Nr 4(43)/2017
Rok XI
ISSN 1898-1453

Kwartalnik policyjny

CZASOPISMO
CENTRUM SZKOLENIA POLICJI
W LEGIONOWIE

CYBER BEZPIECZEŃSTWO

W numerze:

System cyberbezpieczeństwa Polaków ■ Infrastruktura krytyczna ■ Ochrona systemów informatycznych Policji ■ Rodzaje cyberzagrożeń ■ Proces wykrywczy ■ Aspekty procesowe zwalczania cyberprzestępczości ■ Analiza kryminalna w dobie społeczeństwa informacyjnego ■ Dydaktyka policyjna

Kwartalnik policyjny

CZASOPISMO
CENTRUM SZKOLENIA POLICJI W LEGIONOWIE

Wydawca: Centrum Szkolenia Policji

Adres redakcji:
ul. Zegrzyńska 121,
05-119 Legionowo
sekretariat: (22) 605-33-72,
faks: (22) 605-35-80,
e-mail: kwartalnik@csp.edu.pl

Druk: Wydział Wydawnictw i Poligrafii
Centrum Szkolenia Policji

Nakład: 1000 egz.

Numer zamknięto 10.01.2018 r.

Lista recenzentów artykułów w „Kwartalniku Policyjnym” w 2017 r.

DR HAB. MAŁGORZATA GRUCHOŁA
Katedra Komunikacji Wizualnej Instytutu Dziennikarstwa i Komunikacji Społecznej Katolickiego Uniwersytetu Lubelskiego im. Jana Pawła II

DR INŻ. ROBERT JANCZUR
Instytut Pojazdów Samochodowych i Silników Spalinowych Politechniki Krakowskiej im. Tadeusza Kościuszki w Krakowie

PŁK DR PIOTR KONIEC
Komenda Główna Żandarmerii Wojskowej

DR MARZENA KORDACZUK-WĄS
Komenda Główna Policji

DR HAB. MARIUSZ KUBIAK
Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach

DR AGNIESZKA ŁAPIŃSKA
Wydział Prewencji Komendy Miejskiej Policji w Białymstoku

MŁ. INSP. DR INŻ. ROBERT MACIEJCZYK
Centrum Szkolenia Policji

PŁK DR HAB. DARIUSZ MAJCHRZAK
Akademia Sztuki Wojennej

DR ROBERT NETCZUK
Wydział Prawa i Administracji Uniwersytetu Śląskiego w Katowicach

DR ANDRZEJ SKWARSKI
Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim

DR HAB. TADEUSZ SYCZEWSKI
prof. KUL, Wydział Prawa, Prawa Kanonicznego i Administracji Katolickiego Uniwersytetu Lubelskiego im. Jana Pawła II

PODINSP. DR MAREK UJAZDA
Komenda Powiatowa Policji w Wołominie

GEN. DYW. REZ. DR HAB. INŻ. KRZYSZTOF ZAŁĘSKI
prof. Wyższej Szkoły Biznesu w Dąbrowie Górniczej

Szanowni Państwo

Dziesięciolecie „Kwartalnika Policyjnego” zamykamy numerem poświęconym problematyce cyberbezpieczeństwa. Współczesny rozwój technologii teleinformatycznych przynosi bowiem ogromne szanse i możliwości, ale stwarza też nowe, narastające zagrożenia, które stanowią trudne wyzwanie dla instytucji i służb związanych z ochroną bezpieczeństwa.

Próbując sprostać próbie przedstawienia tego zagadnienia, zaprosiliśmy do współpracy przedstawicieli środowiska naukowego, NASK – Państwowego Instytutu Badawczego, Rządowego Centrum Bezpieczeństwa oraz funkcjonariuszy komórek organizacyjnych Policji zajmujących się problematyką cyberbezpieczeństwa: Biura do Walki z Cyberprzestępczością, Biura Kryminalnego, Biura Wywiadu i Informacji Kryminalnej, Biura Łączności i Informatyki Komendy Głównej Policji, Wydziału do Walki z Cyberprzestępczością Komendy Wojewódzkiej Policji w Bydgoszczy oraz Zakładu Służby Kryminalnej Centrum Szkolenia Policji.

W niniejszym wydaniu zawarto też zagadnienia dotyczące dydaktyki policyjnej, opracowane przez kadrę dydaktyczną CSP oraz nauczyciela stowarzyszonego – biegłego sądowego.

Zapraszamy do lektury.

Redakcja „Kwartalnika Policyjnego”

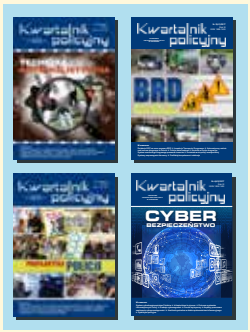
Kwartalnik policyjny 10 lat 2007–2017


PODSUMOWANIE

10 lat „Kwartalnika Policyjnego” to:

43 numery czasopisma,
ponad **820** artykułów kilkuset Autorów,
33,5 tys. stron, ponad **21 mln** znaków.

Warto podkreślić, że zaszczytny tytuł
Autora Dziesięciolecia „Kwartalnika Policyjnego”
przypada
podinsp. Leszkowi Dyduchowi,
obecnemu Zastępcy Kierownika Zakładu Służby Prewencyjnej Centrum Szkolenia Policji w Legionowie.

2007 — 2008 — 2009 — 2015 — 2016 — 2017

Od 2008 r. opublikowaliśmy jego 15 artykułów (w tym 1 współautorstwo) o łącznej objętości prawie pół miliona znaków. Prezentowane przez niego zagadnienia dotyczyły m.in. współdziałania Policji z innymi służbami, praktycznych aspektów służby prewencyjnej, przygotowań do zabezpieczenia EURO 2012 oraz szkolenia spottersów, roli Policji w systemie zarządzania kryzysowego, wspomagania dowodzenia w Policji, a także Krajowej Mapy Zagrożeń Bezpieczeństwa w odniesieniu do interwencji policyjnych.
Przekazujemy mu gratulacje oraz wyrazy wdzięczności i uznania dla jego pasji i wytrwałości.

Zarówno Autorom, którzy zechcieli podzielić się na łamach naszego pisma swoją wiedzą i doświadczeniem zawodowym, jak i Współpracownikom oraz wszystkim Czytelnikom „Kwartalnika Policyjnego”
serdecznie dziękujemy za wspólne 10 lat.

Kwartalnik policyjny

W NUMERZE

Czekamy na listy, propozycje tematów i opinie na temat zamieszczonych tekstów. Prosimy je przesyłać na adres kwartalnik@csp.edu.pl.
Redakcja zastrzega sobie prawo skracania tekstów i dokonywania w nich zmian oraz możliwość nieodpłatnego wykorzystania publikowanych materiałów na stronie internetowej www.kwartalnik.csp.edu.pl.

PAŃSTWOWY INSTYTUT BADAWCZY

NASK

WSPÓŁTWORZYMY SYSTEM CYBERBEZPIECZEŃSTWA POLAKÓW

dr inż. Wojciech Kamieniecki

Dyrektor NASK
Państwowego Instytutu Badawczego

Z NASK związany od 2015 r. jako Dyrektor ds. ICT. Absolwent Wydziału Automatyki i Informatyki Politechniki Śląskiej oraz studiów doktoranckich na Uniwersytecie Szczecińskim na kierunku ekonomia i zarządzanie. Od 2017 r. doktor w dziedzinie nauk ekonomicznych.
Pełnił funkcję Dyrektora Generalnego Multimedia Polska S.A., Prezesa Zarządu Nordisk Polska Sp. z o.o., Dyrektora Projektu TETRA EXATELS.A., a ostatnio – Dyrektora Generalnego Projektu Internet dla Mazowsza.
Od 2013 r. współpracuje z CEE Equity Partners (PE) w zakresie oceny projektów związanych z budową regionalnych sieci szerokopasmowych oraz ostatniej mili. Od 2014 r. – Przewodniczący Rady Nadzorczej Mielec PV S.A. Jest autorem publikacji naukowych z zakresu strategii rozwoju i zarządzania przedsiębiorstwami oraz kształtowania wartości przedsiębiorstwa.

Skala zagrożeń związanych z używaniem internetu wymaga kompleksowej odpowiedzi. Przede wszystkim konieczna jest rozbudowa narzędzi technologicznych, np. systemów do automatycznego wykrywania zagrożeń, ich analizy i wymiany informacji, w tym międzynarodowej infrastruktury obserwacyjnej. Stanowi to obecnie jeden z ważniejszych obszarów prac badawczo-rozwojowych NASK Państwowego Instytutu Badawczego. Security Operation Center (SOC) w NC Cyber pracuje 24 godziny na dobę, korzystając z tych innowacyjnych narzędzi, aby monitorować polską sieć i w razie potrzeby przekazywać informacje do właścicieli zagrożonych sieci. Służy do tego m.in. platforma n6. Jest to usługa dla profesjonalistów – administratorów zajmujących się sieciami w biurach, na osiedlach, w szkołach, firmach.

Drugim istotnym warunkiem utrzymania bezpieczeństwa jest świadomość społeczna. Zagrożenia przychodzące z sieci często polegają na próbie oszustwa, manipulacji, podstępnego podsuwania złośliwego oprogramowania lub wyłudzania poufnych informacji (np. haseł do banku). Zapobieganie tego typu przestępstwom polega przede wszystkim na edukacji użytkowników. NASK PIB organizuje działania edukacyjne, kierowane do osób dorosłych (w tym seniorów) oraz do dzieci i młodzieży w ramach programu Komisji Europejskiej „Safer Internet" oraz w ramach działającej w instytucie Akademii NASK i portalu e-learningowego IT Szkoła.

Bezpieczeństwo wiąże się też z przeciwdziałaniem dystrybucji w internecie treści nielegalnych i szkodliwych. Tym zajmuje się zespół interwencyjny Dyżurnet.pl, który przyjmuje zgłoszenia (również anonimowe) od internautów.

WYZWANIA DLA CYBERBEZPIECZEŃSTWA JESZCZE NIGDY NIE BYŁY TAK POWAŻNE.

W 2016 r. w Europie odnotowywano ponad 4 tys. ataków dziennie z użyciem samego tylko oprogramowania typu ransomware[1], a 80% przedsiębiorstw unijnych doświadczyło co najmniej jednego incydentu związanego z bezpieczeństwem cybernetycznym.

Przewodniczący Komisji Europejskiej Jean-Claude Juncker w swoim orędziu o stanie Unii w 2017 r., wygłoszonym w Parlamencie Europejskim, wyraził opinię, że „ataki cybernetyczne mogą zagrażać stabilności systemów demokratycznych i gospodarek bardziej niż broń i czołgi”[2]. Nie sposób odmówić mu racji. Nie oznacza to, na szczęście, że nasze próby stawienia czoła temu wyzwaniu są z góry skazane na niepowodzenie. Konieczna jest jednak konsolidacja tych wysiłków, zacieśnienie wymiany informacji i doświadczeń pomiędzy ekspertami, a także w obrębie poszczególnych sektorów gospodarki – między sektorami i między państwami. Dla służb odpowiedzialnych za bezpieczeństwo, w tym Policji, współpraca z różnymi środowiskami w kraju i zagranicą jest również jednym z kluczowych warunków efektywnego działania. Niewątpliwie nasze strategie ochrony przed cyberprzestępczością muszą ulegać modyfikacji wraz ze zmianami krajobrazu zagrożeń. NASK Państwowy Instytut Badawczy od początku działania Internetu w Polsce śledzi te zmiany i dynamicznie na nie reaguje, dostosowując obszary swojej pracy do nowych warunków. Poniżej nakreślono główne obszary obecnej działalności instytutu.

Duży Internet – duży problem

Skala zagrożeń jest zależna od liczby urządzeń podłączonych do Internetu i zakresu oferowanych usług. Właśnie z rozwoju rynku internetowego wynika lawinowy wzrost liczby cyberataków, który obserwujemy od kilku lat. Niestety, stuprocentowych zabezpieczeń nie ma. Producenci sprzętu i oprogramowania, nauczeni smutnym doświadczeniem, coraz większą wagę przywiązują do kwestii bezpieczeństwa. Jednak nie wszyscy. Zresztą nawet ci, którzy troszczą się o zabezpieczenia, niekiedy popełniają błędy. W rezultacie technologie niezawodne są takimi tylko do chwili, kiedy ktoś odkryje lukę czyniącą je podatnymi na atak. Wszystkie szanujące się firmy wypuszczają aktualizacje, stale poprawiając swoje produkty i usuwając błędy, których wcześniej nie zauważyli. Luki w oprogramowaniu, które mogą wykorzystać hakerzy, są zresztą przedmiotem handlu. Bywa, że osoba, która odkryje lukę, zgłasza to do producenta, często otrzymując w zamian nagrodę pieniężną. Ale może też przekazać informację o niej przestępcom, którzy prawdopodobnie zapłacą więcej. Organizacje przestępcze niekiedy wręcz zatrudniają etatowych analityków poszukujących słabych punktów w zabezpieczeniach serwerów i innych urządzeń.

Odkrywszy lukę w popularnym produkcie – np. systemie operacyjnym lub przeglądarce internetowej, przestępcy mogą zaprojektować atak wymierzony w miliony osób na całym świecie. Często, aby zmaksymalizować efekt, hakerzy przejmują komputery nieświadomych osób, zamieniając je w tzw. boty, czyli zmuszając je do wykonywania zdalnych poleceń, np. rozsyłania spamu lub szkodliwego oprogramowania.

Sieć botów (ang. *botnet*) to jedno z aktualnie popularnych narzędzi stosowanych przez cyberprzestępców. Systemy NC Cyber do automatycznej analizy malware[3] zidentyfikowały 3344 prawdopodobne adresy serwerów zarządzania botnetami na świecie. W ubiegłym roku odnotowano też nowe zjawisko – masowe wykorzystanie do tworzenia botnetów drobniejszych urządzeń, np. kamerek internetowych i domowych lub biurowych nagrywarek DVR. Procesory tych urządzeń nie nadają się do wykonywania skomplikowanych zadań. Ale każde z nich ma własny adres IP i może połączyć się z wyznaczonym serwerem. Jeśli wiele urządzeń zrobi to jednocześnie, to serwer może zostać przeciążony. Na tym polegają ataki DDoS (ang. *distributed denial of service* – rozproszona odmowa usługi).

Jeden z rekordowych ataków z użyciem takiego botneta (o nazwie Mirai) nastąpił 21 października 2016 r. Zostały przeciążone serwery firmy Dyn świadczącej usługi internetowe, dzięki którym działało wiele popularnych na całym świecie serwisów internetowych, takich jak np. Spotify, Reddit, New York Times czy Wired. Przerwę w ich działaniu odczuły miliony internautów. Szacowana liczba botów biorących udział w tym ataku to około 100 tysięcy, a ich lokalizacja geograficzna była rozproszona. Część z nich mogła pochodzić z Polski, bo i tu eksperci zaobserwowali aktywność botnetu. W okresie od 29 października do 31 grudnia 2016 r. zespół CERT Polska (ang. *Computer Emergency Response Team*), działający w NC Cyber w NASK, obserwował średnio 7283 urządzenia przejęte przez hakerów dziennie. Rekordem było 14 054 botów jednego dnia.

Użytkownicy, poza wąskim gronem specjalistów, przeważnie nie są w stanie na bieżąco śledzić wszystkich doniesień dotyczących zagrożeń ani w porę im przeciwdziałać. Stąd potrzeba wypracowywania narzędzi do automatycznego wykrywania zagrożeń, ich analizy i wymiany informacji. Takie narzędzia umożliwiają niezwłoczną reakcję administratorów sieci na niebezpieczne zdarzenia. Jest to obecnie jeden z ważniejszych obszarów prac badawczo-rozwojowych NASK PIB. Security Operation Center (SOC) w NC Cyber pracuje 24 godziny na dobę, korzystając z tych innowacyjnych narzędzi, aby monitorować polską sieć i w razie potrzeby przekazywać informacje do właścicieli zagrożonych sieci. Służy do tego między innymi platforma **n6**. Jest to usługa dla profesjonalistów – administratorów zajmujących się sieciami w biurach, na osiedlach, w szkołach, firmach. Mogą oni, po rejestracji i uwierzytelnieniu, otrzymywać aktualne dane o incydentach zagrażających ich sieci.

Opracowana przez NASK Platforma n6 funkcjonuje w pełni automatycznie. Dostęp do niej jest bezpłatny. W ciągu roku na platformie są przetwarzane dziesiątki milionów zdarzeń dotyczących bezpieczeństwa z Polski i całego świata. Celem platformy jest efektywne, niezawodne i szybkie dostarczenie dużej liczby informacji o zagrożeniach bezpieczeństwa właściwym podmiotom: właścicielom, administratorom i operatorom sieci.

Źródłem danych systemu n6 jest wiele kanałów dystrybucyjnych przesyłających informacje o zdarzeniach bezpieczeństwa. Zdarzenia te są wykrywane w wyniku działań systemów wykorzystywanych przez różne podmioty zewnętrzne (takie jak inne CERT-y, organizacje bezpieczeństwa, producentów oprogramowania, niezależnych ekspertów od bezpieczeństwa itp.) oraz systemów monitorowania obsługiwanych przez CERT Polska. Większość informacji jest aktualizowana codziennie, niektóre częściej.

