Nauka i edukacja we współczesnym świecie. Część 4
//Наука и образование в современном мире. Выпуск 4
Mirosław Borkowski, Andrey Lymar (red.)

Wydawnictwo GSW Gdańsk 2018
ISBN 978-83-89762-88-7 https://doi.org/10.24426/2018-088

Jerzy Kosiński
Wydział Dowodzenia i Operacji Morskich, Akademia Marynarki Wojennej w Gdyni
ORCID 0000-0003-3823-4526

Podstawy zajęcia i zabezpieczania danych cyfrowych jako element reagowania na naruszenia bezpieczeństwa

https://doi.org/10.24426/2018-088-03

Streszczenie

Rozdział zawiera zwięzły przegląd aktów normatywnych i dobrych praktyk związanych z zajęciem i zabezpieczaniem danych cyfrowych.

Słowa kluczowe: dane cyfrowe, naruszenie bezpieczeństwa, ślady, zabezpieczenie, live forensic.

Wstęp

Zagrożenia bezpieczeństwa we współczesnym świecie mają coraz szerszy zasięg i różnorodną postać. Przestępczość narusza bezpieczeństwo człowieka lub organizacji w każdym obszarze aktywności, ale w ostatnich czasach, wraz z rozpowszechnianiem się płatności elektronicznych oraz nowoczesnych technologii przetwarzania informacji, ślady zagrożeń i naruszeń bezpieczeństwa coraz częściej mają charakter cyfrowy. W związku z powyższym, nie tylko przed organami ścigania, stanęły nowe wyzwania, jak ujawnić, zająć i zabezpieczyć te specyficzne, często niezrozumiałe ślady w postaci danych cyfrowych.

Różnorodne urządzenia mogą tworzyć i przechowywać dane w formie cyfrowej. W nieodległej przeszłości, do opisywania niemal każdego urządzenia przetwarzającego dane cyfrowe używano słowa „komputer". Obecnie, dane cyfrowe znajdują się także w urządzeniach, których forma i wygląd znacznie odbiega od tradycyjnych komputerów, tym niemniej zachowują one swoją

cyfrową funkcjonalność (spotkać można się z nowymi określeniami, które zastąpiły słowo komputer — „e-coś tam", „inteligentne coś tam".

Ogólnie rzecz biorąc, urządzenie związane z przestępstwem i zawierające dane cyfrowe może być interesujące z dwóch powodów. Po pierwsze, urządzenie może być przedmiotem lub narzędziem przestępstwa. Na przykład, komputer używany do przekazywania pornografii dziecięcej jest narzędziem przestępstwa, a skradziony komputer jest przedmiotem przestępstwa. Po drugie, w urządzeniu mogą być przechowywane dowody popełnienia przestępstwa. Na przykład, podejrzany o popełnienie oszustwa na aukcji internetowej, na swoim urządzeniu dostępowym do Internetu może mieć zapisane treści prowadzonej korespondencji, wraz z datami i czasem ich wysłania.

Dane cyfrowe mogą być przechowywane w urządzeniach zawierających te dane na nośniku lub w systemie informatycznym. Dane cyfrowe mogą być także transmitowane.

Mimo, że każde zajęcie i zabezpieczenie danych cyfrowych jest niepowtarzalne, podejmowane strategie działania zależą od rodzaju urządzenia i jego roli w przestępstwie. Jeśli urządzenie jest dowodem, narzędziem lub przedmiotem przestępstwa, zazwyczaj będzie zabezpieczane w całości i dopiero w następnej kolejności analizowane. Ze względów organizacyjnych i technicznych znacznie rzadziej będzie wykonywany klon lub obraz nośnika danych zawartego w urządzeniu. Jeśli sprzęt jest jedynie urządzeniem do przechowywania danych, alternatywą może być zabezpieczenie wyłącznie danych.

Dokumenty normatywne

Jednym z pierwszych europejskich aktów prawnych zajmujących się problemem zabezpieczenia danych cyfrowych była Rekomendacja RE R(95)13 w sprawie problemów prawa karnego procesowego związanych z technologią informatyczną[1]. Rekomendacja wprowadziła 18 zasad skategoryzowanych w 7 rozdziałach, w tym:

I. Przeszukanie i zajęcie:

1) prawne rozróżnienie między przeszukaniem systemów komputerowych i zabezpieczeniem danych w nich zapisanych oraz danych przechwytywanych w trakcie transmisji powinno być jasno określone i stosowane;

[1] Recommendation No. R(95)13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedural Law Connected with Information Technology, przyjęta 11.09.1995 r. http://www.coe.int/t/dghl/standardsetting/media/Doc/CM/Rec(1995)013_en.asp, dostęp: 11.11.2018 r.

2) prawo karne procesowe powinno zezwolić na przeszukanie systemów komputerowych i zabezpieczenie danych na warunkach podobnych jak w tradycyjnych procedurach przeszukania i zatrzymania. Osoba odpowiedzialna za system powinna być poinformowana, że system został przeszukany i jakie dane zostały zabezpieczone. Ogólne przepisy prawne dotyczące przeszukania i zabezpieczenia powinny być odpowiednio stosowane w przypadku przeszukiwania systemów komputerowych oraz w przypadku zabezpieczania danych w nich ujawnionych;
3) podczas przeprowadzania przeszukania prowadzący powinni mieć uprawnienia, z zastrzeżeniem odpowiednich ograniczeń, do rozszerzenia przeszukania na inne systemy komputerowe, które są połączone za pomocą sieci, i do zabezpieczenia danych w nich ujawnionych, jeżeli takie natychmiastowe działanie jest wymagane;
4) w przypadku, gdy dane przetwarzane automatycznie są funkcjonalnym odpowiednikiem tradycyjnego dokumentu, przepisy prawa karnego procesowego dotyczące przeszukania i zabezpieczenia dokumentów powinno się stosować również do tych danych.

Konwencja Rady Europy o cyberprzestępczości z 2001 roku, ratyfikowana przez Polskę w 2015 roku[2], w części II (Prawo procesowe) rozdziału II (Środki, jakie należy podjąć na szczeblu krajowym) zawiera, m.in. zapisy umożliwiające:

– niezwłoczne zabezpieczanie przechowywanych danych informatycznych (art. 16) — przepisy powinny umożliwić właściwym organom nakazanie lub uzyskanie przy użyciu podobnych metod niezwłocznego zabezpieczenia wyspecyfikowanych danych informatycznych, w tym także danych dotyczących ruchu, przechowywanych za pomocą systemu informatycznego, zwłaszcza gdy istnieją podstawy do tego, by sądzić, że dane te są szczególnie podatne na ryzyko utraty lub zmodyfikowania. Zabezpieczenie i zachowanie całości danych informatycznych powinno trwać przez okres tak długi, jak będzie to konieczne, nie dłużej jednak niż 90 dni, aby umożliwić właściwym organom podjęcie starań o ich ujawnienie;
– niezwłoczne zabezpieczenie i częściowe ujawnianie danych dotyczących ruchu (art. 17) — zabezpieczenie powinno być dokonane niezależnie od tego, czy tylko jeden czy też więcej dostawców usług uczestniczyło w przekazywaniu takich informacji, a ujawnienie właściwemu organowi Strony lub osobie wyznaczonej przez ten organ dostatecznej ilości danych dotyczących ruchu, aby umożliwić Stronie identyfikację dostawców usług i kanałów, jakimi przekaz nastąpił;

[2] Dz.U. z 2015 r., poz. 728.

