Piotr Karasek

ORGANY ŚCIGANIA WOBEC PROBLEMU KRYPTOGRAFICZNEGO UKRYCIA DOWODÓW CYFROWYCH

Law enforcement towards the problem of cryptographic hiding of digital evidence

Ogólnie pojęte technologie informacyjne, komputery i Internet stanowią podstawę funkcjonowania współczesnych społeczeństw. Wiąże się to z koniecznością przetwarzania i przechowywania ogromnych ilości danych w postaci cyfrowej. W związku z tym, że do środowiska komputerowego przenoszonych jest obecnie coraz więcej danych wrażliwych, konieczne jest zapewnienie ochrony przed nieuprawnionym dostępem do nich. Dane cyfrowe w coraz większym stopniu są dobrem, które trzeba chronić, gdyż zdobycie prywatnych informacji przez obce osoby może doprowadzić do poważnych strat materialnych lub moralnych, nie wspominając o szkodach, jakie może przynieść nieplanowane ujawnienie informacji krytycznych z punktu widzenia interesów państwa[1]. Dlatego też od lat opracowywane i doskonalone są kryptograficzne techniki zabezpieczania danych cyfrowych. Techniki zabezpieczania informacji przed dostępem niepowołanych do tego osób trzecich, jakie daje nauka kryptografii, mają wiele praktycznych zastosowań we współczesnym świecie. Rozwiązania tego typu stały się już jakiś czas temu bardzo popularne w dużych przedsiębiorstwach pragnących chronić swoje tajemnice, a także wśród osób fizycznych chcących chronić własną prywatność. Można przewidywać, że skala zastosowania narzędzi kryptograficznych będzie jedynie wzrastać[2]. Tworzenie i stosowanie szyfrów do ukrycia informacji nie jest oczywiście niczym nowym ani niepożądanym, należy jednak zwrócić uwagę także na niezamierzony skutek rozwoju cyfrowych narzędzi kryptograficznych, jakim jest korzystanie z nich przez sprawców przestępstw.

W wyniku rozwoju i rozpowszechnienia się technologii komputerowych w codziennym życiu społeczeństw poważnym zagrożeniem stała się szeroko poję-

[1] B. Hołyst, J. Pomykała, *Kryptograficzna ochrona informacji w kryminalistyce*, „Problemy Kryminalistyki" 2011, nr 272, s. 6–7.

[2] Zob. Ponemon Institute, *2010 Annual Study:* UK Enterprise *Encryption Trends*, http://www.symantec.com/content/en/us/about/media/pdfs/Symc_Ponemon_Encryption_Trends_report_Nov2010.pdf, dostęp z dnia 03.03.2014.

ta przestępczość komputerowa. Z nią zaś wiąże się pojęcie dowodów cyfrowych obecnych w komputerze sprawcy i konieczność ich zabezpieczenia oraz analizy[3]. Selektywne usunięcie z systemu informatycznego wszystkich informacji mogących stanowić dowód przestępstwa spośród innych obecnych w systemie danych jest zadaniem skomplikowanym i dającym niepewne rezultaty. Wobec tego problemu wielu sprawców przestępstw komputerowych decyduje się nie tyle na niszczenie cyfrowych dowodów swojej działalności, co na uczynienie takich danych niedostępnymi dla organów ścigania z wykorzystaniem dostępnych narzędzi kryptograficznych. W efekcie te same metody szyfrujące, które mają służyć ochronie danych przed sprawcami przestępstw, są przez nich stosowane do ukrycia dowodów swojej działalności i uniknięcia odpowiedzialności karnej.

Ponieważ sprawcy przestępstw komputerowych coraz częściej szyfrują nośniki danych, dla lepszego zrozumienia tego problemu i jego konsekwencji dla postępowania karnego konieczne jest zapoznanie się z podstawowymi informacjami na temat kryptografii. Najprościej można ją określić mianem nauki o szyfrowaniu, a więc o przekształcaniu informacji do postaci niezrozumiałej dla każdego, kto nie zna odpowiedniego klucza, i o tworzeniu szyfrów. Wraz z kryptoanalizą, czyli nauką o przełamywaniu istniejących już szyfrów, stanowi ona część szerszej dziedziny, jaką jest kryptologia[4]. Jak słusznie zauważyli Niels Ferguson i Bruce Schneier, „kryptografia jest piekielnie trudna”[5], dlatego też na potrzeby niniejszego tekstu jej omówienie ma skrótowy i uproszczony charakter.

Istotą kryptograficznego zabezpieczenia danych przed dostępem do nich osób niepożądanych jest zastosowanie określonego algorytmu szyfrującego (szyfru), za pomocą którego tekst jawny jest przekształcany do postaci zaszyfrowanej i odwrotnie. Algorytm szyfrujący można postrzegać jako funkcję matematyczną, według której przekształcana jest określona treść[6]. Współcześnie panuje przekonanie, że dobry algorytm szyfrujący nie powinien być tajny, za czym przemawia szereg argumentów. Po pierwsze, jeżeli bezpieczeństwo szyfrowania miałoby zależeć od tajności zastosowanego algorytmu, to szyfr taki mógłby być stosowany wyłącznie w ograniczonej grupie użytkowników, a opuszczenie grupy przez któregokolwiek z nich wiązałoby się z koniecznością zmiany algorytmu[7]. Po drugie, utajnienie algorytmu tylko pozornie zwiększa poziom bezpieczeństwa danych, gdyż uniemożliwia ono sprawdzenie szyfru przez niezależnych specjalistów w poszukiwaniu błędów, zanim nastąpi ewentualny atak[8]. Kwestia bezpieczeństwa współczesnych systemów kryptograficznych rozwiązana jest, zgodnie z za-

[3] Zob. A. Adamski, *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000, s. 30–34.
[4] C. Kościelny, M. Kurkowski, M. Srebrny, *Kryptografia – teoretyczne podstawy i praktyczne zastosowania*, Wydawnictwo Polsko-Japońskiej Wyższej Szkoły Technik Komputerowych, Warszawa 2009, s. 1.
[5] N. Ferguson, B. Schneier, *Kryptografia w praktyce*, Helion, Gliwice 2004, s. 28.
[6] C. Kościelny, M. Kurkowski, M. Srebrny, op. cit., s. 2–3.
[7] Tamże, s. 3.
[8] N. Ferguson, B. Schneier, op. cit., s. 32.

sadą Kreckhoffsa[9], w ten sposób, że do wykorzystania z zasady jawnej funkcji szyfrującej konieczny jest dodatkowy element, tzw. klucz kryptograficzny. W istocie jest on dodatkową zmienną w funkcji szyfrującej, z tym że unikalną dla każdego zastosowania szyfru. Klucz szyfrujący ma w praktyce postać ciągu znaków i może przyjąć jedną z wielu wartości, których przedział nazywa się „przestrzenią klucza" (ang. *keyspace*)[10]. Intruz pragnący uzyskać dostęp do zaszyfrowanych informacji może znać zasadę działania szyfru, ale dane pozostaną dla niego niedostępne, o ile nie wykaże się on znajomością klucza. Spośród algorytmów stosujących tę metodę można wyodrębnić dwie zasadnicze grupy. Jedną z nich są tzw. algorytmy z kluczem jawnym, które wykorzystują dwa różne klucze, jawny (publiczny) klucz szyfrujący i tajny (prywatny) klucz deszyfrujący. Drugą grupę stanowią tzw. algorytmy symetryczne, w których do szyfrowania i deszyfrowania wykorzystany jest ten sam klucz (lub klucz deszyfrujący, który da się łatwo wyznaczyć z klucza szyfrującego i na odwrót)[11]. Do zabezpieczania nośników danych praktyczniejsze zastosowanie mają algorytmy symetryczne. Obecnie jednym z najpowszechniej stosowanych jest algorytm o nazwie Rijndael, pełniący funkcję amerykańskiego rządowego standardu szyfrującego AES (*Advanced Encryption Standard*). Algorytm ten został wyłoniony w wyniku otwartego konkursu ogłoszonego przez amerykański Narodowy Instytut Normalizacyjny i Techniczny (NIST)[12] i jest on zatwierdzony do wykorzystania w amerykańskich agencjach rządowych i w sektorze prywatnym, bez ograniczeń licencyjnych[13].