W sytuacji, gdy zagrożenia internetowe są zjawiskiem globalnym, dla którego granice państw nie stanowią bariery, narzędzia służące do obrony również muszą działać transgranicznie. NASK jest koordynatorem międzynarodowego konsorcjum firm i instytucji naukowych wspólnie budujących sieć wczesnego ostrzegania dla całej Unii Europejskiej. Projekt o nazwie SISSDEN (Secure Information Sharing Sensor Delivery Event Network) polega na budowie co najmniej 100 stacji monitorowania zagrożeń, składających się ze specjalnie przygotowanych serwerów (przynajmniej po jednym na terytorium każdego z krajów członkowskich UE) wyposażonych w innowacyjne narzędzia do wykrywania i analizy wirusów, botnetów i innych groźnych zjawisk. Ta sieć wczesnego ostrzegania ma w pełni zacząć działać w 2019 r. Już teraz niektóre jej elementy są testowane z sukcesem.

Razem przeciw fali zagrożeń

Współpraca międzynarodowa w przeciwdziałaniu zagrożeniom nie polega jedynie na tworzeniu wspólnej infrastruktury. Często równie wartościowe, lub nawet wartościowsze, jest jednoczenie wysiłków w dążeniu do wspólnego celu – chociażby był on odległy. W gronie ekspertów NASK PIB działa zespół ds. reagowania na szkodliwe i nielegalne treści w Internecie Dyżurnet.pl, który przyjmuje zgłoszenia (również anonimowe) od internautów. Do zespołu wpływają informacje o napotkanych w sieci obrazach zawierających twardą pornografię, przemoc, treści rasistowskie i ksenofobiczne, nakłanianie do przestępstw lub innych szkodliwych działań. Od lat jednak najliczniejszą grupę incydentów (22% w 2016 r.) stanowią materiały prezentujące seksualne wykorzystywanie dzieci (CSAM – ang. *child sexual abuse materials*), nazywane potocznie pornografią dziecięcą. W sytuacji, gdy materiały te znajdują się na serwerze zlokalizowanym w Polsce, Dyżurnet.pl powiadamia Policję i współpracuje z nią, udostępniając wyniki swoich analiz. O treściach umieszczonych na zagranicznych serwerach Dyżurnet.pl informuje współpracujące z nim siostrzane punkty kontaktowe zrzeszone w stowarzyszeniu INHOPE, które jest współfinansowane przez Komisję Europejską oraz firmy sektora informatycznego. Działa już ponad 50 zespołów interwencyjnych w różnych krajach. Materiały są jak najszybciej usuwane ze stron internetowych, a organy ścigania w danym państwie podejmują działania w celu wykrycia sprawców wykorzystywania dzieci, a także publikacji nagrań i zdjęć, na których to przestępstwo zostało utrwalone. Ponadto grupy eksperckie zrzeszone w INHOPE mają dostęp do prowadzonej przez Interpol bazy danych CSAM, w której zdjęcia i filmy są poddawane analizie w celu określenia miejsca przestępstwa oraz tożsamości ofiar i sprawców.

Dyżurnet.pl odnotował w 2016 r. 14 298 incydentów związanych z publikacją nielegalnych lub szkodliwych treści. Ponad trzy tysiące z nich stanowiła tzw. pornografia dziecięca. Przypadki CSAM (ang. *child sexual abuse materials*) umieszczonych na serwerach w Polsce zgłaszane są Policji. Dyżurnet.pl kontaktuje się też z Policją w sytuacjach, gdy internauta zawiadamia o zdarzeniu potencjalnie niebezpiecznym – np. uwodzeniu dziecka w sieci, szantażu internetowym, groźbach, możliwości próby samobójczej itp.

Międzynarodowa współpraca i zaawansowana technologia umożliwiają coraz częściej ściganie sprawców i ochronę ofiar przed dalszym wykorzystywaniem. Skutecznym narzędziem okazała się międzynarodowa baza danych ICSE (International Child Sexual Exploitation), do której trafiają podejrzane materiały foto i wideo z całego świata. W 2017 r. Interpol ogłosił, że w okresie funkcjonowania systemu (od 2011 r.) zidentyfikowano 10 tys. ofiar. W jednym przypadku funkcjonariuszom udało się zidentyfikować, aresztować sprawcę i oswobodzić jego ofiarę zaledwie 10 godzin po tym, jak materiał trafił do bazy danych. Były to zdjęcia, które do bazy wprowadził zespół interwencyjny w Australii. Specjaliści z USA zidentyfikowali miejsce, gdzie zostały wykonane, a następnie wytypowali podejrzanego. Wtedy wydział Interpolu ds. zwalczania przestępstw przeciwko dzieciom zawiadomił służby w kraju europejskim, w którym doszło do wykorzystania dziecka. Obecnie z bazy korzystają służby i zespoły interwencyjne w 49 krajach, również w Polsce. Ostatnio głośne w mediach przypadki aresztowań osób podejrzanych o wykorzystywanie dzieci również były efektem analizy zdjęć z bazy ICSE.

Dyżurnet.pl współpracuje z bazą od listopada 2015 r. Od tego czasu na zgłoszonych do ICSE stronach eksperci Dyżurnet.pl przeanalizowali łącznie 105 876 plików foto i wideo, spośród których zidentyfikowali 22 153 przypadków prezentujących seksualne wykorzystywanie dzieci.

Inną międzynarodową inicjatywą, w której uczestniczą eksperci NASK PIB, jest No More Ransom[4], zainicjowana przez firmy i organizacje działające na rzecz bezpieczeństwa w Internecie. Ma ona na celu ograniczenie skutków stosowania ransomware. Projekt No More Ransom skupia specjalistów, którzy analizują krążące w sieci wirusy, dostarczając wiedzy organom ścigania i – co najważniejsze – opracowują narzędzia deszyfrujące, bezpłatnie udostępniane następnie ofiarom ransomware. Grupa prowadzi też edukację na temat tego zagrożenia i radzi, jak chronić swoje dane, a także, co robić, gdy już dojdzie do ataku. CERT Polska, należący do NC Cyber zespół analityków, dołączył do tego projektu w 2017 r.

CERT Polska działa od 1996 r. Jest to najstarszy tego typu zespół ekspercki w Polsce. Powstał w instytucie badawczym NASK jako odpowiedź na nowe wyzwania bezpieczeństwa, związane z rozwojem Internetu. W momencie powstania Narodowego Centrum Cyberbezpieczeństwa, CERT Polska stał się jego częścią.

CERT Polska przyjmuje zgłoszenia o incydentach bezpieczeństwa, ponadto aktywnie bada zjawiska zachodzące w sieci pod kątem identyfikowania nowych zagrożeń, wypracowywania narzędzi analitycznych i sposobów przeciwdziałania. W ostatnim roku CERT Polska podjął m.in. badania coraz powszechniejszego zjawiska wyłudzeń z wykorzystaniem fałszywych sklepów internetowych. Opracowuje również nowe narzędzia do analizy botnetów, malware i innych zagrożeń aktualnie stanowiących wyzwanie.

Cyfrowa tożsamość w realnych sytuacjach

Wśród działań związanych z bezpieczeństwem publicznym i indywidualnym istotne są również prace NASK PIB dotyczące weryfikacji tożsamości. We współpracy z instytutem powstała i została uruchomiona niedawno przez Ministerstwo Cyfryzacji aplikacja mObywatel, umożliwiająca przechowywanie na smartfonie danych zawartych w dowodzie osobistym. Aplikacja obsługuje dane osobowe w sposób zabezpieczony, pozwalając na udostępnianie wybranej części z nich – np. tylko imienia, nazwiska i adresu zameldowania – pomiędzy użytkownikami.
Naukowcy z NASK PIB biorą też udział w pracach badawczych nad systemem do automatycznego rozpoznawania twarzy. W wyniku projektu BIOWIZ powstanie system do identyfikacji sprawców przestępstw na podstawie materiałów zdjęciowych i/lub wideo. Umożliwią one porównywanie nowych obrazów z istniejącymi w bazie danych wizerunkami sprawców, co usprawni proces analizy np. nagrań z monitoringu. System ma funkcjonować jako narzędzie interaktywne, mogące działać w kilku scenariuszach, np. detekcja twarzy, wyodrębnianie klatek z obrazami twarzy i śledzenie twarzy w materiałach wideo, identyfikacja osoby zaznaczonej na zdjęciach lub materiale wideo na podstawie profilu biometrycznego. Modułowa konstrukcja pozwoli na przyszłe uzupełnianie listy scenariuszy i technik biometrycznych. Wykorzystanie systemu będzie bardzo istotne dla pracy funkcjonariuszy identyfikujących osoby.

Międzynarodowa konferencja na temat bezpieczeństwa teleinformatycznego SECURE, która od wielu lat gromadzi najlepszych specjalistów z tego obszaru z Polski i ze świata, zarówno z sektora prywatnego, jak i publicznego (zdj. archiwum NASK).

Naukowcy rozwijają też technologie związane z biometrią w urządzeniach mobilnych (identyfikacja linii papilarnych, twarzy, wzoru tęczówki).

Narodowe Centrum Cyberbezpieczeństwa zostało powołane w strukturze NASK w lipcu 2016 r. z inicjatywy minister cyfryzacji Anny Streżyńskiej. Jednym z głównym zadań NC Cyber jest inicjowanie współpracy operacyjnej z sektorem prywatnym, w tym z dostawcami usług kluczowych. W NC Cyber funkcjonuje zespół CERT Polska – pierwszy powstały w Polsce zespół reagowania na incydenty (w strukturze NASK od 1996 r.). Głównym obszarem jego działalności jest obsługa incydentów bezpieczeństwa i współpraca z analogicznymi jednostkami na całym świecie zarówno w ramach działalności operacyjnej, jak i badawczo-wdrożeniowej. W strukturze NC Cyber funkcjonuje także centrum operacyjne, które w trybie 24/7 przyjmuje zgłoszenia od operatorów usług kluczowych. Anonimowe zgłoszenia o niebezpiecznych i nielegalnych treściach od użytkowników przyjmuje zespół Dyżurnet.pl, działający w NASK od 2005 r. Rola Narodowego Centrum Cyberbezpieczeństwa zapisana została w opracowanych pod kierunkiem Ministerstwa Cyfryzacji i przyjętych przez rząd w maju 2017 r. Krajowych Ramach Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 oraz w projekcie ustawy o krajowym systemie cyberbezpieczeństwa, która jest obecnie na etapie konsultacji publicznych.

Humanistyczna strona cyberzagrożeń – czynnik ludzki

Zagrożenia internetowe podlegają mutacji i przekształcają się wraz z rozwojem technologii i zmianami rynkowymi. Zmiany te utrudniają klasyfikację źródeł ryzyka, jednak wyraźnie widać zaznaczający się trend, który w uproszczeniu można nazwać humanistycznym. Chociaż do przestępstwa dochodzi w środowisku nowych technologii, sprawcy często stosują jako metodę znane od starożytności socjotechniki, które w Internecie, gdzie nie dochodzi do bezpośredniego kontaktu, okazują się bardzo skuteczne. Przykładem może być zaskakująca kariera oszustwa „na prezesa" (angielski termin CEO Fraud), polegającego na wysłaniu wiadomości e-mail do pracownika firmy z prośbą o pilny przelew na wskazane konto na osobiste polecenie przełożonego. Osoba podająca się za szefa zdobywa pewną wiedzę o firmie i pracowniku, do którego kieruje korespondencję, a następnie wymyśla wiarygodny pretekst niespodziewanej dyspozycji finansowej – np. pilna zaliczka na wynegocjowany właśnie kontrakt. Według Europolu kwota oszustwa może osiągać nawet miliony euro. FBI informuje, że jego centrum powiadamiania o cyberprzestępczości otrzymało w 2016 r. nieco ponad

12 tys. zgłoszeń o tego typu atakach. Łączne straty poniesione przez poszkodowane firmy mogły wynieść ponad 360 mln dolarów. Należy przy tym pamiętać, że tylko część ofiar tego typu oszustw zgłasza się na policję, z obawy przed utratą wizerunku. Jeden z wiodących amerykańskich publicystów poruszających tę tematykę – Brian Krebs szacuje rzeczywisty „utarg" złodziei na ok. 2,4 mld dolarów.

W polskim krajobrazie cyberprzestępczości także dominują oszustwa. Ponad połowę obsłużonych przez CERT Polska incydentów bezpieczeństwa w 2016 r. stanowił *phishing*, czyli próba wyłudzenia poufnych danych. Przykładem może być e-mail przypominający korespondencję z banku, w którym klient jest proszony o potwierdzenie loginu i hasła. Banki ostrzegają klientów i przypominają, że nigdy nie proszą o wysyłanie haseł przez e-mail. Jednak złodzieje liczą na to, że internauta, rozkojarzony lub nieświadomy zagrożenia, poda dane, które później umożliwią im włamanie na jego konto i kradzież pieniędzy.

Również inne szkodliwe zjawiska internetowe, jak przemoc wśród młodzieży – tzw. *cyberbullying*, czyli prześladowanie dziecka przez grupę rówieśniczą, a także różne rodzaje szantażu, w tym coraz popularniejszy *sextortion* (zbitka angielskich słów *sex* i *extortion* – wymuszenie), opierają się na mechanizmach psychologicznych i socjologicznych, a nie na technologii.

W związku z tym tak istotna jest potrzeba edukacji, zwłaszcza młodzieży. Służy temu program Komisji Europejskiej o nazwie „Łącząc Europę", wcześniej funkcjonujący pod nazwą „Safer Internet". Koordynatorem programu w Polsce jest NASK PIB wspólnie z Fundacją Dajemy Dzieciom Siłę. Program oferuje materiały edukacyjne dla młodzieży oraz rodziców i osób pracujących w oświacie – nauczycieli, pedagogów, psychologów. NASK PIB podejmuje również własne działania w tym zakresie w ramach Akademii NASK oraz platformy e-learningowej IT Szkoła.

NASK PIB koncentruje też wiele swoich działań na promowaniu współpracy i budowaniu wzajemnego zaufania pomiędzy różnymi środowiskami, dla których ważne jest bezpieczeństwo Internetu. Doświadczenia, nie tylko polskie, pokazują, że najskuteczniejszą obroną przed poważnymi atakami jest gromadzenie specjalistycznej wiedzy i wymienianie się nią w gronie potencjalnych ofiar. Jeśli jeden podmiot padnie ofiarą hakerów, może ostrzec innych, którzy już się nie dadzą zaatakować w ten sam sposób.

Ten rodzaj współpracy jest konieczny na każdym szczeblu. Powinniśmy się dzielić informacjami o zaistniałych oraz potencjalnych zagrożeniach w obrębie branż, na poziomie krajowym oraz w sieci międzynarodowej. Unia Europejska stymuluje taką współpracę. Ma temu służyć powołanie krajowych centrów koordynacyjnych we wszystkich państwach członkowskich, wymagane przez obowiązującą od ubiegłego roku dyrektywę NIS[5]. Takim ośrodkiem w Polsce jest właśnie NC Cyber w NASK PIB. Również policja bierze udział w naszych działaniach na rzecz pogłębiania współpracy, uczestnicząc we wspólnych ćwiczeniach z ekspertami. Pokazują one w praktyce, że dopełniając wzajemnie nasze kompetencje, możemy zredukować czas potrzebny na rozwiązanie problemu i uzyskać lepsze rezultaty, niż pracując w izolacji. Wierząc, że kluczowym instrumentem przeciwdziałania zagrożeniom jest wiedza, staramy się budować sieć wymiany informacji, nie tylko między ekspertami i nie tylko na krajowym podwórku. Przyszłością globalnej sieci – jeśli ma być bezpieczna – musi być szeroko zakrojona współpraca. Zagrożenia internetowe nie respektują granic państw, więc obrona przed nimi również musi być globalna.

NASK jest Państwowym Instytutem Badawczym podległym Ministerstwu Cyfryzacji. Siedziba instytutu znajduje się w Warszawie. Instytut prowadzi działalność badawczo-rozwojową w zakresie bezpieczeństwa i efektywności systemów ICT. W strukturze NASK PIB od lipca 2016 r. działa Narodowe Centrum Cyberbezpieczeństwa, którego celem jest koordynacja działań na rzecz rozwijania współpracy w zakresie cyberbezpieczeństwa wśród podmiotów świadczących kluczowe dla społeczeństwa usługi. W instytucie działają też wyodrębnione zespoły eksperckie – Dyżurnet.pl oraz CERT Polska, które również weszły do struktury NC Cyber. NASK PIB uczestniczy w międzynarodowych inicjatywach prowadzonych przez instytucje międzynarodowe lub organizacje pozarządowe, m.in. w programie Komisji Europejskiej Safer Internet (obecnie „Łącząc Europę").

[1] Ransomware (z ang. – zbitka wyrazowa powstała ze słów *ransom* „okup" i *software* „oprogramowanie") to rodzaj szkodliwego oprogramowania, które blokuje system komputerowy lub go szyfruje, a następnie żąda od ofiary okupu za przywrócenie dostępu, https://pl.wikipedia.org/wiki/Ransomware [dostęp: 24.11.2017 r.].

[2] https://ec.europa.eu/poland/news/170913_soteu_live_pl [dostęp: 24.11.2017 r.].

[3] Złośliwe oprogramowania (z ang. *malware* – zbitka wyrazowa powstała ze słów – *malicious* „złowrogi, złośliwy" i *software* – „oprogramowanie") to wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze, groźne lub destrukcyjne działanie w stosunku do użytkownika komputera, https://pl.wikipedia.org/wiki/Złośliwe_oprogramowania [dostęp: 24.11.2017 r.].

[4] http://www.nomoreransom.org/en/index/html [dostęp: 21.11.2017 r.].

[5] NIS – Dyrektywa Parlamentu i Rady UE w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, https://wwww.bs.net.pl/prawo/dyrektywa-nis [dostęp: 24.11.2017 r.].

