwięku*, na: http: //jkluczewski.republika.pl/
16. Kmiecik R., Skrętowicz E., *Proces karny. Część ogólna*, Zakamycze, Kraków 2002.
17. Krzeszewski R., *Zarządzanie i marketing w branży IT*, referat dostępny pod adresem: http://krzeszewski.kis.p.lodz.pl/IwZE/Wyklady/ZiMwIT_1.pdf
18. Lach A., *Dowody elektroniczne w procesie karnym*, Dom Organizatora, Toruń 2004.
19. Littman J., *The Fugitive Game: Online with Kevin Mitnick*. Little, Brown and Company, 1996.
20. MacKay D., *Information Theory, Inference and Learning Algorithms*, Cambridge University Press, Cambridge 2003.

21. Marcella A. J, Greenfield R. S., *Cyber Forensics. A Field Manual for Collecting, Examining and Preserving Evidence of Computer Crimes*, Second Edition, Auerbach Publications, New York, London 2008.
22. Mynarski S., *Elementy teorii systemów i cybernetyki*, PWE, Warszawa 1979.
23. Northcutt S., *Computer Security Incident Handling. An Action Plan for Dealing with Intrusions, Cyber-Theft, and Other Security-Related Events*, SANS Institute, 2003.
24. Pełka M., *Nośniki informacji*, Computerworld nr 08/1991, wyd. IDG.
25. Stefanowicz B., *Informacja*, Szkoła Główna Handlowa, Warszawa 2004.
26. Stoner J., Freeman R., Gilbert D., *Kierowanie*, Polskie Wydawnictwo Ekonomiczne, Warszawa 2001.
27. Turban E., *Decision Support and Expert Systems. Management Support Systems*, Macmillan Publishing Company, New York, 1993.
28. Wójcik J. W., *Przestępstwa komputerowe. Fenomen cywilizacji*, CIM, Warszawa 1999.

Strony WWW

1. http://www.e-fense.com/helix/
2. www.encyklopedia.pwn.pl
3. en.wikipedia.org/wiki/
4. http://fire.dmzs.com
5. http://www.kevinmitnick.com/
6. http://kryminalistyka.fr.pl/
7. http://www.linux-forensics.com/
8. http://www.mandiant.com/
9. www.mediarecovery.pl/
10. http://www.outsourcing.com.pl
11. prawo.vagla.pl.
12. http://www.slownik-online.pl/kopalinski
13. https://www.volatilesystems.com/
14. wikistc.org