– przeszukanie rozszerzone (art. 19 ust. 2) — każda Strona przyjmie środki prawne i inne, które mogą być potrzebne dla zapewnienia, aby właściwe organy dysponowały odpowiednimi środkami pozwalającymi na niezwłoczne rozszerzenie przeszukania lub użycie podobnych metod uzyskiwania dostępu na inny system, jeżeli podczas dokonywania przez nie przeszukania lub uzyskiwania dostępu przy użyciu podobnych metod do konkretnego systemu informatycznego lub jego części oraz do danych informatycznych w nim przechowywanych, pojawią się uzasadnione podstawy, by sądzić, że poszukiwane dane przechowywane są w innym systemie informatycznym lub w jego części na ich terytorium i że do danych tych można legalnie uzyskać dostęp z systemu pierwotnego lub są one dostępne dla tego systemu.

A w części II (Postanowienia szczegółowe) rozdziału III (Współpraca międzynarodowa) zapisano:

– ponadgraniczny dostęp do przechowywanych danych, za zgodą lub gdy są one publicznie dostępne (art. 32) — Strona, bez zezwolenia drugiej Strony, może:
  a) uzyskać dostęp do przechowywanych danych informatycznych, które są publicznie dostępne (źródło otwarte), niezależnie od geograficznej lokalizacji tych danych lub
  b) uzyskać dostęp lub otrzymać za pomocą systemu informatycznego znajdującego się na własnym terytorium dane informatyczne przechowywane na terytorium innego państwa, jeżeli Strona uzyska prawnie skuteczną i dobrowolną zgodę osoby upoważnionej do ujawnienia Stronie tych danych za pomocą tego systemu informatycznego.

Pojęcia prawne danych cyfrowych lub informatycznych nie są zdefiniowane w Polsce ustawowo. Można w tym zakresie posiłkować się definicją zapisaną w art. 1b Konwencji o cyberprzestępczości — „dane informatyczne" oznaczają dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny.

W Polsce, przeszukanie i zatrzymanie dokonywane w odniesieniu do systemów komputerowych, nośników i zasobów poczty elektronicznej reguluje art. 236a k.p.k.[3] z rozdziału 25[4], który stanowi, że „przepisy tego rozdziału stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się

[3] Ustawa z dnia 6 czerwca 1997 r. — Kodeks postępowania karnego (Dz.U. nr 89, poz. 555 ze zm.).

[4] Rozdział 25 k.p.k. w artykułach 217–236a normuje czynności zatrzymania rzeczy i przeszukania.

w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną"[5]. Odpowiednie stosowanie przepisów dotyczących zatrzymania rzeczy i przeszukania dotyczy przede wszystkim:

1) wydania rzeczy i przymusowego odebrania, w tym transferu danych określonych w tym artykule (art. 217);
2) możliwości żądania wydania zapisów wiadomości poczty elektronicznej oraz wykazu połączeń za pomocą poczty elektronicznej (art. 218);
3) możliwości żądania wydania określonych w tym artykule danych, poszukiwania nośnika tych danych oraz poszukiwania zawartości dysków komputerowych (art. 219);
4) dysponowania i przekazywania danych, stosownie do przepisów określających ochronę tajemnicy (art. 225).

Czynności przeszukania rzeczy i systemu informatycznego oraz zatrzymania rzeczy i danych informatycznych wymagają spisania protokołu (art. 143 k.p.k.).

W celu znalezienia rzeczy[6] mogących stanowić dowód w sprawie lub podlegających zajęciu w postępowaniu karnym, można dokonać przeszukania pomieszczeń i innych miejsc, jeżeli istnieją uzasadnione podstawy do przypuszczenia, że osoba podejrzana lub wymienione rzeczy tam się znajdują (art. 219 k.p.k.). Osobę mającą rzeczy mogące stanowić dowód w sprawie wzywa się do ich wydania (na podstawie postanowienia sądu lub prokuratora, a w wypadkach niecierpiących zwłoki — także na żądanie Policji lub innego uprawnionego organu), natomiast w razie odmowy można przeprowadzić ich odebranie (art. 217 § 2 i 5 k.p.k.). W czasie poszukiwania dowodów cyfrowych przypadki niecierpiące zwłoki zdarzają się dosyć często, gdyż z powodów technicznych bardzo prawdopodobna jest obawa, że np. dostęp do danych lub ich odzyskanie staną się niemożliwe lub znacznie utrudnione po wyłączeniu systemu. Podstawą takiego przeszukania może być również przypuszczenie, że osoba podejrzana wie o prowadzonych przez organ ścigania czynnościach i może podjąć próbę zniszczenia danych.

---

[5] Pojęcie korespondencji przesyłanej pocztą elektroniczną należy w tym kontekście interpretować jako odnoszące się do korespondencji elektronicznej, która może być przesyłana, ale w danej chwili nie jest transmitowana, np. została zapisana przed wysłaniem lub odebrana. A. Lach zwraca uwagę na to, że odpowiednie stosowanie oznacza, iż część przepisów stosuje się wprost (art. 227 i 236), część z niezbędnymi modyfikacjami (art. 217 — wydanie przez skopiowanie), a pozostałych nie stosuje się w ogóle (art. 230 — zwrot zatrzymanych rzeczy po skopiowaniu danych). A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 96 i nast.

[6] A. Adamski twierdzi, że dane nie są rzeczą (A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 40). S. Waltoś uważa, że pod określeniem „rzecz" należy rozumieć każdy produkt aktywności człowieka (S. Waltoś, *Proces karny. Zarys systemu*, Warszawa 2009, s. 340).

Sposobem uzyskiwania środków dowodowych jest także dokonanie oględzin. Prof. Arkadiusz Lach trafnie zauważa, że „przepisów o przeszukaniu nie stosuje się w sytuacji, gdy dane mają charakter ogólnodostępny i dla celów dowodowych wystarczy dokonanie ich oględzin (…) z ewentualnym skopiowaniem, np. przez wydruk lub zapis”[7]. Jako przykład podaje znalezienie strony www za pomocą słów kluczowych wpisanych do wyszukiwarki internetowej. Można wyobrazić sobie następujący ciąg działań:

– czytamy zawartość strony, stwierdzamy, że zawiera niedozwolone treści;
– zabezpieczamy zawartość strony, rejestrując komunikację z www oraz swoje działania;
– przechodzimy na podstrony (klikając na odsyłacz) i powtórnie wykonujemy te same działania.