Summary

Polish cyber-security system – together for common safety

The scale of threats related to the use of the Internet requires a comprehensive response. It is necessary to develop technological tools, such as systems for automatic detection of threats, their analysis and exchange of information, including international surveillance infrastructure. It is currently one of the most important areas of research and development activity of the NASK National Research Institute. SOC (Security Operation Center) in NC Cyber is working 24 hours a day using these innovative tools to monitor our network and, if necessary, relay information to endangered network owners. This is possible, for example, thanks to the n6 platform. It is a service for professionals – administrators of networks in offices, housing complexes, schools, businesses.

The second important condition for maintaining security is social awareness. Many threats involve fraud, manipulation, deceptive manipulation, or attempts to obtain security data (e.g. banking passwords). Prevention of this type of crime is done primarily by user education. NASK PIB organizes educational activities aimed at adults (including seniors) and children and youth as part of the European Commission's Safer Internet program and within the NASK Academy and e-learning portal IT Szkoła.

Security means also counteracting the distribution of illegal and harmful content online. This is the role of intervention team Dyżurnet.pl, which receives reports (also anonymous) from Internet users about disturbing content.

KOMPLEKSOWE PODEJŚCIE DO WYŁANIANIA I OCHRONY INFRASTRUKTURY KRYTYCZNEJ

dr inż. Witold Skomra

Doradca
Rządowe Centrum Bezpieczeństwa

Technologie cyfrowe z jednej strony poprawiają jakość usług świadczonych na rzecz obywateli, ale równocześnie są źródłem nowych zagrożeń. W efekcie, poza dotychczasowymi rodzajami zarządzania bezpieczeństwem (bezpieczeństwem fizycznym czy technicznym) pojawiają się jego nowe formy, będące odpowiedzią na nowe zagrożenia (bezpieczeństwo cybernetyczne, bezpieczeństwo danych osobowych itp.). Te zróżnicowane działania, aby mogły osiągnąć zamierzony efekt, powinny być traktowane jako elementy większej całości. Ta większa całość to kompleksowe zarządzanie bezpieczeństwem obejmujące nie tylko działania na rzecz własnej jednostki, ale uwzględniające zarówno oddziaływanie podmiotów zewnętrznych, jak i ewentualne skutki społeczne, jakie może spowodować dysfunkcja usług, które podmiot dostarcza. Podejście usługowe jako metoda pozwalająca na hierarchizację procesów realizowanych w ramach administracji publicznej to zupełnie nowe zagadnienie wymagające zarówno zmian mentalnych wśród kadry zarządzającej, jak i dostosowania struktur formalnych do wymagań związanych z koniecznością wdrożenia nowych form zarządzania bezpieczeństwem.

WPROWADZENIE

Współczesne życie społeczne jest determinowane przez technologie cyfrowe oraz systemy teleinformatyczne. Proces cyfrowej transformacji dotyczy zarówno obszaru biznesu, jak i działań administracji publicznej. Towarzyszą mu nowe zagrożenia i powiązane z nimi ryzyka. Powstają przy tym wzajemne współzależności, w efekcie czego kto inny może być właścicielem infrastruktury (i ryzyk z nią związanych), a kto inny właścicielem skutków wynikających z dysfunkcji tej infrastruktury (ryzyko związane ze skutkami społecznymi). Nawet jeśli potrafimy precyzyjnie określić, czy infrastruktura jest w posiadaniu administracji czy podmiotu prywatnego, to wcale nie musi oznaczać, że potrafimy określić, kto jest odpowiedzialny za wtórne skutki awarii tej infrastruktury. To, że administracja publiczna nie może się obyć bez energii elektrycznej dostarczanej przez podmioty gospodarcze, jest dla wszystkich oczywistością. Natomiast nie jest już tak oczywiste, że administracja, poprzez rejestry państwowe czy dostarczanie programów do rozliczania podatków, oddziałuje na procesy realizowane przez świat biznesu. W tym drugim przypadku można wręcz stwierdzić, że działalność administracji jest źródłem ryzyka operacyjnego dla podmiotu gospodarczego. Już ten pobieżny przegląd zjawisk, z jakimi mamy do czynienia, wskazuje, że wyłanianie i kompleksowa ochrona infrastruktury krytycznej (w skrócie IK) muszą być stale dostosowywane do rzeczywistości technicznej, gospodarczej i społecznej.

Formalne podstawy ochrony IK

Podstawową regulacją prawną w tym zakresie jest ustawa o zarządzaniu kryzysowym[1] (w skrócie uzk), która reguluje tryb wyłaniania obiektów IK, zasady i obowiązki w zakresie ich ochrony, a także zasady współpracy administracji i podmiotów gospodarczych na rzecz tej ochrony. Należy jednak zwrócić uwagę, że ustawodawca za ochronę IK uznał również zapewnienie jej funkcjonalności oraz ciągłości działania, a nie tylko zapewnienie funkcjonowania i szybkiego odtworzenia. Obecne brzmienie terminu ochrony IK jest efektem implementacji dyrektywy Rady w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony[2]. Zgodnie z art. 2 dyrektywy ochrona zdefiniowana została jako wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności IK w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków. Tę definicję zaimplementowano poprzez uzk. W efekcie ustawa określa, że IK ma być chroniona przed wszelkimi zagrożeniami, zarówno spowodowanymi działalnością ludzką (np. atakiem terrorystycznym), jak i przed zagrożeniami naturalnymi czy będącymi skutkiem awarii technicznej[3].

Zgodnie z filozofią uzk dyrektor RCB został zobowiązany do przygotowania w porozumieniu z właściwymi ministrami oraz kierownikami urzędów centralnych wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład IK. Po jego sporządzeniu dyrektor RCB sporządza wyciągi z wykazu dla ministrów i kierowników urzędów centralnych odpowiedzialnych za poszczególne systemy IK oraz wojewodów, na których terenach znajduje się dana infrastruktura. Ponadto dyrektora RCB zobowiązano do poinformowania właścicieli i posiadaczy IK o ujęciu ich obiektów w omawianym wykazie. Ustawodawca upoważnił wojewodę do poinformowania odpowiednich organów administracji publicznej o infrastrukturze znajdującej się na terenie danego województwa, co powoduje, że informacja o IK przekazywana jest jedynie niezbędnym podmiotom. Jednak w celu właściwej realizacji zadań z zakresu IK może zaistnieć potrzeba, by poszczególni wojewodowie, jak i inne organy administracji publicznej mogły się dowiedzieć o ujętej w wykazie infrastrukturze, która może mieć wpływ na realizację ich zadań. W tym celu uzk pozwala organom właściwym w sprawach zarządzania kryzysowego oraz dyrektorowi RCB żądać udzielenia informacji, gromadzenia i przetwarzania danych niezbędnych do realizacji ustawowych zadań[4].

Zazwyczaj ochrona infrastruktury kojarzona jest z ochroną fizyczną. Warto zatem wspomnieć, że zagadnienie to zostało już rozwiązane postanowieniami ustawy o ochronie osób i mienia[5] (UoOOiM). Zgodnie z nią obowiązek stosowania odpowiednich form ochrony obejmuje obszary, obiekty, urządzenia i transporty ważne dla obronności, interesu gospodarczego państwa, bezpieczeństwa publicznego i innych ważnych interesów państwa. Ustawa wprost wskazuje, że jej postanowienia są rozciągnięte na obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi ujęte w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej. Jednak zakres jej oddziaływania jest znacznie szerszy i dotyczy obiektów, które nie są uznawane za IK.

Organem nadzorującym wykonanie obowiązków wynikających z UoOOiM jest komendant wojewódzki Policji, który zatwierdza plany ochrony obiektu oraz sprawuje nadzór nad funkcjonowaniem wewnętrznych służb ochrony (w zakresie zagrożeń o charakterze terrorystycznym plany uzgadnia właściwy terytorialnie dyrektor delegatury Agencji Bezpieczeństwa Wewnętrznego). Nadzór nad firmami zajmującymi się ochroną fizyczną (specjalistycznymi uzbrojonymi formacjami ochronnymi, w skrócie SUFO) sprawuje Komendant Główny Policji, ale realizuje to zadanie poprzez komendanta wojewódzkiego.

Do wyłonienia obiektów i obszarów istotnych dla społeczności lokalnych oraz w celu zapewnienia właściwego poziomu ich ochrony, konieczna jest **współpraca następujących organów**:

- **wójta, burmistrza lub prezydenta miasta** (ustalenie stopnia ważności obiektu dla społeczności lokalnej, szczególnie dla funkcjonowania aglomeracji miejskich);
- **szefa ABW** (określenie poziomu wrażliwości obiektu na ewentualny atak terrorystyczny);
- **wojewody** (decyzje administracyjne związane z wykazem obiektów podlegających ochronie);
- **komendanta wojewódzkiego Policji** (zatwierdzanie planu ochrony obiektu, nadzór nad funkcjonowaniem służb ochrony).

Niekiedy utrzymywanie pełnej ochrony fizycznej obiektu jest ekonomicznie nieuzasadnione. W takim przypadku w planach ochrony obiektów można zawrzeć różne formy ochrony stosowane w zależności od stopnia zagrożenia.

Jednak ochrona fizyczna to tylko jeden z elementów kompleksowej ochrony IK. Działania podejmowane na rzecz zapewnienia bezpieczeństwa mają na celu minimalizację ryzyka zakłócenia IK przez:

- zmniejszenie prawdopodobieństwa wystąpienia zagrożenia,
- zmniejszanie podatności,
- minimalizowanie skutków wystąpienia zagrożenia.

Na te działania składają się:

- **zapewnienie bezpieczeństwa fizycznego** – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które w sposób nieautoryzowany podjęły próbę dostania się lub znalazły się na terenie IK;
- **zapewnienie bezpieczeństwa technicznego** – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie zaburzenia realizowanych procesów technologicznych;
- **zapewnienie bezpieczeństwa osobowego** – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie działań osób, które posiadają uprawniony dostęp do infrastruktury krytycznej;
- **zapewnienie bezpieczeństwa teleinformatycznego** – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie nieautoryzowanego oddziaływania na aparaturę kontrolną oraz systemy i sieci teleinformatyczne;
- **zapewnienie bezpieczeństwa prawnego** – zespół działań organizacyjnych i technicznych mających na celu minimalizację ryzyka zakłócenia funkcjonowania IK w następstwie prawnych działań podmiotów zewnętrznych;
- **plany ciągłości działania i odtwarzania**, rozumiane jako zespół działań organizacyjnych i technicznych prowadzących do utrzymania i odtworzenia funkcji realizowanych przez IK.

Zastosowanie konkretnych środków zapewnienia bezpieczeństwa powinno być ściśle związane z oceną ryzyka zakłócenia funkcjonowania IK[6].

Zgodnie z uzk ochrona IK spoczywa przede wszystkim na właścicielach oraz posiadaczach samoistnych i zależnych obiektów, instalacji lub urządzeń IK. W celu zapewnienia ochrony IK Rada Ministrów wydała rozporządzenie, które określa sposób tworzenia i aktualizacji planów ochrony IK oraz zapewnia warunki i tryb uznania spełnienia obowiązku posiadania planu ochrony. Warunkiem niezbędnym jest, by posiadany już plan spełniał wymagania określone w rozporządzeniu RM w sprawie planów ochrony IK[7].

Właściciel lub posiadacz IK, poza elementami wymaganymi w myśl rozporządzenia, może zawrzeć w planie dodatkowe informacje, które są związane z jej specyficznym charakterem. W celu skorelowania planów ochrony z przygotowywanymi planami zarządzania kryzysowego oraz innymi przepisami z zakresu zarządzania kryzysowego plany wymagają uzgodnienia z następującymi organami:

1) w zakresie ich dotyczącym z właściwymi terytorialnie:
   a) wojewodą,
   b) komendantem wojewódzkim PSP,
   c) komendantem wojewódzkim Policji,
   d) dyrektorem regionalnego zarządu gospodarki wodnej,
   e) wojewódzkim inspektorem nadzoru budowlanego,
   f) wojewódzkim lekarzem weterynarii,
   g) państwowym wojewódzkim inspektorem sanitarnym,
   h) dyrektorem urzędu morskiego;
2) z ministrem lub kierownikiem urzędu centralnego, we właściwości którego znajduje się system, do którego została zaliczona dana IK[8].

Plany, zarówno już posiadane, jak i opracowane na nowo, zatwierdzane są przez dyrektora RCB. Mając na uwadze, że nie wszyscy właściciele oraz posiadacze IK mogą posiadać odpowiednie poświadczenia i warunki przetwarzania informacji niejawnych, do planów stosować można przepisy o ochronie informacji niejawnych albo o ochronie tajemnicy przedsiębiorstwa. Plany podlegają aktualizacji w zależności od potrzeb, ale nie rzadziej niż raz na dwa lata.

Odpowiedzialność za ochronę IK

Jak już zostało wyżej wspomniane, ciężar ochrony IK spoczywa na jej operatorach. Zasadę, że to operator odpowiada za ochronę obiektów IK, podkreślają dokumenty planistyczne. W ustawie zrezygnowano z przygotowywania krajowego planu ochrony IK oraz planów wojewódzkich (pojęcie takich planów istniało w pierwotnej wersji uzk z 2007 r.). Obowiązek sporządzania planów ochrony IK spoczywa tylko na operatorach. Jednak biorąc pod uwagę znaczenie IK dla funkcjonowania państwa, ustawodawca zadania z zakresu ochrony tejże infrastruktury przypisał również podmiotom administracji publicznej. Nie można sobie wyobrazić, by władze publiczne, mając na uwadze potencjalne skutki awarii IK dla ludzi, ich mienia, gospodarki narodowej czy środowiska, odmówiły pomocy poszkodowanym, pozostawiając ten problem wyłącznie operatorowi IK. I bez znaczenia jest tu fakt, czy IK jest w zarządzie administracji publicznej, czy pozostaje całkowicie we władaniu podmiotów gospodarczych. Właśnie ze względu na spodziewane skutki awarii IK zadania z zakresu jej ochrony realizowane są na wszystkich szczeblach administracji, począwszy od administracji rządowej, a skończywszy na administracji samorządowej. Między innymi elementy związane z operacyjnymi działaniami w obszarze ochrony IK stały się załącznikami funkcjonalnymi do planów zarządzania kryzysowego[9].

W ramach działań podejmowanych przez administrację państwową szczególna rola przypada Szefowi ABW. Ustawodawca przypisał mu wiodącą rolę w sytuacji zagrożeń terrorystycznych dla IK. Ponieważ administracja publiczna, poza nielicznymi wyjątkami, nie ma możliwości prowadzenia kontroli w podmiotach gospodarczych, proces zatwierdzania planu jest podstawową formą działań mających na celu zmniejszenie poziomu ryzyka w obiektach IK. Dopiero po wprowadzeniu 2. lub wyższego stopnia alarmowego administracja aktywnie włącza się do działań mających chronić obiekty IK. Między innymi Szef ABW, w uzgodnieniu z ministrem właściwym do spraw wewnętrznych, może wydać Policji zalecenie szczególnego zabezpieczenia poszczególnych obiektów uwzględniające rodzaj zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym[10].

Dwoistość postrzegania IK

W tym miejscu warto zwrócić uwagę na pewien paradoks związany z istnieniem IK. Dla jej właściciela (operatora) infrastruktura powinna przede wszystkim służyć osiąganiu zysku. W razie awarii straty powinny być pokryte ze środków własnych (w ramach bezpieczeństwa finansowego prowadzonej działalności) albo wyrównane poprzez ubezpieczenie (przeniesienie ryzyka na podmiot zewnętrzny). Decyzję o odbudowie powinna poprzedzić analiza kosztów (być może infrastruktury nie opłaca się odbudowywać, a przynajmniej nie w dotychczasowej for-

Rysunek 1. Podział skutków zdarzenia ze względu na podmiot odpowiedzialny. *Źródło: opracowanie własne.*

mie). Z punktu widzenia odbiorcy usługi, infrastruktura, a precyzyjniej usługa świadczona przez infrastrukturę, powinna zostać odtworzona w jak najkrótszym czasie, bez względu na koszty. Stąd wynika dwoistość postrzegania ochrony IK. Jednocześnie należy chronić obiekt IK oraz społeczność, którą mogą dotknąć skutki dysfunkcji IK. Za ochronę przed społecznymi skutkami awarii IK odpowiada już administracja publiczna. Zakres tych skutków można wywnioskować z definicji zawartych w ustawie o zarządzaniu kryzysowym. Zgodnie z ustawą, ilekroć mowa o sytuacji kryzysowej, należy przez to rozumieć: „sytuację wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej". W odniesieniu do obiektów IK ustawa posługuje się dodatkowo takimi pojęciami, jak: „kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców" (uzk, art. 3).
Biorąc powyższe pod uwagę, można dokonać podziału skutków zdarzeń ze względu na właściciela ryzyka (rys. 1).
Uogólniając powyższe spostrzeżenie, omawiany rysunek można zinterpretować następująco.