Metody przeprowadzania ataków mających na celu uzyskanie dostępu do zaszyfrowanych danych bez znajomości prawidłowego klucza mogą być różne. Trzeba podkreślić, że im dłuższy jest klucz i im „silniejszy" algorytm szyfrujący, tym mocniejsze jest całe szyfrowanie[14,15]. Algorytm, którego złamanie jest możliwe jedynie teoretycznie i dla którego nie ma lepszej znanej metody odszyfrowania danej treści niż sprawdzanie kolejnych możliwych wartości klucza kryptograficznego, możemy nazwać bezpiecznym[16], a odkrycie sposobu jego obejścia oznaczałoby kompromitację wszystkich jego zastosowań. Można zresztą przyjąć

[9] Zasada ta stanowi, że „Tajność szyfru zapewniana jest przez tajność klucza szyfrowania, a nie algorytmu szyfrowania", za: D. Sklyarov, *Łamanie zabezpieczeń programów*, RM, Warszawa 2004, s. 39.

[10] N. Ferguson, B. Schneier, op. cit., s. 3–4.

[11] M.R. Ogiela, *Podstawy kryptografii*, AGH, Kraków 2000, s. 10–11.

[12] N. Ferguson, B. Schneier, op. cit., s. 55.

[13] C. Kościelny, M. Kurkowski, M. Srebrny, op. cit., s. 85–86.

[14] B. Schneier, *Kryptografia dla praktyków*, Wydawnictwa Naukowo-Techniczne, Warszawa 2002, s. 207.

[15] Zastosowanie bardzo dużej przestrzeni klucza jest koniecznym warunkiem bezpieczeństwa danego szyfrowania, jednakże nie jest to warunek jedyny. Sam szyfr może być na tyle słaby, że pomimo zastosowania odpowiedniego klucza okaże się podatny na zupełnie innego rodzaju ataki. Zob. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Kryptografia stosowana*, Wydawnictwa Naukowo-Techniczne, Warszawa 2005, s. 67.

[16] Teoretycznie możliwe jest złamanie każdego szyfru. Zob. M.R. Ogiela, op. cit., s. 13.

założenie, że łamanie nowoczesnych algorytmów szyfrujących nie znajduje się w zasięgu możliwości organów ścigania, ani też nie stanowi ich zadania. Zasadniczo więc, aby uzyskać dostęp do zaszyfrowanych danych, organy ścigania stoją przed wyzwaniem odnalezienia prawidłowego klucza kryptograficznego wykorzystanego w danym przypadku lub muszą w inny sposób doprowadzić do zdobycia danych w formie niezaszyfrowanej.

Metody ataków kryptoanalitycznych mogą się różnić w zależności od tego, jakimi wyjściowymi danymi będzie dysponował atakujący. Warto skrótowo wskazać, na czym polegają niektóre z nich, by móc ocenić, przed jakim wyzwaniem mogą stanąć organy ścigania dysponujące cyfrowym materiałem dowodowym w formie zaszyfrowanej.

Zasadniczo można wskazać, że kryptoanalityk będzie zmierzał do odtworzenia jawnego tekstu na podstawie kryptogramu lub do poznania klucza kryptograficznego. Zwykle oceniając poziom bezpieczeństwa danego szyfrowania, bierze się pod uwagę kilka popularnych modeli ataków. Pierwszym z nich jest atak przy użyciu wyłącznie tekstu tajnego. W takiej sytuacji znana jest jedynie zaszyfrowana forma treści informacji, a tekst jawny lub klucz może być dedukowany wyłącznie na jej podstawie. Wygodniejsza dla kryptoanalityka jest możliwość zastosowania ataku z użyciem tekstu jawnego, w którym oprócz zaszyfrowanej wersji jest znany pewien fragment tekstu jawnego. Kolejne metody także mogą bazować na posiadaniu fragmentu tekstu jawnego, ale dodatkowa wiedza może polegać na przykład na tym, że znany jest konkretny fragment jawny i odpowiadająca mu część w formie zaszyfrowanej[17]. Istnieją także bardziej specyficzne metody ataków, jednak zwykle będą one odgrywały mniejszą rolę wobec problemu uzyskania dostępu do zaszyfrowanych danych w postępowaniu karnym.

Poznanie klucza kryptograficznego przy zastosowaniu ataku ze znanym tekstem jawnym jest znacznie prostsze niż wtedy, gdy znana jest jedynie treść informacji w zaszyfrowanej formie[18]. W najgorszym przypadku organy ścigania nie będą jednak dysponować niczym więcej niż tylko w pełni zaszyfrowanym nośnikiem danych zabezpieczonych u podejrzanego i staną przed wyzwaniem odgadnięcia prawidłowego klucza. Przestrzeń klucza jest często bardzo duża, jednak skończona, dlatego teoretycznie możliwe jest sprawdzanie kolejno różnych kombinacji znaków klucza, aż do odnalezienia prawidłowej wartości.

Próby odgadnięcia klucza metodą siłową (ang. *brute force attack*), polegającą na faktycznym sprawdzaniu kolejno wszystkich możliwych kombinacji znaków, są jednak z zasady skazane na porażkę. Jak wskazano wcześniej, klucz kryptograficzny może przyjąć jedną z wielu wartości znajdujących się w przestrzeni klucza. Przestrzeń ta może być bardzo niewielka, co przekłada się na liczbę możliwych kombinacji znaków. Klucz 8-bitowy posiada jedynie 256 możliwych

[17] O metodach ataków kryptoanalitycznych zob. R. Wobst, *Kryptologia – łamanie i budowa zabezpieczeń*, RM, Warszawa 2002, s. 49 i n., por. N. Ferguson, B. Schneier, op. cit., s. 37–41 i M.R. Ogiela, op. cit., s. 12–13.