Całość działań opisuje się w protokole oględzin, do którego załącza zarejestrowane wyniki działań (można to również zrealizować w sposób zautomatyzowany wykorzystując np. program *Forensic Acquisition of Websites*).

Do wydania danych mogących stanowić dowód w sprawie zobowiązani są także dysponent (np. administrator) i użytkownik (np. posiadacz konta pocztowego) systemu informatycznego w zakresie danych przechowywanych w tym systemie lub na nośniku danych znajdującym się w ich dyspozycji lub użytkowaniu. Zapis art. 236a k.p.k. odnosi się także do dysponentów i użytkowników z zagranicy, pod warunkiem że wykonanie tego zobowiązania nie narazi ich na odpowiedzialność karną, cywilną lub administracyjną w ich państwie[8].

Warto pamiętać, że przepis art. 218a k.p.k. nakłada na urzędy, instytucje i podmioty prowadzące działalność telekomunikacyjną obowiązek niezwłocznego zabezpieczenia (zamrożenia), na żądanie sądu lub prokuratora zawarte w postanowieniu, na czas określony, nieprzekraczający jednak 90 dni, danych informatycznych przechowywanych w urządzeniach zawierających te dane, na nośniku lub w systemie informatycznym. Jeżeli zamrożone dane informatyczne są pozbawione znaczenia dla postępowania karnego, to należy je niezwłocznie zwolnić spod zabezpieczenia. Postanowienie powinno wyraźnie określać zakres danych, które powinny zostać zabezpieczone (np. poprzez podanie podmiotów, których dotyczą, numeru telefonu, czasu połączeń). Sąd lub prokurator powinni określić też sposób zabezpieczenia, aby dane można było wykorzystać w postępowaniu karnym.

Na podstawie ustawy o Policji może być dokonane zdalne przeszukanie. Art. 19 ust. 6 punkt 3 stanowi, że kontrola operacyjna zarządzona na podstawie tego artykułu może polegać także na „stosowaniu środków technicznych

[7] A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 109.
[8] *Ibidem*, s. 98.

umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie". Takie przeszukanie nie jest jednak czynnością procesową, tylko operacyjno-rozpoznawczą[9].

Spośród polskich przepisów prawnych zwrócenia uwagi wymaga art. 9 ust. 1 pkt 4 ustawy o działaniach antyterrorystycznych[10] o następującym brzmieniu:

> 1. W celu rozpoznawania, zapobiegania lub zwalczania przestępstw o charakterze terrorystycznym Szef ABW może zarządzić wobec osoby niebędącej obywatelem Rzeczypospolitej Polskiej, w stosunku do której istnieje obawa co do możliwości prowadzenia przez nią działalności terrorystycznej, na okres nie dłuższy niż 3 miesiące, niejawne prowadzenie czynności polegających na: (…)
>
> 4) uzyskiwaniu i utrwalaniu danych zawartych na informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych;

Z powyższego zapisu oraz analogii pozwalającej na uzyskanie przez służbę dostępu do treści dokumentu chronionego w zabezpieczonym miejscu na terenie innego państwa, do którego dostęp uzyskała osoba inwigilowana przez ABW, niebędąca obywatelem RP, ale przebywająca na terenie Polski, czy to z poziomu sieci przesyłającej tę treść, czy to z poziomu urządzenia końcowego (np. odbierającego wiadomość: faksu, smartfona, komputera)[11], to można uznać, że posiadanie przez ABW danych dostępowych (hasła, klucza) do umieszczonego w „chmurze" zasobu takiej osoby, przebywającej na terenie Polski, uprawnia ABW do jego wykorzystania i utrwalenia danych z tej „chmury".

Do powszechnego i wielokrotnego stosowania, przy pozyskiwaniu i zabezpieczaniu śladów cyfrowych, w zakresie technicznym przygotowano zasady, wytyczne i charakterystyki zawarte w normach:

a) PN-EN ISO/IEC 27037:2016-12 Technika informatyczna — Techniki bezpieczeństwa — Wytyczne do identyfikacji, gromadzenia, pozyskiwania i zachowania śladów cyfrowych (dowodowych).

   Dokument ten zawiera wytyczne do specyficznych działań w ramach postępowania ze śladami cyfrowymi. Do tych działań należą:
   - identyfikacja,
   - gromadzenie,
   - pozyskiwanie,
   - utrwalanie

[9] Szerzej na ten temat: A. Lach, *Przeszukanie na odległość systemu informatycznego*, „Prokuratura i Prawo" nr 9/2011.
[10] Dz.U. z 2016 r., poz. 904.
[11] Dostęp w pełni uprawniony, zarówno na podstawie art. 9 ust. 1 pkt 4, jak i pkt 3 u.o.d.a.

cyfrowych śladów dowodowych, które mogą mieć wartość dowodową. Zawiera wskazówki, w odniesieniu do typowych sytuacji spotykanych w całym procesie, postępowania z cyfrowymi śladami dowodowymi i pomaga w ich procedurach dyscyplinarnych oraz w ułatwianiu wymiany potencjalnych śladów cyfrowych pomiędzy różnymi systemami prawnymi. Wytyczne dotyczą niżej wymienionych urządzeń i/lub funkcjonalności, które są stosowane w różnych sytuacjach:

– nośniki danych cyfrowych stosowane w standardowych komputerach, takie jak dyski twarde, dyskietki magnetyczne, dyski optyczne i magnetooptyczne, karty pamięci oraz inne urządzenia do przechowywania danych o podobnych funkcjach;
– smartfony, telefony komórkowe, tablety (Personal Digital Assistants — PDA, Personal Electronic Devices — PED);
– mobilne urządzenia do nawigacji;
– cyfrowe aparaty fotograficzne i kamery wideo (w tym monitoring wizyjny CCTV);
– typowe komputery podłączone do sieci;
– urządzenia sieci opartych na protokole TCP/IP i innych protokołach cyfrowej transmisji danych;
– urządzenia o funkcjach podobnych do wyżej wymienionych.

Oczywiście ta lista urządzeń nie jest wyczerpująca i ma charakter wyłącznie orientacyjny.

b) PN-EN ISO/IEC 27041:2016-12 Technika informatyczna — Techniki bezpieczeństwa — Wytyczne do zapewnienia stosowności i adekwatności metody dochodzeniowej w związku z incydentem.