Dla właściciela (operatora IK) infrastruktura przez niego zarządzana powinna służyć przede wszystkim osiąganiu celów biznesowych (zysku). Jednocześnie ta sama infrastruktura powinna, poza celami biznesowymi, uwzględniać aspekt społeczny, jeśli prowadzona działalność lub jej czasowe zaprzestanie mogą wywołać skutki dla ludzi, ich mienia lub środowiska. Próby zdefiniowania, czym jest taka infrastruktura biznesowo-społeczna, podejmowane są w ramach badań naukowych nad logistyką społeczną. W ramach nich stwierdzono, że istnieją pewne usługi, np. związane z ratowaniem zagrożonego życia i zapewnieniem bezpieczeństwa (publicznego oraz w przestrzeni publicznej), które nie są realizowane z potrzeby zysku. Jednak grupę podmiotów kierujących się takimi celami ograniczono do organizacji non profit [Szołtysek, 2014, s. 5]. Inaczej podeszli do tego zagadnienia twórcy podziału logistyki na wojskową, cywilną i kryzysową. Według tej koncepcji głównym celem działania logistyki cywilnej jest maksymalizacja zysku przedsiębiorstwa, zaś logistyki kryzysowej – zaspokojenie elementarnych potrzeb logistycznych ludności. W tym drugim przypadku rachunek ekonomiczny ma znaczenie trzeciorzędne [Nowak, Nowak, 2009]. Oba te podejścia nie oddają w pełni, czym jest IK, i to zagadnienie wymaga dalszych badań.

Niezależnie jednak od prób zdefiniowania, czym jest IK jednocześnie z biznesowego i społecznego punktu widzenia, należy stwierdzić, że usługi (oraz związane z nimi procesy, podprocesy i procedury) dostarczane przez tę infrastrukturę można podzielić na takie, które służą wyłącznie celom biznesowym, i takie, których dysfunkcja wywoła społeczne skutki na tyle dolegliwe, że zarządzać nimi będzie musiało państwo. To stwierdzenie pozwala zadać pytanie, czy obecnie stosowany sposób wyłaniania obiektów IK uwzględnia aspekt społeczny. Aby udzielić odpowiedzi, konieczne jest spojrzenie na IK poprzez usługi, jakich ta infrastruktura dostarcza. Aby zrozumieć ideę podejścia usługowego, należy zauważyć, że operator IK nie jest właścicielem wszystkich ryzyk (a więc i skutków zdarzeń niekorzystnych) związanych z prowadzoną działalnością. W skali makroekonomicznej działania podmiotów gospodarczych mają wymiar społeczny i w tym przypadku właścicielem ryzyka staje się państwo. Dotyczy to nie tylko awarii i ich skutków, ale również zagadnień związanych z wyczerpywaniem się zasobów, zmianami w środowisku naturalnym czy zagospodarowaniem przestrzennym.

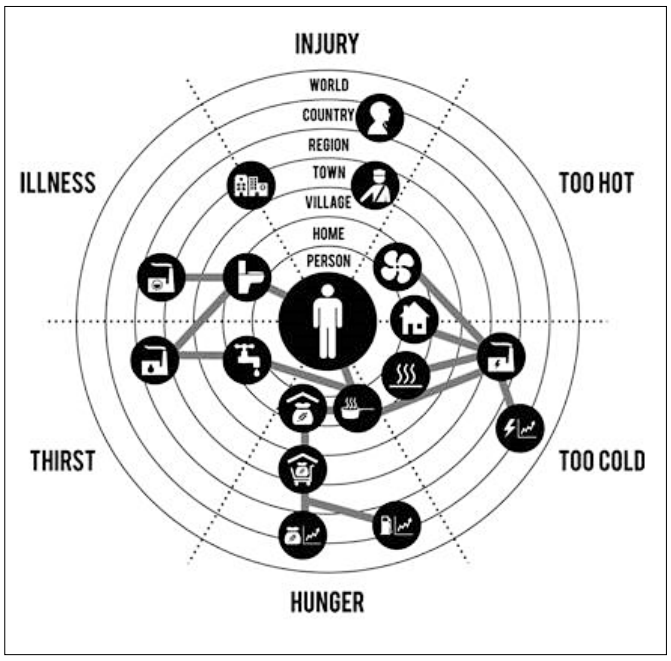
Społeczne skutki dysfunkcji IK

Wracając jednak na grunt sytuacji kryzysowych, trzeba podkreślić, że to oddziaływanie ma charakter bardziej dynamiczny i kompleksowy. Przykładowo – brak prądu w skali mikroekonomicznej oznacza dla elektrowni brak zysków i ewentualnie konieczność wypłaty odszkodowań. W skali makroekonomicznej brak prądu może oznaczać dla odbiorcy brak dostępu do pieniądza (nie działają bankomaty), brak możliwości przemieszczania się (niemożność zatankowania pojazdu) czy trudności z zakupem żywności (znaczna część produktów spożywczych wymaga chłodni). Te rodzaje ryzyk nie wchodzą w zakres odpowiedzialności elektrowni. Narzędziem do regulacji odpowiedzialności i podejmowania działań są w takiej sytuacji rozwiązania ustawowe. Podstawy teoretyczne pozwalające na zastosowanie podejścia usługowego w administracji publicznej istnieją od dawna, jednak dopiero cyfryzacja administracji oparta na realizowanych procesach przyśpieszyła te zmiany. Przykładowo, zorientowanie na procesy w administracji publicznej i usługi, jakie ona zapewnia, jest jedną z czterech podstawowych zasad, na których opiera się informatyzacja zintegrowana wdrażana w ramach e-administracji.
W efekcie w administracji publicznej można obserwować ten sam trend, który nastąpił w działalności biznesowej, gdzie podejście procesowe zaczyna dominować nad podejściem systemowym [Zawiła-Niedźwiedzki, Gołąb, 2010, s. 214]. Należy przyjąć, że ten kierunek działań zapewne będzie się pogłębiać, biorąc pod uwagę postanowienia dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[11] (tzw. dyrektywa NIS). Dyrektywa nakłada obowiązek wyłonienia przez państwa członkowskie tzw. usług kluczowych, tj. takich, które służą utrzymaniu „krytycznej działalności społecznej i gospodarczej". Formalnie dyrektywa odnosi się wyłącznie do bezpieczeństwa sieci i systemów teleinformatycznych w niektórych sektorach (energetyka, transport, bankowość i instytucje kredytowe, infrastruktura rynków finansowych, służba zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, infrastruktura cyfrowa). Jednak celem szerszego zastosowania podejścia usługowego w dziedzinie ochrony IK, w RCB trwają prace koncepcyjne nad nową procedurą wyłaniania IK w oparciu o wcześniej zdefiniowaną listę usług kluczowych. Pierwszym krokiem na tej drodze jest ustalenie listy kryteriów, które uznajemy za krytyczne. Pomocna w tym przypadku może być metodyka „6 ways to die". Zgodnie z tym podejściem rolą administracji publicznej jest eliminacja sześciu czynników, które mogą spowodować śmierć człowieka. Tymi czynnikami są:

- głód,
- pragnienie,

- zranienia,
- choroby,
- zbyt wysoka temperatura,
- zbyt niska temperatura.

Jeśli dodamy do tych czynników niezbędne usługi z nimi związane i kolejne poziomy administracji, powstaje graf obrazujący wzajemne zależności:



Rysunek 2. Mapa infrastruktury krytycznej i jej poziomów.
Źródło: Źródło: Bennett, Gupta, 2010; za: Pyznar, Abgarowicz, 2014, s. 16.

Jak widać na rysunku, każdemu czynnikowi mogącemu spowodować śmierć osoby, można przypisać procesy i systemy oraz szczebel administracji odpowiedzialny za ich sprawne działanie (co nie oznacza, że administracja musi być operatorem danego systemu). Przykładowo – w ramach systemu „zaopatrzenie w wodę" można wyodrębnić procesy:

- ujmowanie i uzdatnianie wody przeznaczonej do spożycia przez ludzi;
- dostarczanie wody przeznaczonej do spożycia przez ludzi;
- odbiór i oczyszczanie ścieków.

Każdemu z nich można przypisać prawdopodobieństwo awarii i ocenić spodziewane skutki, wyliczając poziom ryzyka. Skutki można sparametryzować i przypisać do poszczególnych poziomów administracji, uzyskując w ten sposób podział na krytyczną infrastrukturę lokalną, regionalną i centralną (krajową). Przykładowo – lokalna IK może oznaczać brak usługi dla 100 tys. osób i więcej, regionalna powyżej 300 tys., zaś krajowa powyżej 500 tys. Przy okazji każdemu poziomowi można przypisać odpowiedni poziom ochrony, tak by niezbędne nakłady finansowe były adekwatne do poziomu ryzyka.

Proces wyłaniania obiektów IK przy takim podejściu składałby się z dwóch etapów:

- zidentyfikowanie usług krytycznych świadczonych przez dany obiekt;
- określenie skutków dysfunkcji danej usługi i porównanie z kryteriami przekrojowymi definiującymi IK lokalne, regionalne i krajowe.

Na koniec można wskazać niezbędny poziom zabezpieczeń adekwatny do klasy IK (lokalna, regionalna lub krajowa) i poziomu ryzyka.

Pierwszym etapem wdrożenia kompleksowej ochrony IK w rozumieniu usługowym jest uświadomienie decydentom skali złożoności problematyki związanej z całościowym ujęciem bezpieczeństwa. To z kolei wymaga ścisłej współpracy między administracją publiczną a właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń IK. W celu stworzenia przejrzystego i prostego sposobu kontaktu administracji z właścicielami i posiadaczami IK zostali oni zobowiązani do wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony IK[12]. Ta zasada nieco inaczej jest realizowana w odniesieniu do podmiotów działających w sektorach energii elektrycznej, ropy naftowej i paliw gazowych.

Zgodnie z ustawą o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych zarząd spółki, w porozumieniu z ministrem właściwym do spraw Skarbu Państwa[13] oraz dyrektorem RCB, powołuje i odwołuje pełnomocnika do spraw ochrony infrastruktury krytycznej[14]. Pełnomocnik do spraw ochrony infrastruktury krytycznej jest pracownikiem spółki monitorującym jej działalność w zakresie działań, co do których minister Skarbu Państwa ma prawo zgłoszenia sprzeciwu. Ponadto pełnomocnik może być odpowiedzialny za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej i ma wiele dodatkowych zadań ustawowych. W efekcie powstały dwa różne systemy organizacyjne ochrony obiektów IK ze strony jej właściciela lub posiadacza. Pierwszy, wynikający z uzk, zakłada, że administracja rządowa nie ingeruje w strukturę organizacyjną podmiotu i zakres zadań osoby odpowiedzialnej za bezpieczeństwo IK. Drugi, wynikający z ustawy o szczególnych uprawnieniach (…), opiera się na ingerencji w strukturę podmiotu zarządzającego IK i ściśle zdefiniowanych ustawowo zadaniach pełnomocnika do spraw ochrony IK. Przy okazji pojawiły się dwa różne określenia osoby zajmującej się taką ochroną. Raz jest to „osoba odpowiedzialna za kontakty", w drugim przypadku „pełnomocnik do spraw ochrony IK". Wydaje się, że w dłuższej perspektywie taka dwoistość w podejściu do ochrony IK powinna zostać zlikwidowana na rzecz tego drugiego rozwiązania.

Niezależnie od tego, która ustawa reguluje zasady organizacyjne, z całą stanowczością należy podkreślić, że jedynie dobra współpraca pomiędzy osobą odpowiedzialną za utrzymywanie kontaktów (ewentualnie pełnomocnika) a właściwymi podmiotami, w zakresie których leżą zadania z zakresu ochrony IK, daje gwarancję, iż opisany w niniejszym artykule mechanizm jej ochrony przyniesie spodziewane rezultaty.

PODSUMOWANIE

Całościowe podejście do ochrony IK wymaga kompleksowego zarządzania ryzykiem w rozumieniu oddziaływania na przyczynę (źródło zagrożenia), środowisko, w którym ryzyko może się rozprzestrzeniać (redukowanie podatności), oraz skutki (zarówno w aspekcie technicznym, finansowym, jak i społecznym). Jednocześnie wszystkie formy ochrony muszą być traktowane jako równie istotne. Zatem zarówno ochrona fizyczna, jak i ochrona teleinformatyczna (jak i wszystkie pozostałe) muszą być traktowane równorzędnie, jako element zarządzania bezpieczeństwem.

[1] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209, z późn. zm.).

[2] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. Urz. UE L 345/75).

[3] W kwestii ochrony IK na świecie widoczne są dwa trendy. Pierwszy, w którym ochrona IK nakierowana jest głównie na zagrożenia przed atakami terrorystycznymi, i drugi, w którym ochrona ma na celu przeciwdziałanie wszelkim zagrożeniom. Należy zauważyć, że powoli zmienia się podejście państw w tej kwestii i działania ochrony kierowane są na przeciwdziałanie wszelkim zagrożeniom. Całościowe podejście obejmuje jednocześnie zagrożenia dla IK i zagrożenia powodowane przez dysfunkcję IK. Przykładem kraju, gdzie obowiązuje takie podejście, są Stany Zjednoczone Ameryki.

[4] Tamże, art. 20a.

[5] Ustawa z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz. U. z 2016 r. poz. 1432, z późn. zm.).

[6] NPOIK, RCB 2015, s. 31–32.

[7] Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej (Dz. U. Nr 83, poz. 542).

[8] Tamże, § 4 ust. 1.

[9] Art. 12 ust. 2 pkt 4, art. 14 ust. 2 pkt 7, art. 15, art. 17 ust. 2 pkt 6, art. 19 ust. 2 pkt 6 uzk.

[10] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. poz. 904, z późn. zm.).

[11] Dyrektywa Parlamentu i Rady UE 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1).

[12] Art. 6 ust. 5a ustawy o zarządzaniu kryzysowym.

[13] W odniesieniu do operatora systemu przesyłowego elektroenergetycznego i operatora systemu przesyłowego gazowego rolę ministra właściwego do spraw Skarbu Państwa realizuje Pełnomocnik rządu do spraw Strategicznej Infrastruktury Energetycznej. Zob. szerzej: rozporządzenie Rady Ministrów z dnia 3 grudnia 2015 r. w sprawie Pełnomocnika Rządu do spraw Strategicznej Infrastruktury Energetycznej (Dz. U. poz. 2116).

[14] Zob. szerzej: ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych (Dz. U. z 2016 r. poz. 2012).

Bibliografia

Bennett M., Gupta V., *Dealing in Security understanding vital services and how they keep you safe*, http://resiliencemaps.org/files/Dealing_in_Security.July2010.en.pdf [dostęp: 7.11.2017 r.].

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194/1 z 19.7.2016 r.).

Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. Urz. UE L 345/75 z 8.12.2008 r.).

Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK) z dnia 2 listopada 2015 r. przyjęty uchwałą Rady Ministrów nr 210/2015 z uwzględnieniem uchwały nr 61/2016 Rady Ministrów z dnia 1 czerwca 2016 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej, http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2015-Dokument-G%C5%82%C3%B3wny-tekst-jednolity.pdf [dostęp: 7.11.2017 r.].

Nowak W., Nowak E., *Podstawy logistyki w sytuacjach kryzysowych z elementami zarządzania logistycznego*, SWSPiZ, Łódź–Warszawa 2009.

Pyznar M., *Narodowy Program Ochrony Infrastruktury Krytycznej w systemie ochrony tej infrastruktury – wizja Rządowego Centrum Bezpieczeństwa*, w: *Ochrona infrastruktury krytycznej*, red. A. Tyburska, Wydawnictwo WSPol Szczytno, 2010.

Pyznar M., Abgarowicz G., *Rola infrastruktury krytycznej w funkcjonowaniu państwa*, w: *Bezpieczeństwo infrastruktury krytycznej wymiar teleinformatyczny*, red J. Świątkowska, Instytut Kościuszki, Kraków 2014.

Skomra W., *Ochrona Infrastruktury Krytycznej w systemie zarządzania kryzysowego*, w: *Ochrona infrastruktury krytycznej*, red. A. Tyburska, Wydawnictwo WSPol, Szczytno 2010.

Skomra W., *Zarządzanie kryzysowe – praktyczny przewodnik*, Wydawnictwo Presscom, Wrocław 2016.

Szołtysek J., *Przesłanki i założenia koncepcji logistyki społecznej*, „Gospodarka Materiałowa i Logistyka" 2014, nr 2.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). Public Law 107–56, OCT. 26, 2001.

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. poz. 904, z późn. zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2017 r. poz. 209, z późn. zm.).

Zapłata S., Kaźmierczak M., *Ryzyko, ciągłość biznesu, odpowiedzialność społeczna. Nowoczesne koncepcje zarządzania*, Oficyna Wolter Kluwer Business, Warszawa 2011.

Zawiła-Niedźwiecki J., Gołąb P., *Zapewnienie ciągłości działania jako ograniczenie ryzyka operacyjnego*, w: *Zarządzanie ryzykiem działalności organizacji*, red. J. Monkiewicz, L. Gąsiorkiewicz, C.H. Beck, Warszawa 2010.

Summary

Comprehensive approach for the selection and protection of critical infrastructure

Digital technologies on the one hand improve the quality of services supplied for citizens, but at the same time they are the source of new threats. As a result, apart from current types of security management (physical or technical security) there appear its new forms, being a reply to new threats (cybernetic security, personal data security etc). These diversified actions, to achieve the intentional effect, should be treated as elements of the greater whole. This greater whole means the comprehensive security management including not only actions in favour of the own unit, but also the ones taking into account both the influence of outside entities and possible social effects deriving from a dysfunction of services provided by the entity. A service approach, as a method allowing for the hierarchization of processes carried out as part of the civil service, is a brand new issue requiring both mental changes amongst the managing staff as well as the adaptation of formal structures to requirements connected with the necessity to implement new forms of the security management.