[18] N. Ferguson, B. Schneier, op. cit., s. 37–41.

kombinacji znaków i jest łatwy do odgadnięcia. Liczba możliwych kombinacji rośnie jednak wykładniczo. Odpowiednio dłuższy klucz 128-bitowy posiada 2^{128} kombinacji znaków. Klucz o długości 256 bitów to odpowiednio 2^{256} kombinacji. Wspomniany wcześniej publicznie dostępny szyfr AES umożliwia skorzystanie z szyfrowania 256-bitowego, które współcześnie nadal uważa się za bezpieczne. Wyczerpujące przeszukanie tego rzędu przestrzeni klucza jest obliczeniowo niewykonalne[19]. Moc obliczeniowa potrzebna do przeszukania całej lub choćby większej części przestrzeni takiego klucza znacznie przekracza aktualne możliwości techniczne, a czas do tego potrzebny bywa porównywany z szacowanym wiekiem całego Wszechświata[20]. I chociaż moc obliczeniowa komputerów stale rośnie, nie wydaje się, aby w najbliższej przyszłości było możliwe uzyskanie jej wartości wystarczającego rzędu[21]. Ponadto projektanci rozwiązań kryptograficznych nie pozostają obojętni wobec rozwoju technologicznego i również dostosowują do niego proponowane rozwiązania, m.in. przez zwiększanie przestrzeni stosowanych kluczy. Być może kwestię tę odmieni zastosowanie technologii kwantowej w informatyce, jednakże nie jest to dotychczas rozwiązanie dostępne w praktyce[22].

Oczywiście konieczność korzystania z bezpośredniej metody *brute force* stanowi najgorszy możliwy scenariusz. Istnieją jednak sposoby optymalizacji tego rodzaju ataku, tak aby odpowiednio zmniejszyć liczbę koniecznych do przeprowadzenia dopasowań. Przykładem może być tzw. atak słownikowy. Sam fakt, że konkretny klucz kryptograficzny ma teoretycznie ogromną liczbę możliwych kombinacji, nie oznacza jeszcze, że konkretny użytkownik odpowiednio to wykorzystał. Szczególnie gdy weźmie się pod uwagę, iż często w praktyce klucz kryptograficzny nie jest wygenerowany przez komputer, ale przybiera postać hasła ustalonego przez użytkownika. Programy wykorzystywane do szyfrowania danych umożliwiają zwykle wprowadzenie własnego hasła, które służy do odblokowania „prawdziwego" klucza, co ma służyć wygodzie użytkownika. Można wówczas liczyć na to, że tego rodzaju hasło będzie składało się z mniejszej liczby i bardziej popularnych znaków, także ze słów występujących w języku naturalnym. Warto też wziąć pod uwagę pewne przyzwyczajenia ludzi przy ustalaniu haseł (na przykład duże litery tylko na początku wyrazów, a cyfry na końcu lub na początku). Na tych podstawach można stworzyć odpowiedni „słownik" najpopularniejszych przy tworzeniu haseł zwrotów, znaków i sposobów ich łączenia, i starać się w ten sposób ograniczyć przestrzeń klucza. Do odnalezienia hasła

[19] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, op. cit., s. 67.
[20] Zob. B. Schneier, op. cit., s. 208, 211; M.R. Ogiela, op. cit., s. 13.
[21] Ogólnie na temat długości klucza kryptograficznego w kontekście metody *brute force* zob. B. Schneier, op. cit., s. 208–211.
[22] O informatyce i kryptografii kwantowej zob. J. Klamka, M. Sobota, *Kryptografia kwantowa*, w: A. Grzywak, J. Klamka, A. Kapczyński, M. Sobota, *Współczesne problemy bezpieczeństwa informacji*, Wyższa Szkoła Biznesu, Dąbrowa Górnicza 2008, s. 103–159.

w takim przypadku wystarczy sprawdzić znacznie mniej kombinacji[23]. Niemniej jednak należy podkreślić, że także siłowy atak zmierzający do odnalezienia prawidłowego klucza lub hasła będzie często skazany na porażkę.

Skuteczność omawianych zabezpieczeń jest bardzo duża, nie jest więc zaskakujące, że także środowisko przestępcze stosuje te techniki w coraz większym zakresie. Warto wziąć pod uwagę, że obecnie nieskomplikowane w obsłudze oprogramowanie umożliwiające domowe zastosowanie najnowocześniejszych algorytmów szyfrujących jest dostępne legalnie i nieodpłatnie w Internecie, a także coraz częściej stanowi integralny element systemów operacyjnych[24]. Oprócz szyfrowania z poziomu oprogramowania wielu producentów sprzętu komputerowego wprowadza do sprzedaży nośniki danych wykorzystujące wbudowane tzw. szyfrowanie sprzętowe[25]. Szczególną uwagę warto zwrócić na możliwości, jakie daje popularny TrueCrypt, darmowe oprogramowanie szyfrujące z otwartym kodem źródłowym opracowane przez TrueCrypt Foundation[26]. Umożliwia on stosowanie silnych algorytmów szyfrujących (m.in. AES) z wykorzystaniem 256-bitowego klucza do zaszyfrowania zarówno pojedynczych plików, jak i całych partycji lub dysków, gdzie dane są szyfrowane i deszyfrowane w czasie rzeczywistym podczas korzystania z nich. Dodatkowo możliwe jest stworzenie ukrytych zaszyfrowanych obszarów dysku lub nawet ukrytego systemu operacyjnego, tak że samo jego istnienie może pozostać ukryte przed analizującymi dane osobami[27]. Ponadto ponieważ program ten co do zasady nie pozostawia wyraźnych oznak szyfrowania danych, takie pliki analizowane z zewnątrz mogą być omyłkowo potraktowane jak wygenerowane losowo dane, na przykład pozostałe po formatowaniu dysku[28]. Między innymi z tych względów jest to jedno z najskuteczniejszych narzędzi służących uniknięciu odpowiedzialności karnej w wypadku przestępstw komputerowych.

---

[23] R. Wobst, op. cit., s. 54.

[24] Na przykład program szyfrujący BitLocker, stworzony przez Microsoft, stanowi obecnie element niektórych dystrybucji systemu Windows, zob. http://windows.microsoft.com/pl-l/windows7/products/features/bitlocker, dostęp z dnia 03.03.2014.

[25] Taki sprzęt jest nadal odpowiednio droższy, jednak można spodziewać się wzrostu jego popularności. Jego produkcją i dystrybucją zajęła się m.in. firma Kingston, jeden z wiodących producentów przenośnych pamięci USB, zob. http://www.kingston.com/us/usb/encrypted_security/hardware_vs_software, dostęp z dnia 03.03.2014.

[26] Zob. Truecrypt.org, dostęp z dnia 02.03.2014.

[27] A.M. Balogun, S.Y. Zhu, *Privacy impacts of data encryption on the efficiency of digital forensics technology*, „International Journal of Advanced Computer Science and Applications" 2013, t. 4, nr 5, s. 38.

[28] S. Lowman, *The Effect of File and Disc Encryption on Computer Forensics*, 2010, http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf, dostęp z dnia 02.03.2014, s. 5.