W tej normie zawarto wytyczne do mechanizmów zapewniania, że metody i procesy używane w dochodzeniu w związku z incydentami naruszenia bezpieczeństwa informacji są odpowiedni. W normie wskazano najlepsze praktyki określania wymagań, opisywania metod oraz zapewniania, że wdrożenie tych metod spełni wymagania stosowności i adekwatności. Norma ma na celu:

– zapewnienie wytycznych do przechwytywania i analizy wymagań funkcjonalnych i niefunkcjonalnych odnoszących się do dochodzenia w związku z incydentem naruszenia bezpieczeństwa informacji;
– podanie wytycznych do użycia walidacji jako środka zapewnienia odpowiedniości procesów, które składają się na dochodzenie;
– zapewnienie wytycznych do oszacowania wymaganych poziomów walidacji oraz wymaganej ewidencji wynikającej z testu walidacyjnego;

– podanie wytycznych, w jaki sposób zewnętrzne testowanie i dokumentowanie może zostać włączone w proces walidacji.

c) PN-EN ISO/IEC 27042:2016-12 Technika informatyczna — Techniki bezpieczeństwa — Wytyczne do analizy i interpretacji śladu cyfrowego (dowodowego).

W tej normie zawarto wytyczne do analizy i interpretacji śladu cyfrowego w sposób umożliwiający zachowanie ciągłości, ważności, odtwarzalności i powtarzalności. Zawiera najlepsze praktyki odnoszące się do wyboru, projektowania i wdrażania procesów analizy oraz rejestrowania informacji w ilości wystarczającej do poddania tych procesów niezależnemu badaniu (jeśli pojawią się takie wymagania). Zawiera wytyczne do odpowiednich mechanizmów umożliwiających przedstawienie biegłości i umiejętności zespołu dochodzeniowego. Analiza i interpretacja śladu cyfrowego może być złożonym procesem. W pewnych okolicznościach istnieje wiele metod, które zespół może wykorzystać do analizy i interpretacji. Zastosowanie określonej metody może wpływać na interpretację śladu cyfrowego przetwarzanego za pomocą tej metody. Dostępny ślad cyfrowy może wpływać na wybór metod do dalszej analizy tego już pozyskanego śladu cyfrowego. W procesie sądowym może pojawić się konieczność uzasadnienia, przez zespół dochodzeniowy, wyboru określonego procesu i wykazania jego równoważności w odniesieniu do innego procesu używanego przez innych specjalistów. Jeżeli nie można tego uzasadnić, to należy zaprojektować nowe metody sprawdzenia śladu cyfrowego, które wcześniej nie były rozważane i udowodnić, że wytworzona metoda jest właściwa. W normie przedstawiono wspólną strukturę analitycznych oraz interpretacyjnych elementów obsługi incydentów związanych z naruszeniem bezpieczeństwa systemów, które mogą być użyte jako wsparcie we wdrażaniu nowych metod oraz zawarto minimalny wspólny standard śladu cyfrowego wytworzonego w wyniku tych działań.

d) PN-EN ISO/IEC 27043:2016-12 Technika informatyczna — Techniki bezpieczeństwa — Pryncypia i procesy w dochodzeniach związanych z incydentami.

W dokumencie zawarto wytyczne, wykorzystujące modele teoretyczne, do procesów dochodzeniowych obejmujących wykorzystanie śladów cyfrowych, przy incydentach różnych typów. Wytyczne te obejmują zarówno procesy od przygotowania przed incydentem do zamknięcia dochodzenia, jak i ogólne wskazówki i zastrzeżenia odnoszące się do tych procesów, jed-

nakże bez ich szczegółowego omawiania. W wytycznych opisano procesy i pryncypia mające zastosowanie do dochodzeń różnego rodzaju do:
- nieuprawnionego dostępu;
- naruszenia bezpieczeństwa danych;
- awarii systemu lub korporacyjnych naruszeń bezpieczeństwa informacji;
- a także do jakichkolwiek innych dochodzeń informatycznych.

e) PN-EN ISO/IEC 30121:2016-12 Technika informatyczna — Nadzór nad strukturą ryzyka związanego z informatyką śledczą.

W normie zaproponowano strukturę, przeznaczoną dla organów nadzorujących w organizacjach (w tym właścicieli, członków rad nadzorczych, dyrektorów, partnerów, najwyższego kierownictwa lub podobnych ciał), najlepszego przygotowania organizacji do dochodzeń związanych z informatyką śledczą. Jej zastosowanie dotyczy rozwoju strategicznych procesów (i decyzji) związanych z przechowywaniem, dostępnością, dostępem, opłacalnością i ujawnianiem śladów cyfrowych. Norma jest przeznaczona do stosowania w organizacji każdego rodzaju i wielkości.

Uzupełnieniem powyższych norm są funkcjonujące w systemie PN normy:
- PN ISO/IEC 27000:2014-11 Technika informatyczna — Techniki bezpieczeństwa — Systemy zarządzania bezpieczeństwem informacji — Przegląd i terminologia;
- PN ISO/IEC 27001:2014-12 Technika informatyczna — Techniki bezpieczeństwa — Systemy zarządzania bezpieczeństwem informacji — Wymagania;
- PN ISO/IEC 27002:2014-12 Technika informatyczna — Techniki bezpieczeństwa — Praktyczne zasady zabezpieczania informacji, która powstała na podstawie wycofanej normy PN-ISO/IEC 17799:2007.

Podstawy techniczne i organizacyjne

W trakcie zabezpieczania danych cyfrowych, które mają być dowodami należy przestrzegać podstawowej zasady, nakazującej takie zachowanie i zabezpieczenie materiału dowodowego, aby w toku przeprowadzania dowodów przed sądem można było wykazać, gdyby strony procesowe podały w wątpliwość, że zabezpieczony, a następnie przebadany materiał dowodowy jest tym wła-

śnie, który organy ścigania zastały w miejscu przeprowadzenia przeszukania i zabezpieczania dowodów. Z tej zasady wynikają wytyczne, które dotyczą[12]:

a) zachowania na miejscu przeszukania — odpowiedzialny za przeszukanie i zabezpieczenie materiału dowodowego nie powinien nigdy robić tego samotnie, ze względu na swoje bezpieczeństwo, wiarygodność dowodów, możliwość zauważenia większej ilości szczegółów, a także lepsze rozwiązywanie pojawiających się problemów według zasady „co dwie głowy, to nie jedna";
b) integralności danych — żadne działania podejmowane przez zabezpieczającego nie powinny zmieniać stanu urządzeń elektronicznych albo mediów, które później mogą zostać wykorzystane w sądzie, do momentu ich utrwalenia. Nie wolno zmieniać konfiguracji i połączeń sprzętu komputerowego albo oprogramowania przed ich sfilmowaniem lub sfotografowaniem, ani dokonywać modyfikacji danych na nośnikach danych przed sporządzeniem ich kopii;
c) protokołowania — protokół (lub inna postać dokumentu) musi zawierać zapis wszystkich działań podejmowanych podczas przeszukiwania i zabezpieczania dowodu elektronicznego. Wszystkie działania wiążące się z zatrzymaniem, dostępem, opakowaniem, przemieszczaniem, składowaniem dowodu muszą w pełni zostać udokumentowane (łańcuch dowodowy[13]) i być dostępne dla niezależnej oceny, co powinno zapewnić jego wartość dowodową w sądzie;
d) wsparcia eksperckiego — ze względu na specyficzną postać i właściwości dowodów cyfrowych, w niektórych przypadkach do poszukiwania i zatrzymania dowodu może być konieczna pomoc ekspertów mających wiedzę specjalistyczną spoza organów ścigania. Poza wiedzą specjalistyczną ekspert powinien mieć doświadczenie oraz odpowiednie umiejętności komunikacji pozwalające na werbalne i pisemne wytłumaczenie swoich działań. Wskazane jest także posiadanie przez niego podstawowej wiedzę dochodzeniowej i prawnej związanej z kontekstem sprawy[14];
e) przeszkolenia — jeśli nie jest dostępne wsparcie eksperckie, to dokonujący wyszukania i zatrzymania dowodów elektronicznych musi być właściwie

[12] Prawie identycznie sformułowane zasady można znaleźć w: Jones N. i inni, *Electronic evidence guide — A basic guide for police officers, prosecutors and judges*, CyberCrime@IPA, Version 1.0, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic Evidence Guide/default_en.asp, dostęp: 02.11.2018 r.

[13] Łańcuch dowodowy pozwala na zagwarantowanie, że nikt nieautoryzowany nie miał dostępu do dowodu.

[14] Dyskusję nt. możliwości wykorzystania hakera lub pracownika pokrzywdzonego jako konsultanta można znaleźć w: A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 134–138.

przeszkolony do zabezpieczenia oryginalnych danych, urządzeń elektronicznych, cyfrowych mediów, ich przewiezienia i składowania. Musi zrobić to właściwie prawnie i technicznie, ze znajomością możliwych implikacji jego błędnych działań.

Zabezpieczenia dowodów cyfrowych dokonuje się przez:

a) zatrzymanie całych urządzeń, sprzętu, wyposażenia elektronicznego, mediów, nośników. Do tego rodzaju zabezpieczenia dowodów należy zaliczyć także zatrzymanie zapasowych nośników (tzw. *backupów*), których zwykle należy poszukiwać w innej lokalizacji niż ta, w której znajdował się zabezpieczany sprzęt;
b) przez skopiowanie całych zawartości nośników, wykonanie obrazów i klonów[15];
c) przez wybiórcze kopiowanie danych (np. zawartości skrzynki pocztowej na serwerze pocztowym, logów systemowych).

W przypadkach b) i c) zalecane jest wykonanie dwóch kopii, z których jedna zabezpieczona w obecności świadków będzie przechowywana w prokuraturze, a druga poddana zostanie dalszym badaniom. Kopie powinny być uzupełnione obliczoną wartością jednokierunkowej funkcji skrótu (tzw. *hash*), która powinna zagwarantować, że proces wykonania kopiowania przebiegł poprawnie, a zawartość kopii i oryginału są identyczne (jeżeli *hash* werfikacyjny obliczony z danych oryginalnych i *hash* akwizycyjny obliczony z danych skopiowanych są identyczne). W przyszłości ta wartość będzie służyła do odrzucenia zarzutu modyfikacji materiału dowodowego, jeżeli badany materiał dowodowy będzie miał obliczoną wartość *hash* identyczną, jak materiał zabezpieczony.

Jedna z pierwszych, oficjalnie rozpowszechnionych „dobrych praktyk" dotyczących pozyskiwania i zabezpieczania dowodów cyfrowych opisuje następujące zasady postępowania[16]:

– postępuj zgodnie z Polityką Bezpieczeństwa swojej organizacji, zaangażuj w działania odpowiedni personel ds. obsługi incydentów i z działu prawnego;
– wykonaj najdokładniejszy, jak to możliwe, obraz systemu;
– prowadź szczegółowe notatki zawierające daty i czas wykonanych czynności. Jeżeli jest to możliwe, to prowadź automatyczne generowanie zapisu działań (pamiętaj, że plik wynikowy musi powstać na innym nośniku, niż dowodowy). Notatki i wydruki powinny być podpisane i opatrzone datą;

[15] Klonem określa się wierną kopię (bit po bicie) nośnika dowodowego, wykonaną na innym nośniku, taka sama kopia zapisana w pliku nazywa się obrazem.
[16] RFC 3227, Evidence Collection and Archiving, February 2002, https://www.ietf.org/rfc/rfc3227.txt, dostęp: 06.11.2018 r.

– zanotuj różnicę między zegarem systemowym a czasem UTC (lub lokalnym). Dla każdego zapisu czasu wskazuj, czy to czas UTC, czy czas lokalny;
– bądź przygotowany, że być może kilka lat później, będziesz musiał opisać wszystkie działania, jakie podjąłeś i w jakim czasie (szczegółowe notatki będą wtedy bardzo przydatne);
– minimalizuj zmiany danych podczas ich zbierania. Dotyczy to nie tylko zmian treści, ale także metadanych. Należy unikać aktualizacji czasu dostępu do pliku lub katalogu;
– usuń zewnętrzne możliwości dokonywania zmian;
– w obliczu wyboru między zbieraniem a analizą danych, należy najpierw zbierać, a potem analizować;
– bądź metodyczny, przestrzegaj procedur (powinny być wcześniej przetestowane w celu zapewnienia ich wykonalności), preferuj procedury zautomatyzowane ze względu na ich szybkość i dokładność;
– w odniesieniu do każdego urządzenia należy przyjąć metodyczne podejście, opracowane zgodnie z wytycznymi określonymi w procedurze gromadzenia danych. Zwykle krytycznym elementem będzie czas, więc jeśli liczba urządzeń wymagających zabezpieczenia jest duża, rozdziel pracę na inne osoby, aby zebrać dowody równolegle. Jednak przy zabezpieczaniu jednego systemu działaj krok po kroku;
– zbieraj dowody w kolejności, od najbardziej ulotnych (podatnych na zmianę), do najtrwalszych;
– utwórz kopię bitową nośnika. Unikaj bezpośredniego badania nośnika dowodowego — wszystkie analizy wykonuj na kopii.