Tłumaczenie: Renata Cedro

OCHRONA SYSTEMÓW INFORMATYCZNYCH POLICJI

nadkom. Adam Bogucki
Naczelnik
Wydziału Ochrony Systemów Informatycznych
Biura Łączności i Informatyki KGP

Krzysztof Stasiowski
Główny specjalista
Wydziału Ochrony Systemów Informatycznych
Biura Łączności i Informatyki KGP

W artykule przedstawiono ogólne wskazówki dotyczące bezpiecznego użytkowania systemów teleinformatycznych, które mają swoje źródło w tak zwanych dobrych praktykach, normach, standardach, zaleceniach. Utrzymywanie wysokiego poziomu wiedzy i świadomości użytkowników systemów teleinformatycznych w zakresie bezpieczeństwa teleinformatycznego jest jednym z najważniejszych środków, który pozwala ograniczyć występowanie tzw. incydentów bezpieczeństwa, tj. zdarzeń zagrażających bezpieczeństwu informacji przetwarzanych w systemach teleinformatycznych oraz ciągłości działania tych systemów. W artykule omówiono zalecenia dotyczące m.in. takich obszarów, jak korzystanie z sieci Internet i poczty elektronicznej. W odniesieniu do systemów teleinformatycznych, w których są przetwarzane dane osobowe oraz informacje niejawne, należy stosować właściwe przepisy obowiązującego prawa oraz regulacje wewnętrzne przyjęte w organizacji.

Bezpieczeństwo teleinformatyczne

Niewłaściwy sposób pracy i nieodpowiednie zachowania użytkowników stanowią istotne zagrożenie dla bezpieczeństwa systemów teleinformatycznych. Podstawowym obowiązkiem użytkownika jest eksploatacja systemu teleinformatycznego zgodnie z zasadami określonymi i udokumentowanymi przez twórców systemu oraz zgodnie z procedurami obowiązującymi w miejscu pracy, określonymi np. w instrukcji stanowiskowej. W niniejszym artykule przedstawiono zasady postępowania użytkowników stanowisk komputerowych oraz urządzeń pamięci masowej. Przestrzeganie tych reguł jest zalecane przez Biuro Łączności i Informatyki KGP bądź też wynika z przepisów obowiązujących w Policji. W odniesieniu do systemów teleinformatycznych, w których są przetwarzane dane osobowe lub informacje niejawne, zastosowanie mają przepisy ustaw o ochronie danych osobowych oraz informacji niejawnych.

Upewnienie się co do tożsamości osób postronnych

Do obowiązków użytkownika należy uzyskanie pewności odnośnie do tożsamości oraz uprawnień osób postronnych, które w jakikolwiek sposób mogą wejść w kontakt z wykorzystywanymi przez niego systemami teleinformatycznymi, jeśli osoby te nie zostały wprowadzone przez przełożonego. Do osób takich należą w szczególności serwisanci, osoby współpracujące z innych jednostek organizacyjnych Policji lub z innych instytucji, goście, dostawcy i konsultanci. Obowiązki użytkownika obejmują:

- zweryfikowanie tożsamości danej osoby (np. wykonanie telefonu do przełożonego, w szczególnych przypadkach – zażądanie dokumentów pisemnych),
- zweryfikowanie uprawnienia danej osoby do wykonywanych czynności (np. w zlecającej komórce merytorycznej).

Bezpieczne korzystanie z usług internetowych

Użytkownik mający ze swojego stanowiska pracy dostęp do Internetu powinien z niego korzystać tylko w celach służbowych. Bezpieczne korzystanie z Internetu wymaga stosowania przez użytkowników następujących zasad:

- użytkownik może się łączyć z Internetem jedynie za pośrednictwem zastanej infrastruktury informatycznej (połączenie przez Centralny Węzeł Dostępowy do sieci Internet); nie wolno mu nawiązywać połączeń ze służbowego stanowiska dostępowego (stacji roboczej), za pośrednictwem jakichkolwiek dodatkowych, własnych środków technicznych (np. modemu cyfrowego lub analogowego, karty łączności komórkowej, połączenia bezprzewodowego), nawet gdyby dysponował fizyczną możliwością podłączenia odpowiedniego urządzenia;
- użytkownik może korzystać wyłącznie z przeglądarek internetowych dopuszczonych do eksploatacji w Policji;
- użytkownik nie może zmieniać konfiguracji ustawień bezpieczeństwa przeglądarki internetowej na swojej stacji roboczej ani modyfikować lokalnego oprogramowania zapewniającego bezpieczeństwo (np. oprogramowania antywirusowego);
- użytkownik może jedynie korzystać z usług dopuszczonych przez politykę bezpieczeństwa sieci; nie wolno mu podejmować jakichkolwiek prób obejścia zabezpieczeń w tym zakresie, w szczególności poprzez korzystanie z serwisów anonimizujących;
- w przypadku komunikacji szyfrowanej (https) użytkownik ma obowiązek się upewnić co do tożsamości strony internetowej poprzez sprawdzenie certyfikatu, a także postępować zgodnie z instrukcjami bezpieczeństwa danego serwisu internetowego;
- w przypadku dostępu do serwisu internetowego wymagającego zalogowania użytkownik jest zobowiązany wybierać login i hasło inne, niż stosuje w celu dostępu do jakichkolwiek systemów teleinformatycznych Policji; jeżeli serwis pozwala też na zdefiniowanie pytania/odpowiedzi kontrolnej w celu późniejszego odzyskania hasła, użytkownik nie powinien w odpowiedzi podawać faktów;
- przy rejestrowaniu w serwisach internetowych, udziale w grupach dyskusyjnych itp. użytkownik powinien unikać podawania informacji o swojej tożsamości i miejscu pracy;
- użytkownik nie może pobierać z sieci Internet, składować ani instalować jakichkolwiek komponentów oprogramowania, nawet jeśli jest to sugerowane jako poprawiające wydajność lub funkcjonalność; ewentualne wyjątki publikuje administrator sieci Internet.

Użytkownik powinien mieć świadomość tego, że jego działania w Internecie są rejestrowane i mogą być przeglądane przez administratora sieci, a ponadto niektóre z nich mogą być blokowane przez system.

Bezpieczne korzystanie z internetowej poczty elektronicznej

Użytkownicy mają obowiązek przestrzegania następujących zasad przy korzystaniu z internetowej poczty elektronicznej:

- ze służbowej poczty elektronicznej można korzystać tylko do celów służbowych; nie należy jej używać do celów prywatnych, a w szczególności nie wolno podawać służbowego adresu poczty elektronicznej przy rejestracji w serwisach internetowych niesłużących do realizacji zadań służbowych;
- nie wolno wykorzystywać poczty elektronicznej do przesyłania treści obraźliwych;
- użytkownik może korzystać ze służbowej poczty elektronicznej tylko z użyciem klienta pocztowego dopuszczonego do eksploatacji w Policji;
- użytkownik nie może samodzielnie zmieniać ustawień bezpieczeństwa klienta poczty elektronicznej;
- przesyłanie poczty elektronicznej zawierającej „tajemnicę" Policji jest dopuszczalne jedynie w przypadku jej podpisania i zaszyfrowania; szczegółowych instrukcji w tym zakresie udziela administrator poczty; ewentualna wymiana haseł pomiędzy stronami musi nastąpić inną drogą niż poczta elektroniczna (np. telefon, SMS, kartka papieru);
- przełożony użytkownika może ponadto określić, jakich informacji i/lub do jakich odbiorców nie można w żadnym wypadku przesyłać pocztą elektroniczną; do tych zasad użytkownik musi się bezwzględnie stosować;
- wiadomość elektroniczna wysłana do adresata poza Policją powinna być zakończona klauzulą: „Niniejsza wiadomość jest przeznaczona wyłącznie dla jej adresata i może zawierać treści chronione przepisami prawa. Wgląd w treść wiadomości otrzymanej omyłkowo, dalsze jej przekazywanie, rozpowszechnianie lub innego rodzaju wykorzystanie bądź podjęcie jakichkolwiek działań w oparciu o zawarte w niej informacje przez osobę lub podmiot niebędący adresatem, jest niedozwolone. Jeśli nie są Państwo adresatem tej wiadomości, prosimy o pilną informację zwrotną o otrzymaniu wiadomości przez pomyłkę oraz usunięcie jej z komputera. Z góry dziękujemy za Państwa pomoc.";
- użytkownik powinien przy wysyłaniu przesyłki pocztowej zwrócić uwagę na to, jacy adresaci powinni o sobie nawzajem wiedzieć; w przypadku przesyłki pocztowej, której głównym adresatem jest odbiorca z zewnątrz, a kopie są wysyłane do odbiorców w Policji, zaleca się podanie tych ostatnich jako adresatów kopii ukrytej;
- użytkownik powinien zasadniczo traktować jako podejrzaną każdą przesyłkę pocztową, która pochodzi z nieznanego mu źródła;
- przed otwarciem załącznika przesyłki pocztowej użytkownik powinien: upewnić się co do wiarygodności nadawcy, nie otwierać podejrzanych załączników, nie uruchamiać łącz do podejrzanych lub nieznanych stron internetowych;
- zarówno przychodząca, jak i wychodząca poczta elektroniczna powinny być skanowane przez oprogramowanie antywirusowe; jeżeli użytkownik zauważy jakieś odstępstwa, powinien to zgłosić jako incydent bezpieczeństwa.

Użytkownik musi być świadomy, że zarówno przychodząca, jak i wychodząca poczta elektroniczna są skanowane przez serwer pocztowy, a przesyłki stanowiące zagrożenie dla bezpieczeństwa Policji będą zatrzymywane.

Praca wyłącznie z dopuszczonymi systemami teleinformatycznymi

Użytkownik może korzystać jedynie z systemów teleinformatycznych dopuszczonych do eksploatacji; dotyczy to także oprogramowania standardowego (przeglądarki www,

pakietów biurowych itp.), do których dostał indywidualne uprawnienia. Przed rozpoczęciem pracy powinien zostać uświadomiony, z jakich systemów teleinformatycznych oraz innych zasobów wolno mu korzystać.
Użytkownikowi nie wolno w szczególności:
- instalować własnego oprogramowania lub dowolnego oprogramowania niewiadomego pochodzenia na stacji roboczej, nawet w przypadku zaistnienia takiej technicznej możliwości;
- korzystać w jakikolwiek sposób z systemów, do których nie został upoważniony;
- korzystać z udostępnionego systemu poprzez wykorzystanie konta innej osoby, nawet na jej wyraźną prośbę;
- podejmować prób obejścia lub forsowania zabezpieczeń.

Praca zgodnie z przeznaczeniem systemów teleinformatycznych

Użytkownik ma prawo wykorzystywać system teleinformatyczny wyłącznie do realizacji celów związanych ze stanowiskiem pracy, w dopuszczalnych godzinach pracy. Nie wolno zatem korzystać z systemu do celów prywatnych, także związanych z indywidualną działalnością akademicką lub naukową, chyba że przełożony udzielił użytkownikowi takiej zgody na piśmie.

Dbałość o właściwą eksploatację urządzeń teleinformatycznych

Użytkownik powinien dbać o zapewnienie właściwych warunków eksploatacyjnych urządzeń teleinformatycznych w takim zakresie, w jakim ma wpływ na te warunki, zwłaszcza w odniesieniu do komputerów przenośnych. Obowiązki te obejmują w szczególności:
- podłączanie urządzeń wyłącznie do przeznaczonych do tego obwodów zasilających;
- ustawianie urządzeń na solidnej, poziomej podstawie;
- zapewnianie swobodnej cyrkulacji powietrza (np. niezasłanianie otworów wentylacyjnych);
- zapewnianie pracy we właściwej temperaturze, w szczególności umieszczenie urządzeń w odległości większej niż 20 cm od grzejników;
- zachowywanie czystości urządzeń, w szczególności unikanie gromadzenia się pyłu;
- niewystawianie urządzeń na nadmierne działanie promieni słonecznych;
- stosowanie innych zasad postępowania dotyczących sprzętu elektronicznego, w tym nieumieszczanie ciężkich przedmiotów na urządzeniach, unikanie nadmiernego napinania kabli zasilających oraz sygnałowych, zapobieganie wylaniu cieczy na urządzenie.

Ochrona mechanizmów uwierzytelnienia

Mechanizmy uwierzytelnienia to wszystkie urządzenia techniczne (np. karta mikroprocesorowa, token itp.) oraz dane (np. identyfikator i hasło) niezbędne i wystarczające do uzyskania dostępu do systemu teleinformatycznego. Użytkownik wyposażony w takie mechanizmy jest zobowiązany do ich szczególnej ochrony. Za niestaranność ochrony lub celowe przekazanie osobom trzecim może zostać pociągnięty do odpowiedzialności służbowej. Do obowiązków użytkownika należą w szczególności:
- stosowanie haseł zgodnych z polityką określoną dla danego systemu (jeśli system tego nie wymusza automatycznie);
- regularna zmiana haseł zgodnie z polityką określoną dla danego systemu (jeśli system tego nie wymusza automatycznie);
- zmiana hasła w przypadku omyłkowego udostępnienia danych konta lub podejrzenia o przechwycenie ich przez stronę trzecią;
- zgłoszenie incydentu bezpieczeństwa w przypadku omyłkowego udostępnienia danych konta lub podejrzenia o przechwycenie ich przez stronę trzecią;
- niezapisywanie haseł w postaci jawnej w jakimkolwiek miejscu ani w formie elektronicznej (w szczególności w plikach tekstowych lub bazach danych albo jako parametrów plików wykonywalnych), ani papierowej;
- wprowadzanie identyfikatorów i haseł w obecności osób postronnych tylko w przypadku upewnienia się, że nie ma możliwości podejrzenia;
- niewykorzystywanie starych haseł (poprzednio używanych) przy kolejnej zmianie hasła;
- niezapisywanie haseł domyślnie w przeglądarce www;
- przechowywanie nośników informacji uwierzytelniających (np. tokenów, kart mikroprocesorowych itp.) w zamknięciu (co najmniej indywidualne szuflady ograniczające dostęp osób trzecich);
- w przypadku możliwości wyboru nazwy konta i hasła – stosowanie w pracy innych nazw kont i haseł niż używane do prywatnych celów (np. dostępu do kont bankowych, prywatnej poczty elektronicznej, portali społecznościowych).

Wylogowanie z systemu przed dopuszczeniem osób trzecich

Przed dopuszczeniem osób trzecich do stacji roboczej (zarówno współpracowników, jak i autoryzowanych osób spoza aktualnego kręgu współpracowników) użytkownik musi obowiązkowo wylogować się z systemu.
Zasada ta nie obowiązuje, jeśli użytkownik wykonuje określone czynności na prośbę serwisanta lub innej autoryzowanej osoby trzeciej (administratora, kontrolera bezpieczeństwa itp.), wówczas jednak nie może tej osoby dopuścić bezpośrednio do wykonania jakiejkolwiek czynności w systemie.

Ochrona informacji dotyczących systemów teleinformatycznych

Użytkownikowi nie wolno się dzielić informacją dotyczącą eksploatowanego systemu teleinformatycznego z osobami postronnymi, chyba że udzielenie informacji odbywa się na polecenie przełożonego. W szczególności nie wolno ustnie ani na piśmie udzielać informacji dotyczącej:
- pochodzenia, przeznaczenia i funkcjonalności systemu;
- administratorów i użytkowników systemu;
- zasad i procedur związanych z pracą użytkową w systemie;

- zasad i procedur związanych z administracją systemu;
- architektury logicznej i fizycznej systemu, w tym powiązań z innymi systemami;
- lokalizacji systemu i jego komponentów;
- parametrów konfiguracyjnych systemu;
- środków ochrony zastosowanych w odniesieniu do systemu, w tym polityki bezpieczeństwa systemu;
- słabości, podatności lub błędów systemu;
- awarii, kłopotów lub incydentów bezpieczeństwa związanych z systemem.

Zabezpieczenie systemu teleinformatycznego pozostawionego bez opieki

Użytkownik systemu teleinformatycznego powinien w miarę swoich możliwości przeciwdziałać dostępowi osoby niepowołanej do systemu. W tym celu, przed odejściem od stacji roboczej poza odległość wzroku, powinien się wylogować z systemu oraz zablokować konsolę systemu operacyjnego.
Przed opuszczeniem pomieszczenia na dłużej, np. w związku z zakończeniem pracy, użytkownik jest zobowiązany wyłączyć stację roboczą. Jeżeli uwierzytelnienie w systemie następuje za pomocą urządzenia lub nośnika fizycznego, np. karty mikroprocesorowej, użytkownik powinien w obu powyższych przypadkach bezwzględnie zabrać je ze sobą.

Ochrona komputera przenośnego

Komputer przenośny powinien być szczególnie zabezpieczony na wypadek zguby lub kradzieży. Użytkownik powinien przestrzegać następujących zasad:

- stosowanie co najmniej zabezpieczenia BIOS i systemu operacyjnego hasłami – nie wolno usuwać istniejących w tym zakresie zabezpieczeń;
- unikanie przechowywania na dysku twardym komputera przenośnego danych lub dokumentów, które nie są absolutnie niezbędne do wykonywania aktualnej pracy;
- szyfrowanie dysku mocnymi metodami kryptograficznymi (jeżeli istnieje taka techniczna możliwość) lub co najmniej szyfrowanie dokumentów stanowiących „tajemnicę" Policji;
- przytwierdzanie komputera do stanowiska pracy linką;
- usytuowanie komputera w taki sposób, aby utrudnić podgląd jego monitora przez osoby postronne;
- niepodłączanie komputera do sieci lokalnych lub bezprzewodowych, chyba że w celu nawiązania połączenia szyfrowanego (typu VPN) zgodnie z przyjętą polityką bezpieczeństwa sieci komputerowej.