Jak już wskazano, natura rozwiązań kryptograficznych rzadko pozwala na siłowe uzyskanie dostępu do zaszyfrowanych danych, bez znajomości klucza kryptograficznego lub hasła. W tym kontekście § 69 pkt 10 Wytycznych numer 3 Komendanta Głównego Policji, który stanowi, że „gdy zasoby przeszukiwanego systemu […] są zaszyfrowane i niemożliwe jest zapoznanie się z nimi bez podania hasła lub klucza prywatnego, można użyć urządzeń lub programów komputerowych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym”[29], wydaje się pozbawiony faktycznej skuteczności. Trzeba jednak poszukiwać metod, dzięki którym organy śledcze mogłyby omijać takie zabezpieczenia. Należy przy tym rozróżnić dwie możliwe sytuacje, w jakich prowadzący śledztwo mogą stanąć przed omawianym zadaniem. Po pierwsze, zaszyfrowane mogą być tylko niektóre dane na ogólnie niezaszyfrowanym nośniku, na przykład wybrane pliki lub foldery, które użytkownik uznał za wrażliwe. Po drugie, zaszyfrowany może być cały nośnik, na przykład cały dysk komputera wraz z systemem operacyjnym i wszystkimi sektorami[30]. Uzyskanie dostępu jedynie do pewnych zaszyfrowanych elementów na nośniku stanowi generalnie mniejsze wyzwanie niż uzyskanie dostępu do danych, gdy zaszyfrowany jest cały dysk. Niektóre techniki uzyskania dostępu do danych można zastosować w obu przypadkach, podczas gdy inne będą skuteczne tylko wobec jednego z nich. Przy założeniu, że podejrzany o popełnienie przestępstwa nie zdecyduje się na dobrowolne udostępnienie niezaszyfrowanych danych organom ścigania, celem ich działań powinno być uzyskanie w inny sposób klucza kryptograficznego lub hasła, które umożliwiłyby nieograniczony dostęp do danych mogących stanowić dowód w sprawie karnej, albo uzyskanie pełni tych danych w formie niezaszyfrowanej, choćby bez znajomości klucza.

Pierwsza metoda ich uzyskania może polegać na dokonaniu zabezpieczenia danych w momencie, gdy użytkownik korzysta z nich w niezaszyfrowanej postaci[31]. Wówczas, niezależnie od sposobu, w jaki dane są zaszyfrowane, obecne na miejscu osoby dokonujące czynności są w stanie zabezpieczyć ich kopię binarną, tak by dane były dostępne nawet gdy komputer zostanie wyłączony i nie będzie już możliwe ponowne uzyskanie do niego dostępu. Wymaga to bardzo dobrego zaplanowania czynności zatrzymania, by zastać podejrzanego w momencie korzystania z danych. Może się także przypadkowo zdarzyć, że prowadzący czynności przeszukania czy oględzin zastaną komputer podejrzanego uruchomiony. Podejrzenie, że dane mogą być szyfrowane, stanowi istotny element uzasadniający specyficzne postępowanie z uruchomionym komputerem zastanym na miejscu oględzin czy przeszukania, a zalecenia, by taki komputer z zasady odłączyć od

[29] Wytyczne nr 3 Komendanta Głównego Policji z dnia 15 lutego 2012 r. w sprawie wykonywania czynności dochodzeniowo-śledczych przez policjantów (Dz. Urz. KGP z 16 lutego 2012 r., poz. 7).
[30] S. Lowman, op. cit., s. 2.
[31] A.M. Balogun, S.Y. Zhu, op. cit., s. 37.

zasilania bez ingerowania w istniejące w nim dane, należy odrzucić[32]. Oprócz wykonania kopii niezaszyfrowanych danych zastanie na miejscu uruchomionego komputera umożliwia wykonanie zrzutów pamięci operacyjnej i zabezpieczenie pozostałych ulotnych danych, wśród których możliwe jest odnalezienie samego klucza kryptograficznego niezależnie od tego, czy zaszyfrowany jest cały system, czy tylko niektóre obecne w nim pliki. W przypadku gdy szyfrowanie dotyczy całego dysku wraz z systemem operacyjnym, zastanie uruchomionego przez podejrzanego komputera może być jedyną okazją do zabezpieczenia znajdujących się w nim informacji lub uzyskania klucza kryptograficznego w drodze dokładnej analizy zabezpieczonych danych ulotnych. Dobrze ilustruje to sprawa z 2006 roku, w której na granicy kanadyjsko-amerykańskiej celnik zauważył w laptopie Sebastiana Bouchera treści o prawdopodobnie pedofilskim charakterze. Laptop został wyłączony i zatrzymany do analizy. Dopiero później okazało się, że jego zawartość jest zaszyfrowana i nie ma technicznej możliwości dostępu do niej[33].

Warto przy tym wspomnieć także o znanej, jednak rzadko stosowanej i dość nietypowej technice odzyskiwania danych z pamięci operacyjnej, która wykorzystuje zjawisko zalegania informacji w pamięci elektrostatycznej. Co do zasady pamięć operacyjna funkcjonuje i przechowuje dane, jedynie gdy jest podłączona do zasilania. Jednakże od odłączenia dopływu prądu do całkowitego zaniku ładunków w pamięci operacyjnej upływa pewien czas (od kilkunastu sekund do kilku minut), także po wymontowaniu pamięci RAM z komputera. Badania przeprowadzone nad tym zjawiskiem wykazały jednak, że obniżenie temperatury kości pamięci do -50^{o}C powoduje, że dane opierają się zanikowi znacznie dłużej[34]. Taka temperatura jest wbrew pozorom stosunkowo łatwa do uzyskania, najprostszym sposobem może być wykorzystanie puszki sprężonego powietrza. Dzięki temu zjawisku możliwe jest zabezpieczenie zawartości pamięci RAM bez jej istotnego uszkodzenia, jeżeli od wyłączenia komputera przez podejrzanego upłynął niedługi czas albo gdy komputer zastano w trybie hibernacji. Nie oznacza to oczywiście, że wyodrębnienie właściwych kluczy kryptograficznych lub haseł spośród danych pamięci RAM jest zadaniem prostym, jednakże odpowiednie zabezpieczenie zawartości pamięci operacyjnej jest w tym kontekście kluczowe.

[32] E. Casey, G.J. Stellatos, *The impact of full drive encryption on digital forensics*, „Digital Forensics. ACM SIGOPS Operating Systems Review" 2008, nr 42(3), s. 97.

[33] E. Nakashima, *In Child Porn Case, a Digital Dilemma*, http://www.washingtonpost.com/wp-dyn/content/article/2008/01/15/AR2008011503663.html, dostęp z dnia 03.03.2014.

[34] Eksperymenty w tym zakresie zostały przeprowadzone na Uniwersytecie w Princeton. Wykazano także, że zmrożenie kości pamięci do jeszcze niższych temperatur (na przykład z wykorzystaniem skroplonego azotu) zapewnia zachowanie danych nawet przez kilka godzin w niemal nieuszkodzonej formie. Zob. J.A. Halderman, S.D. Heninger, W. Clarkson, W. Paul, J.A. Calandrino, A.J. Feldman, J. Appelbaum, E.W. Felten, *Lest We Remember: Cold Boot Attacks on Encryption Keys*, w: *2008 USENIX Security Symposium*, Princeton University 2008, http://citp.princeton.edu/pub/coldboot.pdf, dostęp z dnia 05.03.2014.

Na podstawie wspomnianych badań opracowano także propozycje narzędzi programistycznych służących ich praktycznemu zastosowaniu i wydobyciu kluczy kryptograficznych z uzyskanego tą drogą zbioru danych[35].

Drugim sposobem uzyskania dostępu do danych zaszyfrowanych jest odnalezienie hasła użytkownika lub klucza kryptograficznego w innym miejscu niż komputer. Aby szyfrowanie było rzeczywiście skuteczne, należy wykorzystać klucz kryptograficzny o odpowiedniej długości i stopniu skomplikowania. Jednakże silne hasło czy klucz są z oczywistych przyczyn trudne do zapamiętania, dlatego też może się zdarzyć, że użytkownik dla własnej wygody je zapisze. Przystępując do przeszukania lub oględzin, w szczególności miejsca zamieszkania podejrzanego, należy fotograficznie dokumentować wszelkie znalezione notatniki, zapisane kartki i tym podobne przedmioty, w szczególności te znajdujące się w otoczeniu komputera, by móc je później przeanalizować pod kątem zawartości haseł dostępu. Oczywiście należy dbać o to, by podejrzany nie miał możliwości zniszczenia takiej notatki[36].