Poradnik Ministerstwa Sprawiedliwości USA[17] zwraca uwagę na cztery działania związane z zabezpieczaniem danych cyfrowych (rys. 1):
– zabezpieczenie miejsca — należy podjąć kroki w celu zapewnienia bezpieczeństwa osobom oraz zidentyfikowania i ochrony integralności potencjalnych tradycyjnych i elektronicznych dowodów. Po wstępnej ocenie należy sformułować (zmodyfikować) plan wyszukiwania i identyfikacji potencjalnych dowodów. Wszystkie potencjalne dowody powinny być udokumentowane i/lub sfotografowane. Na tym etapie przeprowadzane są także wywiady;
– dokumentowanie miejsca — należy tworzyć trwały zapis całości miejsca, jakie zauważyli pierwsi zabezpieczający, dokładnie zarejestrować dowody elektroniczne i tradycyjne. Dokładnie nagrać lokalizację i stan komputerów, nośników pamięci, innych urządzeń cyfrowych oraz konwencjonalnych

[17] *Electronic Crime Scene Investigation: A Guide for First Responders*, U.S. Department of Justice, NCJ 187736, July 2001, http://www.ncjrs.org/pdffiles1/nij/187736.pdf, dostęp: 02.11.2018 r.

dowodów. Udokumentować stan systemu komputerowego, w tym stan zasilania komputera (włączony, wyłączony lub w trybie uśpienia). Zidentyfikować i udokumentować powiązane elementy elektroniczne, które nie będą zabezpieczone;

– zbieranie dowodów — należy pozyskać i zabezpieczyć dowody tradycyjne i cyfrowe w taki sposób, aby zachować ich wartość dowodową. Warto zwrócić szczególną uwagę na zapisane hasła, odręczne notatki (czyste kartki z odciśniętym zapisem), podręczniki do sprzętu i oprogramowania, kalendarze, literaturę, wydruki komputerowe oraz fotografie;
– pakowanie, transport i przechowywanie — po zabezpieczeniu dowodów należy je, zachowując odpowiednie środki ostrożności zapakować, przetransportować i zmagazynować, dbając o zachowanie łańcucha dowodowego. Nie wolno podejmować żadnych działań, które mogłyby zmodyfikować lub zniszczyć zabezpieczone urządzenia i dane. W transporcie i magazynowaniu należy unikać wysokich i niskich temperatur, wilgoci, wstrząsów, wibracji, pól elektrostatycznych, pól magnetycznych i wszelkich czynników, na które wrażliwe są zabezpieczone dowody. Dokładnie opisać sporządzoną dokumentację.

Rys. 1. Etapy zabezpieczania dowodów cyfrowych

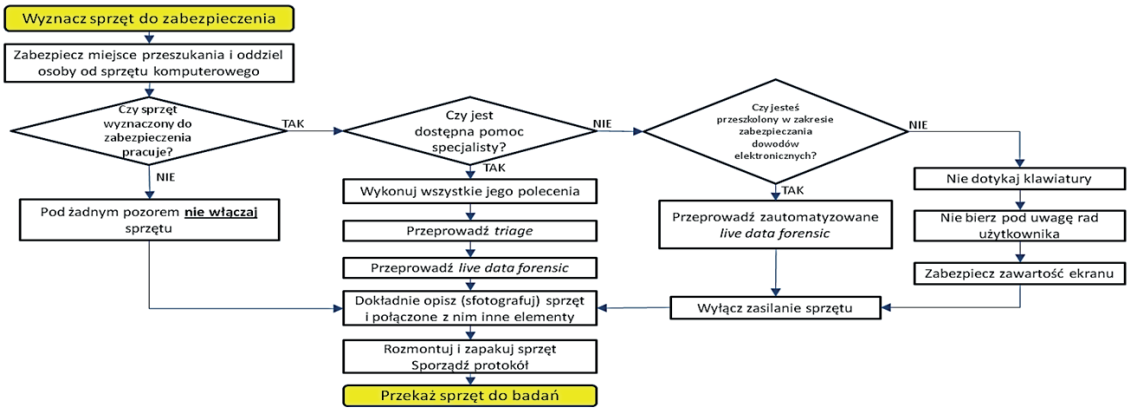
Źródło: Opracowanie własne na podstawie *Electronic Crime Scene Investigation: A Guide for First Responders*, U.S. Department of Justice, 2001.

Rozsądne jest również rozważenie, zalecanych w niektórych „dobrych praktykach”[18], jakie inne rodzaje dowodów, np. DNA lub odciski palców mogą być przydatne (np. z telefonu lub karty płatniczej).

[18] Na przykład ACPO Good Practice Guide for Digital Evidence, Association of Chief Police Officers, Version 5, 2011, http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf, dostęp 06.11.2018 r.

Propozycje

Bardzo często, kluczowym dla poprawnego i optymalnego zabezpieczenia danych cyfrowych jest wykonanie rozpoznania przedmiotowo-podmiotowego. W zależności od tego, jaki jest cel przeszukania, co będzie poszukiwane, jakiego rodzaju sprzęt i oprogramowanie mogą zostać zastane na miejscu przeszukania oraz jaką wiedzą dysponuje dysponent tego sprzętu i oprogramowania, podejmowana jest decyzja, w jaki sposób przeprowadzić przeszukanie i zabezpieczenie, z jakich narzędzi skorzystać i jakie wsparcie eksperckie jest niezbędne. W wyniku rozpoznania opracowywany jest wniosek o wydanie postanowienia o przeszukaniu i sporządzany plan przeszukania. W większości przypadków prawidłowo wykonane rozpoznanie i sporządzony plan przeszukania pozwalają skutecznie ujawnić i zabezpieczyć dowody cyfrowe.



Rys. 2. Uproszczona procedura zabezpieczania sprzętu komputerowego

Źródło: opracowanie własne.

Zawsze działania zmierzające do przeszukania i zabezpieczenia danych rozpoczyna się od prewencyjnego zabezpieczenia i przejęcia kontroli nad pomieszczeniem i znajdującymi się tam osobami. Dzięki temu uzyskuje się pewność, że w czasie realizowanych dalszych działań nie pojawią się zagrożenia życia i zdrowia funkcjonariuszy lub innych uczestniczących w nich osób. Kolejne podejmowane działania mają za zadanie zminimalizowanie ryzyka celowego zmodyfikowania lub zniszczenia dowodów przez osoby znajdujące się w przeszukiwanym pomieszczeniu (poprzez uniemożliwienie im korzystania ze sprzętu elektronicznego) lub ich zdalnego zmodyfikowania lub zniszczenia (poprzez odłączenie urządzeń od łączy komunikacyjnych). Po wyznaczeniu sprzętu podlegającego zabezpieczeniu następuje techniczne pozyskanie i za-

bezpieczenie materiału dowodowego. Sposób pozyskania danych cyfrowych jest uzależniony od sposobu ich przechowywania na nośnikach danych i ich charakteru — może obejmować odczytanie żądanych danych z nośnika, skopiowanie wybranych danych, skopiowanie wszystkich danych lub zabezpieczenie urządzenia. Ten sposób zależy także od umiejętności przeprowadzającego zabezpieczenie, posiadanej pomocy specjalistycznej i możliwych do użycia narzędzi i materiałów (rys. 2).