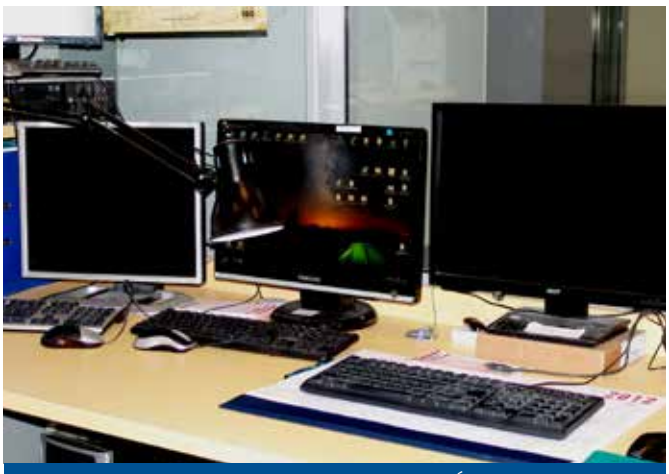
Bezpieczny nadzór nad serwisem i konserwacją systemu

Należy przestrzegać następujących zasad dotyczących konserwacji lub serwisu systemu teleinformatycznego:

- użytkownik powinien w miarę swoich możliwości zweryfikować tożsamość serwisanta i sprawdzić jego uprawnienia do wykonywanych czynności;

Struktura teletechniczna. Fot. Katarzyna Lipińska, Źródło: BŁiI KGP.

Serwerownia BŁiI KGP. Fot. Katarzyna Lipińska. Źródło: BŁiI KGP.



Serwerownia BŁiI KGP. Fot. Katarzyna Lipińska. Źródło: BŁiI KGP.

- fizyczny dostęp serwisanta do pomieszczenia i urządzeń powinien być ograniczony do niezbędnego minimum;
- prace wykonane przez serwisanta powinny zostać udokumentowane zgodnie z przyjętą procedurą serwisową, a użytkownik powinien potwierdzić ich zgodność z opisem (w zależności od swojej wiedzy technicznej);
- podmiot dokonujący czynności serwisowych lub konserwacyjnych powinien potwierdzić znajomość przepisów BHP obowiązujących w Policji;

- użytkownik powinien poświęcić czas na sprawdzenie funkcjonalności systemu w obecności serwisanta bezpośrednio po wykonaniu prac serwisowych lub konserwacyjnych, a także zgłosić ewentualne problemy;
- po wizycie serwisowej użytkownik powinien przeprowadzić skanowanie antywirusowe systemu;
- w przypadku zainstalowania przez serwisanta jakiegokolwiek oprogramowania (np. diagnostycznego) użytkownik powinien zażądać od serwisanta dowodu, że takie oprogramowanie zostało usunięte po zakończeniu prac.

Bezpieczne postępowanie z nośnikami i urządzeniami pamięci zewnętrznej

Użytkownik powinien szczególnie chronić nośniki danych (np. płyty CD, DVD) oraz urządzenia pamięci zewnętrznej (np. pamięć flash, zewnętrzny dysk twardy) zawierające dane wykorzystywane do pracy zawodowej. Jednocześnie powinien zapewnić, aby zawartość nośników i urządzeń nie stała się zagrożeniem dla eksploatowanego systemu teleinformatycznego. Powinien zatem przestrzegać następujących zasad:

- zapisywać dane na nośnikach i urządzeniach pamięci zewnętrznej tylko w razie rzeczywistej potrzeby, unikając tworzenia niepotrzebnych kopii danych;
- zapisywać dane stanowiące „tajemnicę" Policji tylko w postaci zaszyfrowanej;
- przechowywać nośniki i urządzenia w zamknięciu, jeśli nie są aktualnie wykorzystywane;
- przed przekazaniem nośnika lub urządzenia pamięci zewnętrznej innej osobie upewnić się, że nie zawiera innych danych, których udostępnienie nie jest pożądane;
- nie opisywać nośników i urządzeń pamięci zewnętrznej lub opisywać je w taki sposób, który nie daje wskazówek odnośnie do ich zawartości;
- regularnie czyścić zawartość nośników i urządzeń pamięci zewnętrznej, usuwając z nich dane niewymagane do bieżącej pracy;
- unikać stosowania lub podłączania niesprawdzonych lub nieznanych urządzeń wymiennych należących do innych osób;
- usuwać dane z nośników wielokrotnego zapisu w sposób bezpieczny.

Użytkownik powinien przekazywać do zniszczenia:

- wszystkie nośniki danych jednokrotnego zapisu, których nie będzie użytkował lub które uległy uszkodzeniu,
- urządzenia pamięci zewnętrznej, które uległy uszkodzeniu niepozwalającemu na ich naprawę.

Niedopuszczalne jest pozbywanie się nośników albo urządzeń poprzez ich wyrzucanie do śmieci.

Bezpieczne postępowanie z dokumentami papierowymi

Dokumenty papierowe związane z systemami teleinformatycznymi, w szczególności wydruki z systemów teleinformatycznych oraz dokumentacja systemów teleinformatycznych, mogą zawierać wrażliwe informacje, które nie powinny dostać się w niepowołane ręce. Użytkownik powinien stosować podobne środki ostrożności wobec wydruków i dokumentacji jak wobec nośników danych, a w szczególności:

- przechowywać wydruki i dokumentację poza zasięgiem wzroku innych osób (zasada czystego blatu i ekranu);
- nie wykonywać niepotrzebnych lub nadmiarowych wydruków;
- nie pozostawiać wydruków w drukarce;
- nie przekazywać wydruków osobom niepowołanym;
- utylizować wydruki za pomocą niszczarki w momencie, kiedy nie są już potrzebne do wykonywanej pracy, a nie muszą zostać umieszczone w archiwum.

Za pomocą niszczarki należy obowiązkowo utylizować:

- każdy wydruk z centralnego systemu teleinformatycznego wykorzystywanego w Policji;
- każdy rodzaj dokumentacji systemu teleinformatycznego;
- każdy dokument zawierający informacje służbowe.

Zgłaszanie incydentów bezpieczeństwa

Użytkownik powinien zgłaszać przełożonym incydenty bezpieczeństwa. Ze względu na ograniczoną wiedzę techniczną lub ograniczony dostęp do systemu nie zawsze może rozpoznać określone zjawisko jako incydent bezpieczeństwa, powinien wykonać jedną z dwóch opisanych poniżej czynności:

- problemy lub obserwacje związane z użytkowaniem systemu teleinformatycznego (np. inne niż zwykle zachowanie systemu, kłopoty z uzyskaniem dostępu do systemu, trudności z wykonaniem działań w systemie, podejrzenie dotyczące spójności czy też poprawności przetwarzanych danych) powinny być zgłaszane do BŁiI KGP;
- inne incydenty, które użytkownik systemu teleinformatycznego sam rozpozna jako związane z bezpieczeństwem (np. kradzież lub utrata nośnika danych, zaobserwowane próby sforsowania zabezpieczeń, obecność osób niepowołanych, próby wyłudzenia informacji), powinny być zgłaszane przez użytkownika przełożonemu.

Summary

Protection of IT systems of the Police

The article presents general guidance on the safe use of ICT systems, which is based on good practices, norms, standards and recommendations. Maintenance of a high level of users' knowledge and awareness in the area of ICT security is one of the key means of achieving the lowest possible number of security incidents. Such incidents pose the threat to security of data processed in the ICT systems and the continuity of actions. The article describes recommendations on, among others using the Internet or electronic mail. In respect of ICT systems which process personal data and classified information, one should apply relevant provisions of law and internal regulations of the organisation.

Tłumaczenie: Joanna Łaszyn

CYBERPRZESTĘPCZOŚĆ
– próba diagnozy zjawiska

nadkom. Mariusz Stefanowicz

ekspert Wydziału Rozpoznania
Biura do Walki z Cyberprzestępczością KGP

Celem artykułu jest ukazanie w przystępnej formie każdemu czytelnikowi, będącemu jednocześnie użytkownikiem komputera i Internetu, kluczowych definicji i zagadnień z zakresu cyberprzestępczości. W zamyśle jest również przedstawienie podstawowego podziału tego typu przestępczości, charakterystycznych cech pozwalających na wyróżnienie poszczególnych czynów przestępczych, a także największych problemów i trudności – zarówno prawnych, jak i organizacyjnych – z jakimi borykają się polskie organy ścigania w ich zwalczaniu.

Z uwagi na dynamiczny rozwój Internetu, usług internetowych czy coraz częstsze udostępnianie danych wrażliwych w urządzeniach mobilnych, to zagadnienie powinno być w zainteresowaniu każdego z nas.

W jak najlepiej pojętym własnym interesie każdy użytkownik Internetu, komputerów czy urządzeń telekomunikacyjnych, z uwagi na coraz to bardziej wyszukane sposoby popełniania przestępstw lub oszustw internetowych dokonywanych z wykorzystaniem socjotechniki i najnowszych technologii, powinien dobrze poznać zagadnienia, takie jak podstawy zwalczania cyberprzestępczości czy „dobre praktyki" niezbędne do bezpiecznego korzystania z Internetu.

Wstęp

Od początku swojego istnienia, tj. lat 70. i 80. dwudziestego wieku, Internet w olbrzymi sposób zmienił sposób postrzegania otaczającego nas świata. Zatarły się podziały istniejące w oparciu o granice państw czy bariery językowe. Świat stał się mniejszy i bliższy dla każdego użytkownika Internetu. W istniejącej sieci każdy miał jednakowe prawa i każdy mógł się stać zarówno odbiorcą informacji, jak i ich twórcą dla innych użytkowników.

Koniec XX i początek XXI wieku to okres, nie tylko na świecie, ale także w Polsce, gwałtownego rozwoju komputerów, samego Internetu oraz dostępu do niego z użyciem technologii mobilnych. Internet jest obecnie wykorzystywany w tak wielu ważnych aspektach naszego codziennego życia, takich jak operacje bankowe, zakupy, e-urzędy czy zwykła poczta elektroniczna, że trudno sobie wyobrazić dzień bez sprawdzenia najświeższych informacji, odwiedzin najpopularniejszych portali społecznościowych czy oglądania telewizji lub słuchania radia on-line.

W czasach, kiedy Internet raczkował i był dostępny tylko dla ograniczonego kręgu osób, kwestię bezpieczeństwa traktowano po macoszemu i pozostawiano raczej problemem marginalnym. Dziś, z uwagi na niespotykane dotychczas nasycenie wszystkich dziedzin życia nowoczesnymi technologiami, przestępczość komputerowa stanowi poważniejszy problem, a z każdym rokiem liczba przestępstw odnotowywana w po-

licyjnych statystykach się zwiększa. Dodatkowo, z uwagi na zaangażowanie coraz większych środków finansowych poprzez bankowość internetową, rosnącą liczbę kwot przelewów elektronicznych czy zwiększające się obroty sklepów internetowych oraz portali aukcyjnych i ogłoszeniowych, stopniowo kładzie się coraz większy nacisk na zwalczanie tego typu przestępczości. Internet jest dziś powszechnie wykorzystywany jako narzędzie służące do dokonywania wszelkiego rodzaju czynów zabronionych.

Definicja cyberprzestępczości

Polskie prawodawstwo do dzisiaj nie stworzyło jednolitej definicji cyberprzestępczości. Pojęcie przestępczości komputerowej nie jest jednoznacznie zdefiniowane nawet na gruncie Kodeksu karnego. Funkcjonuje natomiast wiele tworzonych doraźnie, w zależności od potrzeb, definicji opierających się na najprostszym założeniu, iż ogólnie są to przestępstwa popełniane za pomocą komputerów oraz Internetu.
Innym źródłem definicji, z którego można korzystać, mogą być międzynarodowe podmioty, takie jak ONZ, Unia Europejska czy Interpol, które opracowały definicję cyberprzestępczości na własne potrzeby. Jednak bez względu na to, jaką definicję cyberprzestępczości przyjmiemy, zawsze to będą czyny zabronione, skierowane przeciwko systemom informatycznym, w których komputer jest celem samym w sobie, oraz czyny dokonane z użyciem komputera, w których stanowi on jedynie narzędzie.

Definicja Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej

W myśl definicji opracowanej i zamieszczonej w „Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej" przyjętej w dniu 25 czerwca 2013 r. w drodze uchwały przez Radę Ministrów, cyberprzestępstwo stanowi czyn zabroniony popełniony w obszarze cyberprzestrzeni, czyli przestrzeni przetwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570, z późn. zm.) wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[1].

Definicja cyberprzestępczości według Interpolu

Definicja sformułowana przez Interpol jest bardzo praktyczna i określa cyberprzestępczość w dwóch ujęciach – tzw. wertykalnym oraz horyzontalnym. Ujęcie wertykalne dotyczy przestępstw specyficznych dla cyberprzestrzeni, czyli takich, które tylko tam mogą być dokonane, np. hacking, sabotaż komputerowy. Z kolei ujęcie horyzontalne zakłada popełnianie przestępstw za pomocą technik komputerowych (np. oszustwa komputerowe, fałszowanie pieniędzy, pranie brudnych pieniędzy etc.)[2].

Definicja cyberprzestępczości według Rady Europy

W przedmiocie cyberprzestępczości Rada Europy przyjęła konwencję z dnia 23 listopada 2001 r. o cyberprzestępczości (Dz. U. z 2015 r. poz. 728). Z jej zapisów wyłania się obraz definicji cyberprzestępczości jako:

- umyślnego i bezprawnego dostępu do całości lub części systemu informatycznego;
- umyślnego i bezprawnego przechwytywania za pomocą urządzeń technicznych niepublicznych transmisji danych informatycznych do, z, lub w ramach systemu informatycznego, łącznie z emisjami elektromagnetycznymi pochodzącymi z systemu informatycznego przekazującego takie dane informatyczne;
- umyślnego i bezprawnego niszczenia, wykasowywania, uszkadzania, dokonywania zmian lub usuwania danych informatycznych, poważnego zakłócania funkcjonowania systemu informatycznego poprzez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych;
- produkcji, sprzedaży, pozyskiwania z zamiarem wykorzystania, importowania, dystrybucji lub innego udostępniania urządzenia, w tym także programu komputerowego, przeznaczonego lub przystosowanego przede wszystkim dla celów popełnienia któregokolwiek z przestępstw lub hasła komputerowego, kodu dostępu lub podobnych danych, dzięki którym całość lub część systemu informatycznego jest dostępna z zamiarem wykorzystania dla celów popełnienia któregokolwiek z przestępstw.

Konwencja ta wyróżnia następujące rodzaje przestępstw:

- przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów;
- przestępstwa komputerowe – fałszerstwo komputerowe oraz oszustwo komputerowe;
- przestępstwa ze względu na charakter zawartych informacji;
- przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych[3].

Definicja cyberprzestępczości według Unii Europejskiej

Definicja ta została zawarta w Komunikacie Komisji Do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z 22 maja 2007 r. „W kierunku ogólnej strategii zwalczania cyberprzestępczości".
W praktyce terminu cyberprzestępczość używa się w odniesieniu do trzech rodzajów przestępstw. Pierwszy obejmuje tradycyjne formy przestępstw, takie jak oszustwo czy fałszerstwo, jednak w kontekście cyberprzestępczości dotyczą one konkretnie przestępstw popełnionych z użyciem elektronicznych sieci informatycznych i systemów informatycznych. Drugi rodzaj stanowi publikacja nielegalnych treści w mediach elektronicznych (np. materiałów związanych z seksualnym wykorzystywaniem dzieci czy też nawoływaniem do nienawiści rasowej). Trzeci rodzaj obejmuje przestępstwa typowe dla sieci łączności elektronicznej, tj. ataki przeciwko systemom informatycznym, ataki typu DOS oraz hakerstwo[4].

Definicja cyberprzestępczości według ONZ

Definicję w przedstawionej poniżej formie przyjął X Kongres ONZ w Sprawie Zapobiegania Przestępczości i Traktowania Przestępców. Zgodnie z przyjętymi zapisami definicji zostało wyróżnione cyberprzestępstwo w ujęciu wąskim oraz w ujęciu szerokim. I tak:

- cyberprzestępstwo w wąskim sensie (przestępstwo komputerowe) – jest to wszelkie nielegalne działanie wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych lub procesowanych przez te systemy danych;
- cyberprzestępstwo w szerokim sensie (przestępstwo dotyczące komputerów) – wszelkie nielegalne działanie popełnione za pomocą lub dotyczące systemów lub sieci komputerowych, włączając w to między innymi nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych[5].

Podstawowy podział i charakterystyka cyberprzestępczości

W najbardziej uproszczony sposób cyberprzestępczość można podzielić na dwie podstawowe kategorie:

- przestępstwa charakterystyczne dla cyberprzestępczości,
- przestępstwa popełniane z wykorzystaniem sieci Internet.

Pierwszą kategorię stanowią przestępstwa, w których przedmiotem ataku jest sam komputer oraz szeroko pojęte przetwarzanie danych w systemach informatycznych. Do tej grupy można zaliczyć takie czyny, jak:

- podawanie się za inną osobę, fałszywe profile,
- nieuprawnione uzyskanie informacji (hacking),
- podsłuch komputerowy (sniffing),
- udaremnienie uzyskania informacji,
- udaremnienie dostępu do danych informatycznych,
- sabotaż komputerowy,
- rozpowszechnianie złośliwych programów oraz cracking,
- stosowanie tzw. narzędzi hackerskich,
- oszustwo komputerowe.