Po trzecie, należy uważnie przyjrzeć się metodzie szyfrowania. Może się bowiem okazać, że zastosowany został przestarzały algorytm lub klucz o niewystarczającej długości. Miało to miejsce w przypadku Richarda Reida, skazanego w 2002 roku za działania terrorystyczne polegające na planowaniu zamachu bombowego na samolot amerykańskich linii lotniczych[37]. Dane w jego laptopie były zaszyfrowane, jednak wykorzystany przez niego 40-bitowy klucz kryptograficzny umożliwił skuteczne przeprowadzenie ataku siłowego i wyliczenie prawidłowej jego wartości w ciągu pięciu dni pracy komputerów[38]. Podobny atak może się udać także w razie ustalenia przez użytkownika zbyt prostego hasła.

Czwarta metoda może opierać się na wykorzystaniu nieostrożności i tendencji do ustalania przez użytkowników podobnych haseł dostępu do różnych usług[39]. Ogólnie można powiedzieć, że wielu użytkowników przedkłada wygodę użytkowania nad abstrakcyjnie postrzegane bezpieczeństwo, dlatego też hasła często przybierają postać znanych słów czy zwrotów, wzbogaconych ewentualnie o kilka cyfr. Badania nad tym zjawiskiem wykazały, że 46% brytyjskich użytkowników Internetu wykorzystuje te same hasła w dostępie do większości kont

[35] Zob. C. Maartmann-Moe, S.E. Thorildsen, A. Arnes, *The persistence of memory: Forensic identification and extraction of cryptographic keys*, „Digital Investigation" 2009, nr 6, s. 132–140 oraz R. Carbone, C. Bean, M. Salois, *An in-depth analysis of the cold boot attack. Can it be used for sound forensic memory acquisition?*, Defence Research and Development Canada – Technical Memorandum 2011.

[36] S. Lowman, op. cit., s. 7.

[37] Do zamachu bombowego na lecący samolot planował on wykorzystać materiał wybuchowy ukryty w butach, zob. BBC News, *Who is Richard Reid?*, http://news.bbc.co.uk/2/hi/uk/1731568.stm, dostęp z dnia 04.03.2014.

[38] S. Lowman, op. cit., s. 8.

[39] Tamże, s. 3, 8.

internetowych[40]. Inne badanie wykazało, że 30% użytkowników stosuje hasła o długości około sześciu znaków, 60% wykorzystuje jedynie litery i cyfry z pominięciem znaków specjalnych, a prawie połowa stosuje przy tworzeniu haseł imiona, zwroty języka potocznego lub hasła w postaci ciągu kolejnych cyfr[41]. Możliwe jest więc w drodze odpowiedniego postanowienia prokuratorskiego uzyskanie haseł dostępu od dostawców usług internetowych, z których korzystał podejrzany, i wykorzystanie ich przy tworzeniu słownika haseł do przeprowadzenia słownikowego wariantu ataku siłowego. Jeżeli hasła dostępu do różnych wykorzystywanych usług okażą się zbliżone do siebie, to można przewidywać, że także hasło dostępu do danych zaszyfrowanych będzie podobne lub zbudowane na podobnych zasadach co pozostałe i atak słownikowy ma znacznie większe szanse powodzenia.

Piąta proponowana metoda także polega na przeprowadzeniu ataku słownikowego, jednakże z wykorzystaniem jeszcze pełniejszego słownika. Możliwości stworzenia odpowiedniego słownika haseł są znacznie szersze, gdy zaszyfrowane zostały pojedyncze pliki lub foldery, a środowisko systemu operacyjnego jest dostępne. Istnieją duże szanse, że zwroty wykorzystane do stworzenia hasła będą znajdowały się w tej samej lub nieznacznie zmienionej formie, pośród pozostałych danych w komputerze podejrzanego. Aby zbudować bazę dla ataku słownikowego, należy w pierwszej kolejności zebrać dane, o ile to możliwe ze zrzutu pamięci operacyjnej RAM, z pliku stronicowania (pagefile.sys), pliku hibernacyjnego (hiberfil.sys) i z rekordów rejestru systemowego[42], a także dane zapisane w przeglądarkach internetowych, które często przechowują wykorzystywane przy pracy hasła[43].

Rozważając zastosowanie ataku słownikowego (będącego przecież jedynie zoptymalizowaną wersją ataku siłowego), warto też dodać, że jego skuteczność będzie ściśle zależeć od wykorzystanej do tego celu mocy obliczeniowej. Obecnie istnieje możliwość skorzystania z komercyjnych chmur obliczeniowych do zwielokrotnienia siły takiego ataku, a koszty finansowe takiego rozwiązania wydają się co do zasady akceptowalne[44].

Jeżeli jednak także tego typu atak z jakichś przyczyn się nie powiedzie, istnieje możliwość pośredniego ustalenia zawartości zaszyfrowanych fragmentów dysku. Ślady korzystania z pojedynczo zaszyfrowanych plików czy folderów

[40] Badanie przeprowadziła w 2010 roku firma ubezpieczeniowa CPP, zob. http://www.telegraph.co.uk/technology/news/6922207/Almost-16-million-use-same-password-for-every-website-study-finds.html, dostęp z dnia 04.03.2014.

[41] The Imperva Application Defense Center, *Consumer Password Worst Practices*, 2010, http://www.imperva.com/docs/wp_consumer_password_worst_practices.pdf, dostęp z dnia 04.03.2014.

[42] K. Bińkowski, *TrueCrypt z perspektywy informatyki śledczej*, w: J. Kosiński (red.), *Przestępczość teleinformatyczna*, Wyższa Szkoła Policji, Szczytno 2012, s. 90.

[43] S. Bowman, op. cit., s. 8.

[44] K. Bińkowski, op. cit., s. 96.

pozostaną dostępne w systemie komputera. Odnajdywanie cyfrowego materiału dowodowego może wówczas polegać na działaniach podobnych jak w przypadku odnajdywania śladów po trwale usuniętych plikach. Części informacji o zaszyfrowanych plikach mogą być odnalezione pośród metadanych, w plikach tymczasowych, rejestrach systemu i tym podobnych. Niekiedy będzie możliwe wnioskowanie o zawartości zaszyfrowanych elementów na podstawie nazw i właściwości otwieranych wcześniej plików[45]. W części przypadków taki materiał może okazać się wystarczający do przypisania mu określonej wartości dowodowej lub poszlakowej.

Wskazywano też na możliwość całkowicie odmiennego rozwiązania problemu trudności dostępu organów ścigania do zaszyfrowanych danych. Miałoby ono polegać na ścisłej współpracy rządów państw i organów ścigania z producentami sprzętu i oprogramowania szyfrującego, która umożliwiłaby stworzenie haseł uniwersalnych lub intencjonalnych luk, pozwalających uprawnionym organom na dostęp do takich danych na potrzeby postępowań karnych[46]. Jednakże pomijając kontrowersyjność takiego rozwiązania, dotychczas nie nawiązano tego rodzaju porozumienia i nie wydaje się ono realną perspektywą w najbliższej przyszłości[47].