Od wielu lat dyskutowany jest sposób postępowania z zabezpieczanym komputerem (laptopem, tabletem) — czy i jak wyłączyć jego zasilanie. Oczywiście wyłączonego komputera nie należy włączać. Jeżeli komputer sprawia wrażenie wyłączonego, należy to zweryfikować, np. poruszając myszą, obserwując diody. Pamiętać należy, że niektóre komputery przenośne mogą włączyć się przy otwieraniu pokrywy. W przypadku, kiedy komputer działa, a nie można zasięgnąć porady eksperta, trzeba rozważyć jakie działanie przyniesie mniej szkód. W przypadku „zwykłych użytkowników", kiedy nie podejrzewamy ich o szyfrowanie danych i posiadanie zaawansowanych systemów operacyjnych, takim działaniem jest wyjęcie kabla zasilającego z gniazda komputera (lub wyjęcie akumulatora). W przeciwnym przypadku, przed wyłączeniem zasilania należy obowiązkowo wykonać procedury zabezpieczające dane ulotne (opisane dalej).

Powyższy problem jest istotnym także w przypadku telefonów i smartfonów. Jeśli urządzenie jest włączone, w większości przypadków należy je wyłączyć. Pozwoli to na odizolowanie urządzenia od odbierania sygnałów z sieci, które mogłyby wprowadzić zmiany w danych zapisanych w urządzeniu (w skrajnym przypadku zdalnie usunąć dane). W wyjątkowych okolicznościach można podjąć decyzję o pozostawieniu urządzenia włączonego, kiedy wymagany jest natychmiastowy dostęp do danych w nim zawartych. Rozważyć może wówczas przechowywanie urządzenia w klatce Faraday lub wykorzystanie zagłuszacza telefonii komórkowej.

Ostatecznym efektem tego etapu jest zatrzymanie sprzętu, nośników i/lub zabezpieczenie danych. W trakcie wszystkich działań sporządzana jest dokumentacja procesowa i kryminalistyczna.

Zmiany technologiczne, w szczególności wykorzystywanie przez przestępców systemów operacyjnych live[19], wirtualnych maszyn i pełnego szyfrowania nośników, a także potrzeba natychmiastowego uzyskania wyników (np. przy zagrożeniu bombowym lub życia) wymusiły wprowadzenie do przedstawionego powyżej, tradycyjnego modelu przeszukania i zabezpieczenia danych

[19] Terminem tym określa się system operacyjny uruchamiany z nośnika wymiennego (np. płyty CD/DVD, pamięci USB) i rezydujący w pamięci RAM. System taki nie wymaga instalacji na dysku twardym i może nie zapisywać trwale żadnych danych.

nowego elementu — przeszukania działającego systemu (ang. *live data forensic*) pozwalającego zabezpieczyć dane ulotne[20]. Ulotność danych w zależności od ich nośnika została przedstawiona w tabeli 1.

Tabela 1. Ilustracja wysokiego prawdopodobieństwo usunięcia, nadpisania lub zmiany danych

Rodzaj danych	Ulotność
Rejestry, pamięci cache, pamięci robocze urządzeń	Nanosekundy
Pamięć operacyjna	Dziesiątki nanosekund
Stan sieci	Milisekundy
Działające procesy	Sekundy
Pamięci dyskowe	Minuty
Nośniki backupowe i archiwalne	Lata
CD-ROM-y, wydruki	Dziesiątki lat

Źródło: opracowanie własne na podstawie: D. Farmer, W. Venema, *Forensic Discovery*, Addison-Wesley 2005.

Live data forensic nie gwarantuje nieingerowania w zabezpieczane dane, w zamian jednak pozwala uzyskać dane, które byłyby niedostępne (lub trudnodostępne) po wyłączeniu komputera, np. dane szyfrowane czy znajdujące się w pamięci RAM. Przy takich działaniach wzrasta znaczenie starannego dokumentowania wszelkich czynności wykonywanych na zabezpieczanym urządzeniu. Olbrzymie pojemności współczesnych nośników danych wymagają wstępnej selekcji materiału (ang. *triage*[21]), który należy poddać analizie. Zatrzymać trzeba maksymalnie dużą część materiału do późniejszych badań, ale do analizy wybrać tylko te miejsca, obszary informacyjne, które są natychmiast potrzebne, gdyż mogą potwierdzić lub odrzucić postawione hipotezy. Pojęcie *triage* staje się określeniem na początkowe i szybkie działania w różnych obszarach pozyskiwania i zabezpieczania danych, np. w Internecie rzeczy, kradzieżach tożsamości i dokumentów, posiadaniu pornografii dziecięcej. *Triage* i *live data forensic* mogą być oparte wyłącznie na wykorzystaniu doświadczenia przeszukującego i jego narzędzi[22], ale można je także dokonać

[20] Dane, które są zapisane cyfrowo w taki sposób, że istnieje bardzo duże prawdopodobieństwo ich usunięcia, zastąpienia lub zmodyfikowania w krótkim czasie przez człowieka lub zautomatyzowany proces.

[21] W informatyce śledczej terminem *triage* określa się selekcję i zabezpieczanie tylko tych danych, które są istotne dla sprawy. Zastosowanie *triage* pozwala ograniczyć czas potrzebny na zabezpieczenie i analizę danych.

[22] Dobre przykłady takiego postępowania zawarte są w publikacji: A.M. Kalinowski, *Metody inwigilacji i elementy informatyki śledczej*, Kwidzyn 2011. Propozycję podstawowych narzędzi

za pomocą systemów automatyzujących (np. *OSTriage*[23]). Zaletą systemów automatyzujących przeszukanie jest rejestrowanie wszystkich działań funkcjonariusza i otrzymywanych wyników. Korzystając z *triage* i *live data forensic* można osiągnąć kompromis pomiędzy trzema potrzebami:
– rozpoznaniem — trzeba znaleźć maksymalnie dużo dowodów;
– odpowiedniością — zachować je w sposób jak najlepszy;
– wiarygodnością — powiązać je w łańcuchu dowodowym.

Zarówno ten kompromis, jak i rozdzielenie etapów przygotowania narzędzia, wykorzystania narzędzia do pozyskania danych oraz analizy pozyskanych w trakcie przeszukania danych do osobnych procesów spełniają zalecenia metodyk i ramy FORZA[24]. Zaletą stosowania tej metodyki przy przeszukaniu jest maksymalne wykorzystanie ekspertów w pierwszej fazie — tworzenia narzędzia, i ostatniej — analizy wyników, pozostawiając najbardziej czasochłonne zadanie pozyskania danych osobom zaledwie przeszkolonym do wykorzystania narzędzia.