Do drugiej kategorii należy zaliczyć przestępstwa, w których komputer jest jedynie środkiem do jego popełnienia. W tej grupie można wymienić takie działania, jak:

- obrazę uczuć religijnych (przestępstwa przeciwko wolności sumienia i wyznania),
- składanie propozycji obcowania płciowego z małoletnim,
- publiczne propagowanie lub pochwalanie zachowań o charakterze pedofilskim,
- publiczne propagowanie faszystowskich lub innych totalitarnych ustrojów państwa lub nawoływanie do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość (szeroko pojęta mowa nienawiści),
- handel fikcyjnymi kosztami,
- zbywanie własnego lub cudzego dokumentu stwierdzającego tożsamość (przestępstwa przeciwko wiarygodności dokumentów),
- oszustwa popełniane za pośrednictwem Internetu, np. na portalach aukcyjnych.

Polska przestępczość w cyberprzestrzeni charakteryzuje się tym, iż czyny te w większości można zakwalifikować do drugiej kategorii, czyli są popełniane z wykorzystaniem Internetu. Taki stan rzeczy wynika w dużej mierze z postępu technologicznego, coraz łatwiejszego i obciążonego niskimi kosztami dostępu do sieci, uruchamiania coraz większej liczby hotspotów z anonimowym, darmowym dostępem do Internetu czy coraz większej liczby komputerów i urządzeń mobilnych.
Innym czynnikiem jest „wygoda" osób, które takie czyny popełniają. Sprawca nie musi angażować tylu sił i środków jak w świecie realnym. Siedząc w domu, kilkoma kliknięciami może dokonać oszustwa, wymienić się materiałami pedofilskimi czy też dokonać wpisu szkalującego inną osobę lub obrażającego uczucia religijne.

Dodatkowym ułatwieniem dla sprawców jest głębokie przeświadczenie, że cyberprzestrzeń zapewnia im anonimowość, oraz mała świadomość ich ofiar w zakresie bezpiecznego wykorzystywania zasobów sieci Internet. Inną charakterystyczną cechą cyberprzestępczości jest sporadyczne zgłaszanie przestępstw popełnionych w Internecie, co powoduje wzrost ciemnej liczby przestępstw. W tym przypadku wynika to z wielu czynników. Jednym z nich jest niska świadomość użytkowników, którzy często nie wiedzą, że stali się ofiarą cyberprzestępstwa. Przykładem może być wirus Weelsof, który infekuje komputery użytkowników, podszywając się pod organa ścigania, i za odblokowanie zasobów komputera żąda wniesienia opłaty. Osoby, których komputery zostały zainfekowane, nie wiedzą, że takie procedury są niedozwolone i niestosowane przez organy ścigania, a także nie mają wiedzy niezbędnej do samodzielnego odblokowania komputera.

Ponadto ofiary tych działań bardzo niechętnie składają zawiadomienia o popełnieniu przestępstwa z uwagi na to, iż rzeczywiście posiadają nielegalne zasoby w komputerze w postaci materiałów chronionych prawami autorskimi w formie filmów lub muzyki czy też korzystają ze specjalistycznego oprogramowania bez wykupionych i opłaconych niezbędnych, wymaganych przepisami prawa, licencji. Kolejnym czynnikiem może być fakt, że stanie się ofiarą cyberprzestępstwa może być ukrywane w obawie przed kompromitacją i utratą reputacji.

Trudności zwalczania cyberprzestępczości

W związku z intensywną działalnością cyberprzestępców władze wielu państw od dawna poszukują rozwiązań – prawnych i technologicznych – które umożliwiłyby skuteczną walkę z przestępczością komputerową. Polska nie jest wyjątkiem. Skuteczne ściganie cyberprzestępców z wielu stron napotyka trudności, których przezwyciężenie jest konieczne do

pozytywnego zakończenia procesu wykrywczego i w efekcie – ukarania sprawcy.
Jednym z aspektów utrudniających lub czasami wręcz uniemożliwiających skuteczne ściganie przestępstw popełnianych w cyberprzestrzeni jest fakt, iż obowiązujące przepisy prawa często nie nadążają za błyskawicznymi zmianami, jakie następują zarówno w życiu codziennym, jak i w Internecie. Inną przyczyną są wprowadzane zmiany w obowiązujących przepisach prawnych, które chroniąc wolności obywatelskie, znacząco zakłócają podjęcie niezbędnych czynności przez organy ścigania.
Przykładem takich przepisów może być ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907, z późn. zm.), w której w styczniu 2013 r. przez wprowadzoną nowelizację skrócono okres przechowywania istotnych dla organów ścigania danych retencyjnych z 24 do 12 miesięcy. Ponadto w wyniku wprowadzonych zapisów wszystkie dane starsze niż 12 miesięcy, licząc od daty wejścia w życie nowelizacji ustawy, zostały usunięte przez operatorów i dostęp do nich stał się niemożliwy.
Jedyną pozytywną zmianą w przepisach prawa telekomunikacyjnego, ułatwiającą ściganie sprawców przestępstw, jest wprowadzony w połowie 2016 r., powiązany z wejściem w życie ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. poz. 904, z późn. zm.), obowiązek rejestracji u polskich operatorów wszystkich kart SIM działających w systemie pre-paid. Karty niezarejestrowane przez użytkowników do 31 stycznia br. zostały dezaktywowane przez operatora.
Należy jednak stwierdzić, że zmiany te to tylko niewielka przeszkoda dla osób zajmujących się przestępczym procederem. Mogą one bez większego problemu pozyskać przez Internet z zagranicznych portali aukcyjnych lub sklepów internetowych karty SIM zagranicznych operatorów nieobarczone obowiązkiem rejestracji lub kupić kartę SIM „z drugiego obiegu" zarejestrowaną na tzw. słupa.
Innym przykładem może być ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219, z późn. zm.), w której zabrakło precyzyjnych zapisów w zakresie okresu retencji danych. Dane, które usługodawca jest zmuszony gromadzić, są zbierane i przechowywane w zależności od możliwości finansowych i „dobrych chęci" przez dowolny okres – może to być pół roku, miesiąc czy tydzień.
Skutkiem takich nieprecyzyjnych zapisów są bezpowrotnie tracone dane mające olbrzymie znaczenie dla prowadzonych postępowań i niejednokrotnie stanowiące jedyną podstawę prowadzenia dalszych czynności wykrywczych.

Dużym ułatwieniem i pomocą w realizacji działań przestępczych było też wprowadzenie do obiegu przez banki kart płatniczych w systemie „pre-paid" (przedpłaconych). Można je było uzyskać z banku bez potwierdzenia i przypisania do nich tożsamości użytkownika, a umożliwiały one dokonywanie całkowicie anonimowych płatności internetowych, przelewów na inne konta bankowe czy wypłat środków pieniężnych w całej sieci bankomatów.

Jednak w wyniku przeprowadzonej przez Urząd Komisji Nadzoru Finansowego (UKNF) analizy, Komisja Nadzoru Finansowego (KNF) w dniu 10 lipca 2015 r. wystosowała do zarządów banków krajowych pismo, w którym zajęła stanowisko, że prowadzona przez banki działalność w zakresie kart pre-paid nie jest wydawaniem pieniądza elektronicznego w rozumieniu obowiązujących przepisów prawa i nie powinna być kontynuowana bez przyjęcia istotnych zmian[6].
W wyniku podjętych przez KNF działań instytucje bankowe zaprzestały wydawania kart na okaziciela w pierwotnie przyjętej formie.

Aspektem utrudniającym zwalczanie cyberprzestępczości jest także dynamiczny rozwój narzędzi, które wykorzystane przez nawet niezaawansowanego użytkownika zapewniają mu ukrycie jego tożsamości i prawdziwej lokalizacji. Służą do tego narzędzia anonimizujące sieć – TOR lub usługa serwera Anonymous Proxy – używane przez sprawców przestępstw.

Kolejnym ułatwieniem, z którego cyberprzestępcy chętnie korzystają, jest anonimowy dostęp do Internetu realizowany z wykorzystaniem punktów darmowego dostępu do Internetu – hotspot.
Inną trudnością w zwalczaniu cyberprzestępczości są różnice legislacyjne pomiędzy krajami, co wydłuża lub wręcz uniemożliwia szybkie ustalenie sprawcy. Wnioski o ściganie sprawców lub dane udostępniane przez firmy prowadzące działalność poza granicami Polski trafiają do tamtejszych sądów i są rozpatrywane według przepisów prawa, które obowiązują w danym państwie. W przypadku, gdy w określonym kraju czyn nie stanowi przestępstwa lub nie ma podstaw do wydania danych, takie wnioski pozostają rozpatrzone odmownie. Te procedury w znaczący sposób wydłużają czas realizacji czynności niezbędnych do wykrycia sprawcy czynności, a szybkość działania przy tego typu przestępczości jest niejednokrotnie kluczem do sukcesu. Co więcej, w niektórych przypadkach to firmy zagraniczne, same, bez udziału sądu czy prokuratury, interpretują przesłanki przemawiające za udostępnieniem danych i ich zakresu. Przykładowo, administratorzy portali, takich jak np. google.com, facebook.com czy youtube.com, we własnym zakresie analizują żądania policji i podejmują decyzje, czy udostępnić dane.
Kolejnym istotnym utrudnieniem dla organów ścigania jest transgraniczność Internetu polegająca na bardzo łatwym dostępie do usług świadczonych przez firmy zagraniczne (konta e-mail, komunikatory itp.). Nie obowiązują ich przepisy polskiego prawodawstwa w zakresie udostępniania danych niezbędnych dla prowadzonych postępowań, co wymusza prowadzenie dodatkowych czynności z zaangażowaniem organów ścigania innych państw. Obecnie stosowany system międzynarodowej wymiany informacji, w którym jest brak jednolitego, elektronicznego i bezpośredniego systemu międzynarodowej wymiany informacji pomiędzy komórkami zajmującymi się cyberprzestępczością, powoduje liczne trudności. Należy również zauważyć, że o ile wymiana informacji z organami ścigania z Europy Zachodniej, z mniejszymi lub większymi proble-

mami, ale jest w sposób ciągły prowadzona, o tyle uzyskanie informacji z krajów egzotycznych, takich jak Chiny, Indie czy Ameryka Południowa, jest praktycznie niemożliwe.
Wszystkie te elementy powodują co najmniej wydłużenie czasu uzyskiwania informacji lub w ogóle uniemożliwiają jej otrzymanie, co ma istotny wpływ na skuteczne i efektywne zwalczanie przestępczości internetowej.

Tendencje i ewentualne nowe trendy w zagrożeniach bezpieczeństwa cyberprzestrzeni

Całe zjawisko cyberprzestępczości jest napędzane bardzo prostą zależnością. Rosnąca liczba użytkowników Internetu i – co za tym idzie – coraz większa ilość ulokowanych tam środków finansowych powoduje wzrost liczby przestępstw popełnianych za pomocą komputera. Na podstawie analizy bieżących tendencji przewiduje się szybki wzrost przestępczości w zakresie wykorzystania zaawansowanych technologii informatycznych, które mogą objąć nowe dziedziny życia społecznego i gospodarczego. Telefony komórkowe, smartfony, tablety czy komputery oraz sieć Internet – poprzez możliwości jakie dają – odgrywają coraz większą rolę w nielegalnej działalności lub też w znaczny sposób ułatwiają jej prowadzenie. Handel przedmiotami uzyskanymi w wyniku przestępstwa, oszustwa internetowe, pirackie oprogramowanie, naruszenia praw autorskich czy coraz częściej spotykana przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych to tylko niewielka część czynów, jakie można popełnić, nie wychodząc z domu, nie narażając się na bezpośredni kontakt ze swoją ofiarą, przypadkowym świadkiem, służbami porządkowymi, takimi jak straż miejska lub pracownicy ochrony czy przedstawicielami organów ścigania.
Sprawcy przestępstw, którzy z premedytacją dążą do zapewnienia sobie „sukcesu przestępczego", coraz częściej wykorzystują specjalne oprogramowanie umożliwiające kamuflowanie miejsca, z którego działają. Również zjawiska takiego typu jak np. sieć TOR czy wirtualne systemy dokonywania płatności w Internecie BitCoin, pozostające poza jakąkolwiek kontrolą instytucji finansowych, sprzyjają realizacji przestępczych celów.
Jest przewidywany dalszy wzrost przestępczości w zakresie wykorzystania zaawansowanych technologii informatycznych, które mogą dotyczyć nowych aspektów, jak np. upowszechniający się podpis elektroniczny. Internet będzie używany także do szantażu i wyłudzeń, np. poprzez groźbę wykorzystania luk w zabezpieczeniach systemów komputerowych lub „eksploatację" skradzionych informacji. Będzie ujawniana coraz większa liczba przestępstw komputerowych o wysokiej jednostkowo wartości strat, a także nastąpi dalszy wzrost liczby oszustw na aukcyjnych portalach internetowych. Największym zagrożeniem najprawdopodobniej będzie – ze względu na mało skomplikowany charakter przestępstwa – oszustwo dokonywane z wykorzystaniem platform handlowych i portali aukcyjnych. W najbliższych latach, jak można przypuszczać, wzrośnie obrót na aukcjach internetowych i serwisach darmowych ogłoszeń, gdyż coraz więcej osób będzie poszukiwać tzw. „zakupowych okazji", z kolei inni będą sprzedawać przedmioty codziennego użytku, które są im już zbędne lub w celu poprawy stanu budżetu domowego, co bezpośrednio może się przełożyć na wzrost przestępstw internetowych. Nieograniczony dostęp do szerokich zasobów Internetu na całym świecie spowoduje, iż należy się spodziewać dynamicznego rozwoju nowych form cyberprzestępczości i nasilenia już istniejących, takich jak akty terroru, oszustwa, przestępstwa związane z phishingiem, handlem ludźmi, rozpowszechnianiem pornografii dziecięcej czy oferowaniem do sprzedaży przedmiotów pochodzących z przestępstwa, przestępstwa związane z naruszeniem praw własności intelektualnej, a także szpiegostwo elektroniczne, nieuprawniony dostęp do informacji czy kradzieże tożsamości i szantaż.

[1] *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Komitet Stały Rady Ministrów, 25 czerwca 2013 r., https://www.cert.gov.pl/cer/publikacje/polityka-ochrony-cyber/639,Polityka-Ochrony-Cyberprzestrzeni-Rzeczypospolitej-Polskiej.html [dostęp: 13.12.2017 r.].

[2] http://www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298370,Czym-jest-cyberprzestepstwo.html [dostęp: 13.12.2017 r.].

[3] Konwencja Rady Europy o cyberprzestępczości („Konwencja o cyberprzestępczości") podpisana w dniu 23 listopada 2001 r.

[4] Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów „W kierunku ogólnej strategii zwalczania cyberprzestępczości" 22 maja 2007 r., http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52007DC0267 [dostęp: 13.12.2017 r.].

[5] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wolters Kluwer Polska, 2010, s. 55.

[6] Stanowisko KNF w sprawie wydawania przez banki tzw. kart przedpłaconych. 10 lipca 2015 r., https://www.knf.gov.pl/knf/pl/komponenty/img/stanowisko_ws_wydawania_kart_przedplaconych_42192.pdf [dostęp: 13.12.2017 r.].

Summary

Cybercrime – an attempt to diagnose the phenomenon

The purpose of the article is to present to an every reader, being simultaneously a user of a computer and the Internet, crucial definitions and issues in cybercrime in an accessible form. It is also intended to present the basic division of this type of crime, characteristic features allowing for distinguishing individual criminal acts, as well as the biggest problems and difficulties – both legal and organizational – which the Polish law enforcement agencies deal with in fighting them.
Due to the rapid development of the Internet, internet services or making available sensitive data in mobile devices more and more often, this issue should be of great interest for each of us.
In the best comprehended self-interest every Internet, computers or telecommunications devices user, due to more and more sophisticated ways of committing offences or Internet frauds committed with the application of the social engineering and new technologies, should familiarize well with the problems such as bases of fighting cybercrime or "best practices" essential for the safe use of the Internet.

Tłumaczenie: Renata Cedro

ZWALCZANIE CYBERPRZESTĘPCZOŚCI W KONTEKŚCIE MIĘDZYNARODOWYM

kom. Tomasz Pawlicki

radca Wydziału Rozpoznania
Biura do Walki z Cyberprzestępczością KGP

Od 11 lat bierze udział w realizacji spraw, w których wykorzystywana jest nowoczesna technologia informatyczna, zarówno jako narzędzie do popełniania przestępstw, jak i jako jeden z elementów pozwalających na uzyskanie szerszej wiedzy na temat zdarzenia. W latach 2006–2016 pracował w Laboratorium Kryminalistycznym Komendy Wojewódzkiej Policji w Łodzi, gdzie od 2013 r. kierował Sekcją Badań Dokumentów, w skład której wchodziły pracownie badań: informatycznych, wizualnych, dokumentów, antroposkopijnych, poligraficznych (wariograficznych). Jest członkiem Polskiego Towarzystwa Informatycznego, które ma na celu wspieranie działalności naukowej związanej z informatyką i jej popularyzacją w każdej dziedzinie życia. Od 2017 r. wykłada w Krajowej Szkole Sądownictwa i Prokuratury w Lublinie – centralnej instytucji odpowiedzialnej za szkolenie wstępne oraz ustawiczne kadr sądownictwa i prokuratury w Polsce.

podkom. Agnieszka Stąpór

ekspert Wydziału Rozpoznania
Biura do Walki z Cyberprzestępczością KGP

Absolwentka Instytutu Nauk Politycznych Uniwersytetu Warszawskiego. Przez większość swojej 15-letniej pracy w Policji związana ze służbą kryminalną. Od 2013 r. zajmuje się realizacją spraw oraz zagadnień z zakresu zwalczania cyberprzestępczości. Obecnie – jako ekspert krajowy wykonuje zadania w ramach EMPACT-u (European Multidisciplinary Platform Against Criminal Threats) przy Europolu, realizując z ramienia polskiej Policji przedsięwzięcia w ramach AP (Analysis Project Terminal) dotyczące skutecznej współpracy z organami ścigania państw członkowskich UE z zakresu zwalczania cyberprzestępczości dotyczącej oszustw z wykorzystaniem elektronicznych oraz internetowych instrumentów płatniczych.