Wymienione powyżej możliwe do zastosowania techniki odszyfrowania danych polegają w zasadzie na wykorzystaniu nieostrożności podejrzanego, dzięki której realne jest przechwycenie hasła lub klucza kryptograficznego albo odpowiednia optymalizacja ataku siłowego. Dowolny system zabezpieczeń jest tak skuteczny, jak jego najsłabsze ogniwo. W wielu przypadkach sprawcy przestępstw, skuszeni bezpieczeństwem oferowanym przez współczesną kryptografię, nie będą dochowywać zalecanych środków ostrożności i umożliwią przez to skuteczne działanie organom śledczym. Należy jednak wyraźnie podkreślić, że jeżeli narzędzie kryptograficzne zostanie zastosowane prawidłowo, to uzyskanie dostępu do zabezpieczonych w ten sposób danych całkowicie przekracza dzisiejsze możliwości techniczne. Wobec tego istnieje zauważalna tendencja do wprowadzania specyficznych rozwiązań prawnych, mających zapobiegać temu problemowi, między innymi przewidujących obowiązek dostarczenia przez podejrzanego danych w postaci niezaszyfrowanej lub obowiązek ujawnienia haseł dostępu do danych[48]. Warto więc pokrótce omówić niektóre z takich rozwiązań, a także ocenić sytuację z perspektywy przepisów polskiego postępowania karnego.

Jednym z najczęściej omawianych przykładów jest Wielka Brytania, gdzie w 2007 roku weszła w życie część III ustawy o uprawnieniach policyjnych[49], w której zawarto szczególne przepisy zobowiązujące każdego do przedstawienia haseł dostępu do danych zaszyfrowanych lub do dostarczenia danych w postaci

[45] Tamże, s. 10.
[46] Zob. D. Forte, *Do encrypted disks spell the end of forensics?*, „Computer Fraud and Security" 2009, nr 2, s. 18–20.
[47] A.M. Balogun, S.Y. Zhu, op. cit., s. 39.
[48] A. Lach, *Dowody elektroniczne w procesie karnym*, TNOiK, Toruń 2004, s. 100–101.
[49] *Regulation of Investigatory Powers Act 2000*, c. 23, part III.

niezaszyfrowanej na pisemne lub zaprotokołowane wezwanie upoważnionego do tego urzędnika (np. policjanta przeprowadzającego przeszukanie). Obowiązek ten dotyczy zarówno świadków, osób trzecich, jak i podejrzanych o przestępstwa. Rozwiązanie to jest o tyle interesujące, że niepodporządkowanie się temu nakazowi stanowi osobne przestępstwo, zagrożone karą do dwóch lat pozbawienia wolności (lub do pięciu lat pozbawienia wolności, gdy toczące się postępowanie prowadzone było w związku z podejrzeniami o działania terrorystyczne). Przepisy te wzbudziły wiele kontrowersji spowodowanych naruszeniem ogólnej zasady postępowania karnego zabraniającej zmuszania do samooskarżenia, jednakże utrzymano je w mocy. Sąd, który podejmował decyzję w tej sprawie, uzasadnił ją następująco: „Klucz do danych w komputerze nie różni się niczym od klucza do zamkniętej szafki. Zawartość takiej szafki istnieje niezależnie od osoby podejrzanego i podobnie niezależnie wobec klucza do niej. Zawartość może być obciążająca lub nie, jednak sam klucz jest elementem neutralnym”[50]. Przepisy te funkcjonują w praktyce i od wejścia w życie doprowadzono już na ich podstawie do oskarżenia lub skazania co najmniej kilku osób[51]. Przepisy obowiązujące w Wielkiej Brytanii zostały przedstawione w niniejszym opracowaniu jako modelowe. Podobnej treści przepisy wprowadziło także kilka innych państw, m.in. Francja[52] czy Australia[53].

Z problemem braku dostępu do zaszyfrowanych materiałów zderzyły się także organy wymiaru sprawiedliwości w Stanach Zjednoczonych, jednak precedensowy charakter prawa amerykańskiego tworzy specyficzne i niejednolite warunki dotyczące możliwości zobowiązania podejrzanego do ujawnienia zaszyfrowanych danych informatycznych mogących stanowić cyfrowy materiał dowodowy w sprawie karnej. Wobec braku bezpośrednich przepisów odnoszących się do tej kwestii dyskusja toczy się tam na gruncie Piątej Poprawki do Konstytucji Stanów Zjednoczonych, która stanowi m.in., że: „nikt nie może być zmuszony do zezna-

[50] S. Bowman, op. cit., s. 4, za: England and Wales Court of Appeal (Criminal Division), *EWCA Crim 2177*, http://www.bailii.org/ew/cases/EWCA/Crim/2008/2177.html, dostęp z dnia 04.03.2014.

[51] Zob. M. Ward, *Campaigners hit by decryption law*, http://news.bbc.co.uk/2/hi/technology/7102180.stm, dostęp z dnia 10.12.2013.

[52] Obowiązująca we Francji ustawa o bezpieczeństwie publicznym zezwala prokuratorowi lub sędziemu na nakazanie każdemu, kogo może to dotyczyć, dostarczenia danych niezaszyfrowanych lub kluczy kryptograficznych pod karą trzech lat pozbawienia wolności i 45 000 euro grzywny. Kara jest podwyższana do 5 lat pozbawienia wolności i 75 000 euro, w razie gdyby zastosowanie się do nakazu mogło zapobiec przestępstwu lub złagodzić jego skutki. Zob. *Loi n^{o} 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne*, article 30.

[53] Policja australijska dysponująca odpowiedniej treści nakazem może żądać dostępu do komputerów i danych w nich się znajdujących. Przez to pojęcie rozumie się też obowiązek ewentualnej deszyfracji danych. Niezastosowanie się do nakazu zagrożone jest karą 6 miesięcy pozbawienia wolności. Zob. *The Cybercrime Act 2001 No. 161, 2001*, pkt 12 i pkt 28.

wania w sprawie karnej na swoją niekorzyść”[54]. Prawo to podlega jednakże specyficznej interpretacji. Już w 1911 roku Sąd Najwyższy Stanów Zjednoczonych uznał, że nie stanowi naruszenia zakazu zmuszania do samooskarżenia obowiązek przekazania organom ścigania rzeczowego materiału dowodowego. Nie stanowi ono bowiem „zeznania” chronionego przez Piątą Poprawkę[55]. Dlatego też zasadniczą kwestią rozważaną przez sądy amerykańskie jest to, czy w danej sprawie dostarczenie haseł dostępu do danych stanowi „zeznanie”, pozwalające organom ścigania na uzyskanie nowych informacji obciążających podejrzanego. Można wskazać kilka istotnych spraw z ostatnich lat, które zdają się wytyczać kierunek orzecznictwa amerykańskiego w tej kwestii[56].