W nowoczesnych środowiskach IT dane nie zawsze są przechowywane i przetwarzane na urządzeniach dostępnych lokalnie. Szeroki zakres usługodawców oferuje tanie, a nawet bezpłatne przechowywanie i przetwarzanie potężnych zasobów na zdalnych systemach. Dane nie muszą być wówczas przetwarzane i przechowywane na tym samym fizycznym komputerze. Wykorzystanie „cienkich" klientów[25] bez jakiejkolwiek pamięci trwałej sprawia, że zabezpieczane dane znajdują się w zasobach wirtualnych maszyn w chmurze. Może się zdarzyć, że nawet dostawca usługi nie będzie w stanie powiedzieć, gdzie pewne dane, które mogą stanowić dowody, są przechowywane. Jeśli w trakcie przeszukania okaże się, że organ dokonujący przeszukania musi dostać się do zasobów połączonego siecią komputera znajdującego się w pomieszczeniu, które nie jest objęte postanowieniem o przeszukaniu, organ może skorzystać z prawa do przeszukania bez postanowienia sądu lub prokuratora. Identycznie dzieje się w przypadku, gdy przeszukiwany komputer połączony

do zabezpieczania danych ulotnych można znaleźć w J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin 2015, s. 201–202.

[23] Program autorstwa Erica Zimmermana.

[24] FORZA (FORensics ZAchman framework) — metodyka prowadzenia przeszukania systemu komputerowego zgodna z przepisami prawa amerykańskiego. Więcej o FORZA w: *R.S.C. Ieong, FORZA — Digital forensics investigation framework that incorporate legal issues*, Digital investigation 3 (Supplement-1)/2006, s. 29–36.

[25] Ang. *thin client* oznacza technologię alternatywną dla tradycyjnego komputera PC opartą o aplikacje działające w architekturze klient-serwer. Terminale graficzne tej technologii służą wyłącznie jako urządzenia wejścia-wyjścia, a wszystkie operacje są wykonywane na wirtualnych serwerach.

jest z odległym komputerem[26]. W tym przypadku dane z odległego komputera mogą zostać zabezpieczone poprzez przekopiowanie ich na lokalny dysk. Jak wcześniej wspomniano takie przeszukanie nie jest czynnością procesową, tylko operacyjno-rozpoznawczą.

Podsumowanie

Pozyskanie i zabezpieczenie danych cyfrowych powinno być przeprowadzane zgodnie z wcześniej opracowanymi procedurami, najlepiej przy wsparciu specjalisty. Z wykonanych czynności musi być sporządzony protokół (art. 143 § 1 pkt 3, 6 i 7 k.p.k.), w którym odnotowuje się przeprowadzone czynności, parametry identyfikujące zabezpieczane oprogramowanie i sprzęt, sposób utrwalenia danych oraz informacje na temat indywidualnych oznaczeń nośników, na których dane zostały utrwalone. Niestety nie ma jednej uniwersalnej metodyki tych działań. Ze względu na dużą różnorodność urządzeń zawierających dane cyfrowe oraz zróżnicowane potrzeby pozyskania i zabezpieczenia danych cyfrowych można jedynie posiłkować się dobrymi praktykami oraz sugestiami zawartymi w dokumentach normatywnych.

Bibliografia

1. *ACPO Good Practice Guide for Digital Evidence*, Association of Chief Police Officers, Version 5, 2011, http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf.
2. Adamski A., *Prawo karne komputerowe*, Warszawa 2000.
3. *Electronic Crime Scene Investigation: A Guide for First Responders*, U.S. Department of Justice, NCJ 187736, July 2001, http://www.ncjrs.org/pdffiles1/nij/187736.pdf.
4. Farmer D., Venema W., *Forensic Discovery*, Addison-Wesley 2005.
5. Ieong R.S.C., *FORZA — Digital forensics investigation framework that incorporate legal issues*, Digital investigation 3 (Supplement-1)/2006.
6. Jones N. i inni, *Electronic evidence guide — A basic guide for police officers, prosecutors and judges*, CyberCrime@IPA, Version 1.0, http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic Evidence Guide/default_en.asp.
7. Kalinowski A.M., *Metody inwigilacji i elementy informatyki śledczej*, Kwidzyn 2011.
8. Konwencja Rady Europy o cyberprzestępczości.
9. Kosiński J., *Paradygmaty cyberprzestępczości*, Difin 2015.
10. Lach A., *Dowody elektroniczne w procesie karnym*, Toruń 2004.
11. Lach A., *Przeszukanie na odległość systemu informatycznego*, „Prokuratura i Prawo" nr 9/2011.

[26] Aktualnie obowiązujące przepisy uniemożliwiają — bez skierowania wniosku o pomoc prawną — dokonanie przeszukania na odległość w przypadku ustalenia, że urządzenie lub zasoby znajdują się poza granicami kraju.

12. PN ISO/IEC 27000:2014-11 Technika informatyczna — Techniki bezpieczeństwa — Systemy zarządzania bezpieczeństwem informacji — Przegląd i terminologia.
13. PN ISO/IEC 27001:2014-12 Technika informatyczna — Techniki bezpieczeństwa — Systemy zarządzania bezpieczeństwem informacji — Wymagania.
14. PN ISO/IEC 27002:2014-12 Technika informatyczna — Techniki bezpieczeństwa — Praktyczne zasady zabezpieczania informacji.
15. PN-EN ISO/IEC 27037:2016-12 Technika informatyczna — Techniki bezpieczeństwa — Wytyczne do identyfikacji, gromadzenia, pozyskiwania i zachowania śladów cyfrowych (dowodowych).
16. PN-EN ISO/IEC 27041:2016-12 Technika informatyczna — Techniki bezpieczeństwa — Wytyczne do zapewnienia stosowności i adekwatności metody dochodzeniowej w związku z incydentem.
17. PN-EN ISO/IEC 27042:2016-12 Technika informatyczna — Techniki bezpieczeństwa — Wytyczne do analizy i interpretacji śladu cyfrowego (dowodowego).
18. PN-EN ISO/IEC 27043:2016-12 Technika informatyczna — Techniki bezpieczeństwa — Pryncypia i procesy w dochodzeniach związanych z incydentami.
19. PN-EN ISO/IEC 30121:2016-12 Technika informatyczna — Nadzór nad strukturą ryzyka związanego z informatyką śledczą.
20. Rekomendacja RE R(95)13 w sprawie problemów prawa karnego procesowego związanych z technologią informatyczną.
21. RFC 3227, Evidence Collection and Archiving, February 2002, https://www.ietf.org/rfc/rfc3227.txt.
22. Ustawa z dnia 6 czerwca 1997 r. — Kodeks postępowania karnego.
23. Waltoś S., *Proces karny. Zarys systemu*, Warszawa 2009.

Fundamentals of the digital data seizure and protection as a part of the response to security breaches

Abstract

This chapter provides a concise overview of normative acts and good practices related to the seizure and preservation of digital data.

Keywords: digital data, security breaches, traces, security, live forensic.