Jedną z nich może być wcześniej wspomniana sprawa *U.S. v. Sebastian Boucher*. Początkowo jego prawo do odmowy zeznawania na swoją niekorzyść zostało uwzględnione. Ostatecznie, po odwołaniu złożonym przez prokuratora, w 2009 roku sąd uznał jednak, że skoro przekraczając granicę, pokazał on funkcjonariuszowi dane ze swojego komputera w niezaszyfrowanej postaci (w efekcie czego został zatrzymany), to można przyjąć, że formalnie organy ścigania mają już wiedzę na temat zawartości laptopa. A skoro znana jest zawartość laptopa, to dostarczenie niezaszyfrowanych danych przez Sebastiana Bouchera nie będzie stanowiło „zeznania na własną niekorzyść”[57]. Podobnie potraktowano tę kwestię w sprawie *U.S v. Ramona Fricosu* z 2012 roku. Na podstawie nagrania rozmowy pomiędzy podejrzaną a jej mężem przebywającym w zakładzie karnym ustalono, że w zabezpieczonych, lecz zaszyfrowanych laptopach znajdują się obciążające ją materiały. Także w tym wypadku sąd uznał, że skoro istnienie i lokalizacja obciążających dowodów cyfrowych są znane władzy, to przekazanie ich w formie niezaszyfrowanej nie stanowi „zeznania” w rozumieniu konstytucyjnym[58]. Inaczej było w postępowaniu w sprawie *In re John Doe*[59], które także toczyło się w 2012 roku. W sprawie zabezpieczono kilka komputerów i zewnętrznych dysków twardych, jednakże wszystkie były zaszyfrowane. Stwierdzono, że nie ma możliwości obejścia tych zabezpieczeń i tak naprawdę nie wiadomo nic na temat treści zabezpieczonych danych. Ostatecznie sąd apelacyjny podtrzymał prawo oskarżonego

[54] Piąta Poprawka do Konstytucji Stanów Zjednoczonych, zob. http://libr.sejm.gov.pl/tek01/txt/konst/usa.html, dostęp z dnia 05.03.2014.

[55] „The question is not of testimony, but of surrender”, zob. J. Goodman, *Forced data decryption: Does it violate the Fifth Amendment?*, „Criminal Justice” 2013, t. 27, nr 4, http://www.crowell.com/files/Forced-Data-Decryption-Does-It-Violate-the-Fifth-Amendment.pdf, dostęp z dnia 05.03.2014, za: *In re Harris*, 221 U.S. 274 (1911).

[56] Zob. J. Goodman, op. cit.

[57] J. Goodman, op. cit., za: *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

[58] J. Goodman, op. cit., za: *U.S. v. Fricosu*, 841 F. Supp. 2d 1232, 1235 (D. Colo. 2012).

[59] „John Doe” jest męskim imieniem i nazwiskiem stosowanym, gdy prawdziwe dane osoby nie są ujawniane publicznie, zob. https://www.princeton.edu/~achaney/tmve/wiki100k/docs/John_Doe.html, dostęp z dnia 05.03.2014.

do odmowy ujawnienia danych i stwierdził, że: „czynność dostarczenia [danych w formie niezaszyfrowanej] może mieć charakter zeznania, jeżeli wiąże się z nią pośrednio lub bezpośrednio ujawnienie faktu istnienia określonych materiałów”[60]. Ponieważ prowadzący śledztwo w tej sprawie nie wiedzieli nic o treści zaszyfrowanych danych, nie mogli żądać ich dostarczenia w innej formie.

Można więc podsumować, że w Stanach Zjednoczonych możliwość zobowiązania podejrzanego do dostarczenia niezaszyfrowanych danych mogących stanowić dowód przeciwko niemu jest uzależniona od tego, jaką wiedzą na ich temat dysponują organy ścigania. Potencjalne sankcje związane z niepodporządkowaniem się prawomocnemu nakazowi wydania danych wynikają z przepisów ogólnych dotyczących nakazów sądowych w Stanach Zjednoczonych. Jeżeli podejrzany nie podporządkuje się takiemu nakazowi, może być ukarany za pośrednią obrazę sądu.

Przenosząc rozważania na grunt polskiej procedury karnej, trzeba zauważyć, że nie zawiera ona szczególnych rozwiązań w kwestii danych zaszyfrowanych. Należy więc stosować ogólnie obowiązujące przepisy postępowania karnego, w związku z czym zgodnie z treścią art. 74 k.p.k. ani oskarżony, ani osoba podejrzana (na podstawie art. 74 w zw. z art. 71 § 2 k.p.k.) nie są obowiązani do dostarczenia dowodów na swoją niekorzyść oraz mają prawo do odmowy składania wyjaśnień bez ponoszenia negatywnych tego konsekwencji (art. 175 k.p.k.), mogą więc także odmówić przekazania kluczy kryptograficznych, haseł czy danych w formie niezaszyfrowanej. Świadek z kolei, z wyjątkiem sytuacji, gdy przysługuje mu prawo odmowy składania zeznań lub odpowiedzi na pytania (art. 182 i art. 183 k.p.k.), lub gdy objęty jest zakazem dowodowym (art. 178, art. 179, art. 180 i art. 185 k.p.k.), oraz gdy ewentualnie zostanie zwolniony z obowiązku zeznawania (art. 185 k.p.k.), ma obowiązek złożenia zeznań i odpowiedzi na pytania. Jeżeli więc w ogóle posiada tego typu wiedzę, nie może uchylić się od udzielenia odpowiedzi na pytania zmierzające do ujawnienia zaszyfrowanych danych. Warto zwrócić uwagę, że o ile regulacje przyjęte przez Wielką Brytanię przewidują alternatywnie możliwość ujawnienia hasła dostępu lub dostarczenie danych w czytelnej formie, o tyle w Polsce świadek nie mógłby się uchylić od odpowiedzi na zadane wprost pytanie o brzmienie hasła dostępu. Świadek może nie mieć obiekcji przed wydaniem organom danych niezaszyfrowanych, ale jednocześnie może z różnych przyczyn nie chcieć ujawniać stosowanego przez siebie hasła, i w tym kontekście przepisy brytyjskie są dla niego korzystniejsze. Podsumowując, w Polsce odmowa składania wyjaśnień, także w zakresie ujawnienia informacji o zaszyfrowanych dowodach cyfrowych, jest ustawowym prawem podejrzanego, świadek zaś uchylający się od zeznawania w tym zakresie naraża się na konsekwencje przewidziane dla nieuzasadnionej odmowy składania zeznań, a więc na grzywnę lub areszt (art. 285 i art. 287 k.p.k.). Można zatem powiedzieć, że w pełni zostało zagwarantowane prawo do niesamooskarżania się, a świadkowie muszą zeznawać na okoliczność ujawnienia zaszyfrowanych informacji, choć

[60] J. Goodman, op. cit., za: *In re Doe*, 670 F.3d 1335 (11th Cir. 2012).

możliwości zmuszenia niechętnych organom ścigania świadków do podania pożądanych informacji są dosyć ograniczone.

Wszystkie wymienione powyżej prawne sposoby uzyskiwania dostępu do zaszyfrowanych danych opierają się jednak na zeznaniu bądź wyjaśnieniu osoby, z czego wynikają też typowe problemy związane z osobowymi środkami dowodowymi. Świadek, nawet gdy ma obowiązek zeznawania i odpowiadania na pytania, nie zawsze jest prawdomówny, a żadna regulacja prawna nie uchroni postępowania karnego przed fałszywą „niewiedzą" lub „niepamięcią" świadków czy podejrzanych. Z jednej z warszawskich kancelarii adwokackich znany jest też przypadek przedsiębiorcy, przeciwko któremu wszczęto postępowanie karne i w którego przedsiębiorstwie zabezpieczono zaszyfrowane dyski. Podejrzany oświadczył, że pragnie współpracować z organami ścigania, jednak zapytany o hasło dostępu do dysków poinformował prokuratora, że hasła nie pamięta, bo było ono zmieniane raz w tygodniu, i że lista aktualnych haseł znajduje się wśród zabezpieczonych przez policję dokumentów. Listy tej jednak nie odnaleziono i trudno jest ocenić, czy rzeczywiście ona istniała i została zagubiona w toku czynności śledczych, czy też podejrzany zwodzi organy ścigania w tej kwestii. Niemniej jednak żadna istniejąca regulacja prawna nie zapewni faktycznego dostępu do dowodów cyfrowych w takiej sytuacji. Trzeba też pamiętać o tym, że twórcy oprogramowania szyfrującego nie pozostają obojętni wobec ustanawianych przepisów i umożliwiają m.in. tworzenie tak ukrytych zaszyfrowanych obszarów dysku komputera, że trudne jest samo wykazanie ich istnienia[61].

Podsumowując, możliwości, jakie daje kryptografia w zakresie ograniczenia dostępu do danych cyfrowych, są bardzo szerokie. Nowoczesne rozwiązania szyfrujące są pewne, bezpieczne, darmowe, stosunkowo proste w obsłudze i stosowanie ich staje się coraz bardziej popularne, niestety nie tylko wśród obywateli chcących chronić swoją prywatność, lecz także wśród sprawców przestępstw komputerowych chcących uniknąć odpowiedzialności. Paradoksalnie, chcąc chronić dane przed sprawcami przestępstw i opracowując w tym celu coraz bezpieczniejsze metody szyfrowania, wręcza się im równocześnie coraz skuteczniejsze narzędzia służące uniknięciu odpowiedzialności karnej. Jeżeli szyfrowanie danych zostało prawidłowo skonfigurowane przez użytkownika, to uzyskanie dostępu do nich jest zadaniem praktycznie niemożliwym z perspektywy organów ścigania. Rodzi to bardzo poważne skutki dla postępowań karnych w sprawach przestępstw komputerowych, w których dane cyfrowe często stanowią najistotniejszy element materiału dowodowego. Trwałe zlikwidowanie tego problemu od strony technicznej musiałoby się wiązać z pozbawieniem skuteczności stosowa-

[61] Można np. skonfigurować ukryty system operacyjny, a osoba zobowiązana do podania hasła może ujawnić jedno z kilku haseł, przez co udostępni organom ścigania jedynie fasadowy system operacyjny, twierdząc jednocześnie, że jest to jedyny zainstalowany system w danym komputerze, tymczasem „prawdziwy" system pozostaje ukryty. Zob. *Plausible deniability*, dokumentacja programu TrueCrypt, http://www.truecrypt.org/docs/plausible-deniability#Y0, dostęp z dnia 06.03.2014.

nych szyfrów (lub z obniżeniem stopnia ich bezpieczeństwa, na przykład przez wprowadzanie „tylnych furtek" w oprogramowaniu), co nie wydaje się rozsądne, gdyż istnienie rzeczywiście bezpiecznych szyfrów jest współcześnie konieczne dla zapewnienia ochrony danych w dobrze pojętym interesie ich dysponentów. Wobec ograniczeń technicznych czynione są próby rozwiązania tego problemu na gruncie prawnym. Wyraźnie jednak trzeba podkreślić, że nawet ustanowienie niczym nieograniczonego obowiązku dostarczenia hasła dostępu do danych na wzór brytyjski nie zagwarantuje tego, że osoba o to zapytana nie oświadczy, iż hasła nie zna lub z jakichś przyczyn go nie pamięta. Należy więc poszukiwać innych sposobów dostępu organów ścigania do zaszyfrowanych danych. W niniejszym opracowaniu przedstawione zostały niektóre spośród technik mogących służyć ominięciu zabezpieczeń kryptograficznych przez organy ścigania, w dużej mierze opierających swoją skuteczność na nieostrożności osoby stosującej szyfrowanie danych. Mimo to, w obliczu braku innych skutecznych możliwości uzyskania dostępu do zaszyfrowanych informacji, prawdopodobnie należy skupić się na opracowaniu, usystematyzowaniu i stosowaniu technik i taktyk postępowania w sprawach, w których mogą wystąpić dowody cyfrowe w zaszyfrowanej formie, by maksymalnie wykorzystać wszystkie ewentualne błędy osoby podejrzanej. Do najważniejszych sposobów należy takie planowanie czynności zatrzymania sprzętu i osoby, by następowało to w momencie korzystania przez podejrzanego z szyfrowanych danych. Jeżeli okaże się to niemożliwe, warto starać się tworzyć możliwie odpowiedni słownik haseł do ataku słownikowego. Praca biegłego, który będzie starał się odszyfrować zabezpieczone dane, może być w znacznym stopniu ułatwiona przez odpowiednie zachowanie się osób dokonujących zabezpieczenia dowodów, na przykład jeżeli uda się wykonać zrzut pamięci RAM, a także osoby nadzorującej postępowanie, która może na przykład przekazać biegłemu uzyskane wcześniej hasła dostępu do innych usług, z których korzystał podejrzany. Kryptograficzne ukrycie dowodów cyfrowych stanowi, i prawdopodobnie jeszcze długo będzie stanowić, poważne wyzwanie dla organów ścigania i współczesnej kryminalistyki, a metody radzenia sobie z nim muszą być stosowane precyzyjnie i wymagają dużej uwagi oraz współpracy policji, prokuratury i powoływanych biegłych z zakresu technik komputerowych.

Streszczenie:
W celu ochrony informacji przechowywanych w formie cyfrowej w systemach informatycznych opracowywane są specjalne narzędzia szyfrujące dane. Niestety, z narzędzi tych korzystają także sprawcy przestępstw w celu uczynienia dowodów przestępstw niedostępnymi dla organów ścigania. Poprawne zastosowanie współczesnej kryptografii czyni przeanalizowanie zabezpieczonych danych technicznie niemożliwym, a dotychczas proponowane rozwiązania prawne nie są w pełni skuteczne i często naruszają zakaz zmuszania do samooskarżenia. W obliczu tych problemów należy opracowywać taktyki i techniki zabezpieczania oraz analizy dowodów cyfrowych, które pozwolą, w pewnych okolicznościach, uzyskać dane w formie niezaszyfrowanej. Jest to możliwe szczególnie wtedy, gdy

szyfrowanie danych zostanie przeprowadzone bez zachowania wszystkich środków ostrożności.

Słowa kluczowe: kryptografia, kryptoanaliza, dowód cyfrowy, TrueCrypt, szyfrowanie danych, przestępczość komputerowa.

Summary:
Special encryption tools are developed in order to protect digital data stored in computer systems. Unfortunately, these tools are also used by computer crimes perpetrators in order to make digital evidence inaccessible to law enforcement. Correct application of modern cryptography often makes analysis of digital evidence technically impossible. Legal solutions to this problem are not fully effective and often violate the right against forced self-incrimination. It is crucial to develop tactics and techniques of digital evidence preservation and analysis that will allow, in certain circumstances, to obtain the data in unencrypted form. It is possible especially when the perpetrator failed to comply with all safety precautions concerning data encryption.

Keywords: cryptography, cryptanalysis, digital evidence, TrueCrypt, data encryption, cyber crime.