W artykule omówiono kwestie dotyczące cyberprzestępczości. Pierwsza część tekstu skupia się na różnicach pomiędzy pojęciem „cybercrime” (cyberprzestępczość) oraz „cybersecurity” (cyberbezpieczeństwo). Zgodnie z opinią autora istnieją problemy z rozróżnianiem powyższych dwóch definicji. Należy stwierdzić, iż odnoszą się one do różnych poziomów technologii IT. Środkowa część artykułu poświęcona jest organizacji międzynarodowej współpracującej z Polską, a zwłaszcza z Policją. Bezsprzecznie, jednym z najważniejszych dokumentów stanowiących podstawę współpracy w zakresie informatyki pomiędzy Polską oraz innymi krajami Unii Europejskiej jest konwencja budapeszteńska. W publikacji autor próbuje również interpretować proceduję IP. Omawia też aspekty cyberprzestępczości, takie jak: definicje prawne, zagrożenia, wyzwania.

Mam nadzieję, iż czytelnicy znajdą w artykule odpowiedzi na najbardziej nurtujące ich pytania dotyczące cyberprzestępczości.

WSTĘP

The number of transistors in a dense integrated circuit doubles approximately every two years (Liczba tranzystorów w układzie podwaja się co dwa lata – tłumaczenie autorów)[1]. Jakie znaczenie mają te słowa dla przeciętnego użytkownika elektroniki? Oznaczają one, że w przypadku zakupu jakiegokolwiek sprzętu elektronicznego możemy się spodziewać, że jego możliwości obliczeniowe znacznie zmniejszą się w ciągu dwóch lat. W praktyce oznacza to również, że wartość rynkowa produktu zmaleje.

W przypadku technologii informatycznych skutkuje to daleko idącymi zmianami dotyczącymi komunikacji, przekazu danych, *modus operandi* w sprawach związanych z cyberprzestępczością. Od specjalistów IT, biegłych oraz osób zajmujących się cyberprzestępczością wymaga się nieustannego uczenia się, poznawania i zgłębiania kolejnych możliwości technicznych, wykorzystywanych do popełniania cyberprzestępstw.

Niniejszy artykuł ma na celu wprowadzenie i zapoznanie czytelnika z obecnymi trendami w zakresie przeciwdziałania cyberprzestępczości, zapobiegania jej oraz stosowania prawa z tego zakresu.

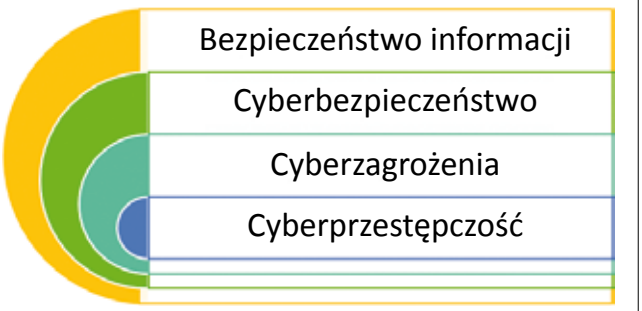
Cyberprzestępczość a cyberbezpieczeństwo

Z własnych obserwacji autorów wynika, że terminy te są często mylone. Nie ulega jednak wątpliwości, że istnieje wyraźne rozróżnienie obydwu pojęć. Na poziomie krajowym cyberprzestępczość dosyć precyzyjnie wyjaśniono jako: „czyn zabroniony popełniony w obszarze cyberprzestrzeni". Definicja ta została zawarta w *Rządowym Programie Ochrony Cyberprzestrzeni RP na lata 2011–2016*[2], kluczowym dla tej sprawy dokumencie (obecnie obowiązuje dokument *Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020*[3]). Z kolei cyberprzestrzeń definiowana jest jako: „cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami". Sama problematyka związana z cyberprzestępczością została dostrzeżona na początku XX wieku, jednak dowodem podjęcia faktycznych prac w przedmiotowym zakresie jest ogłoszona 23 listopada 2001 r. w Budapeszcie Konwencja Rady Europy o cyberprzestępczości (*Convention On Cybercrime*)[4].

Natomiast cyberbezpieczeństwo RP znalazło swoją definicję w dokumencie pn. „Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015[5]", w której to czytamy: „proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni". Jest to zatem pojęcie znacznie szersze, obejmujące całość systemów teleinformatycznych. Zakres powyższych pojęć został dobrze zobrazowany w kontekście bezpieczeństwa informacji na rysunku nr 1.

Z punktu widzenia organów ścigania i wymiaru sprawiedliwości jednym z kluczowych dokumentów zajmujących się cyberprzestępczością na poziomie ogólnym jest wspomniana już wcześniej Konwencja Rady Europy o cyberprzestępczości. Pomimo upływu kilku lat w dalszym ciągu dokument ten jest

Rysunek 1. Zasięg oddziaływania związany z bezpieczeństwem informacji.



Źródło: opracowanie własne na podstawie J. Kosiński, *Paradygmaty cyberprzestępczości*, rysunek 1, s. 14.

podstawą do tworzenia wspólnej polityki krajów członkowskich Rady Europy w zakresie zwalczania cyberprzestępczości. Ponadto wciąż stanowi punkt odniesienia wielu rozwiązań prawnych w pracach nad przeciwdziałaniem zagrożeniom cyberbezpieczeństwa i zwalczania tych zagrożeń.

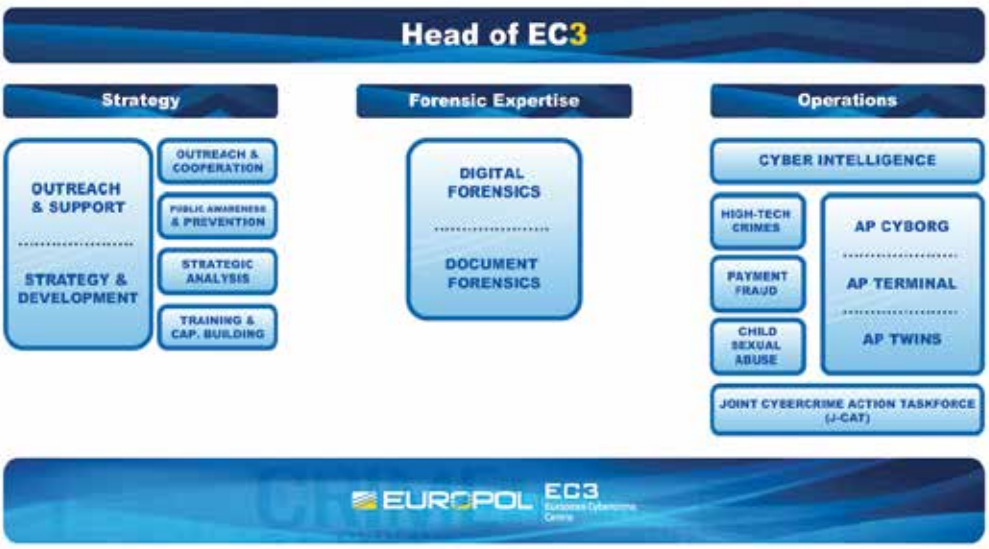
Co prawda w konwencji nie zdefiniowano wprost pojęcia cyberprzestępczości, ale wskazano na zagrożenia wymagające wspólnego działania w ramach ochrony sieci informatycznych i informacji elektronicznych przed ich wykorzystaniem w celu popełniania przestępstw.

Cyberprzestępczość – współpraca w ramach UE

Z każdym rokiem wzrasta liczba użytkowników Internetu oraz elektronicznych nośników/mediów transmisyjnych. To właśnie urządzenia elektroniczne stanowią znaczące źródło pozyskiwania informacji ważnych dla wykrywania, dowodzenia, a także zapobiegania przestępstwom. Należy zauważyć wyraźne tendencje do przenoszenia pewnych zachowań przestępczych ze świata rzeczywistego do sieci komputerowej. Dotyczy to szczególnie oszustw, wyłudzeń, handlu nielegalnymi substancjami oraz treściami. Coraz częściej Internet wykorzystywany jest przez międzynarodowe organizacje przestępcze jako narzędzie komunikacji. Dzieje się tak przede wszystkim ze względu na ogólnoświatowy zasięg Internetu, a granice państw nie stanowią w tym przypadku żadnej bariery dla przestępców. Z tego też względu pojęcie cyberprzestępczości nabiera nowego znaczenia, zaś badania cyfrowych nośników danych i pozyskane tą drogą informacje są niezwykle istotne szczególnie dla przestępstw o charakterze transgranicznym. Dalszy rozwój badań pozwoliłby na podniesienie bezpieczeństwa międzynarodowego oraz pozyskiwanie informacji ważnych dla prowadzonych śledztw i dochodzeń. Wymiana doświadczeń oraz informacji między ekspertami z całego świata to jedyny skuteczny sposób (poza technologią), który może przeciwdziałać takim tendencjom. Dlatego też nie ulega wątpliwości, że sprawną walkę Państwa z cyberprzestępczością gwarantuje międzynarodowa współpraca w tym zakresie. Z uwagi na zakres merytoryczny, jedną z podstawowych komórek organizacyjnych Policji powołanych do wymiany informacji w zakresie cyberprzestępczości jest Biuro do Walki

z Cyberprzestępczością (dalej: BdWzC) Komendy Głównej Policji. Biuro aktywnie uczestniczy w międzynarodowych panelach oraz warsztatach dotyczących zwalczania cyberprzestępczości. Dąży również do wykreowania strony polskiej jako gotowego do podjęcia działań partnera w walce z przestępczością w sieci.
Obok przedstawiono przykładowe organizacje międzynarodowe zwalczające cyberprzestępczość. W niniejszym artykule postanowiono przybliżyć jedynie wybrane. Należy przy tym pamiętać, że Interpol, UNDOC, Eurojust i wiele innych organizacji mają również znaczący wpływ na kształtowanie oraz egzekwowanie prawa w zakresie cyberprzestępczości.

Rysunek 2. Struktura Europol EC3.



Źródło: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [dostęp: 16.11.2017 r.].

European Cybercrime Center (EC3)

Europejskie Centrum ds. Cyberprzestępczości (European Cybercrime Center – EC3[6]) powstało w 2013 r. jako komórka Europolu, mająca na celu wzmocnienie działań związanych z egzekwowaniem prawa w zakresie cyberprzestępczości na terenie Unii Europejskiej. Z punktu widzenia Europejskiego Urzędu Policji bezpieczeństwo w Internecie jest bardzo ważnym elementem w walce z przestępczością. Jak podaje EC3, globalne koszty związane z przeciwdziałaniem cyberprzestępczości są liczone w setkach miliardów euro rocznie. Tym samym jest to ogromny problem, który wymaga dodatkowego wsparcia ze strony UE. Cyberprzestępczość stanowi w rzeczywistości problem zróżnicowany, obejmujący wiele aspektów techniczno-prawnych, zaś EC3 − kluczowy element odpowiedzi na to zagrożenie, wdrażając trzypoziomowe podejście mające na celu walkę z cyberprzestępczością poprzez:

- strategię,
- kryminalistykę,
- działania operacyjne.

W zainteresowaniu Europolu znajduje się pomoc w zwalczaniu dziewięciu priorytetowych obszarów przestępczych. Dla każdego z nich wdrożono wieloletni plan strategiczny, tzw. projekt EMPACT − European Multidisciplinary Platform Against Criminal Threats (Europejska Interdyscyplinarna Platforma przeciw Przestępstwom Kryminalnym) oraz plan działania operacyjnego na lata 2014−2017, który obejmuje następujące rodzaje przestępczości:

- nielegalną imigrację,
- handel ludźmi,
- podrabianie produktów wpływających na zdrowie i bezpieczeństwo publiczne,
- oszustwa podatkowe, w tym akcyzowe i karuzele VAT,
- produkcję narkotyków syntetycznych i handel tymi narkotykami,
- handel kokainą i heroiną w UE,
- cyberprzestępczość (w tym cyberataki, pornografię dziecięcą w Internecie, fałszerstwa kart płatniczych),
- nielegalny handel i wykorzystanie broni palnej,
- zorganizowaną przestępczość przeciwko mieniu (grupy mobilne).

Od 2018 r. należy się spodziewać modyfikacji obecnego podejścia.
Bardzo przydatnym narzędziem pozwalającym na szybką wymianę informacji pomiędzy ekspertami z różnych krajów jest Europejska Platforma Wymiany Danych przez Ekspertów (EUROPOL Platform for Experts – EPE[7]). Ta platforma wymiany informacji obejmuje wszystkie dziedziny będące w zainteresowaniu Europolu/EC3, wspomagając i uzupełniając tym samym wiedzę poszczególnych uczestników.

EMPACT

Za priorytetowe działania można przyjąć uczestnictwo polskiej Policji w przedsięwzięciach EMPACT. Obecnie BdWzC KGP uczestniczy w ramach działań operacyjnych (patrz rysunek 2) w niżej przedstawionych przedsięwzięciach. Należy dodać, iż *Analysis Project* (dawniej *Focal Point*) to skoordynowane działania ukierunkowane na nadawanie priorytetów zasobom w celu zapewnienia trafności decyzji, przy jednoczesnym ograniczeniu celów wspieranych przez organizacje partnerskie UE.

Analysis Project Terminal (w ramach EMPACT Payment Fraud) – koordynacja krajowa od 2018 r. przez Wydział Rozpoznania BdWzC KGP.
Projekt skupiający swoje działanie na realizowaniu czynności operacyjnych związanych ze śledztwami w sprawie międzynarodowych oszustw związanych z płatnościami elektronicznymi i online. Dzięki takiemu podejściu Europol EC3 pomaga przeciwdziałać nowym zagrożeniom przestępczym pojawiającym się w sieci poprzez współpracę z organami ścigania, sektorem prywatnym i organami regulacyjnymi płatności, takimi jak Eu-

ropejski Bank Centralny i banki krajowe, w celu zapewnienia bezpieczeństwa i podniesienia zaufania klientów do płatności elektronicznych i internetowych.

W ramach przedsięwzięcia realizowane są m.in. międzynarodowe akcje:

- **Global Airlines Action Day** (GAAD)[8]

Międzynarodowa akcja koordynowana przez EC3 Europol, przy wsparciu Interpolu w Singapurze i Ameripol w Bogocie, oraz kanadyjskie i amerykańskie organy ścigania, skierowana przeciwko nadużyciom tożsamości, fałszowania dokumentów i nielegalnej migracji.

- **The European Money Mule Action** (EMMA)[9]

Międzynarodowa akcja koordynowana przez EC3 Europol skierowana przeciwko oszustwom płatniczym. Money Muling („Muły") to osoby rekrutowane przez organizacje przestępcze w celu otrzymywania i przekazywania nielegalnie uzyskanych pieniędzy między rachunkami bankowymi i/lub krajami.

- **Analysis Project Cyborg**[10] – koordynacja krajowa od 2018 r. przez Wydział Wsparcia i Badań BWC KGP.

Projekt wspiera badania dotyczące cyberprzestępczości wpływającej na krytyczną infrastrukturę komputerową i infrastrukturę sieciową w UE. Szczególny nacisk położony jest na cyberprzestępczość zorganizowanych grup, które osiągają duże zyski z przestępstw. Działanie obejmuje szeroki zakres przestępstw z wykorzystaniem zaawansowanej technologii, m.in. złośliwego oprogramowania (kreacja i dystrybucja kodu), ransomware, włamań, phishingu, kradzieży tożsamości i oszustw związanych z Internetem.

European Union Agency for Law Enforcement Training[11] (CEPOL)

Europejska Akademia Policyjna (CEPOL), utworzona w 2000 r. na mocy decyzji Rady UE 2000/820/WSiSW[12] z dnia 30 grudnia 2000 r., początkowo nie posiadała osobowości prawnej i nie była agencją wspólnotową. Dopiero na mocy decyzji Rady UE ds. WSiSW nr 681/2005/JHA z dnia 20 września 2005 r. CEPOL uzyskał status agencji UE. Decyzja ta weszła w życie z dniem 1 stycznia 2006 r. i do chwili obecnej stanowi podstawę prawną funkcjonowania CEPOL. Budżet roczny CEPOL stanowi subsydium z budżetu UE z sekcji budżetowej Komisji Europejskiej Celem CEPOL – zgodnie z art. 6 decyzji 681/2005/JHA jest optymalizacja współpracy między instytucjami szkoleniowymi policji państw członkowskich, w szczególności zaś:

- podnoszenie poziomu wiedzy o systemach i strukturach policji państw członkowskich oraz o przestępczości transgranicznej,
- międzynarodowej współpracy policyjnej,
- podniesienie poziomu wiedzy o instytucjach UE, ich roli, funkcjonowaniu oraz mechanizmach decyzyjnych, w szczególności związanych ze zwalczaniem przestępczości na szczeblu UE,
- zapewnienie szkoleń zgodnych z demokratycznymi standardami.

Zadania te CEPOL realizuje poprzez następujące działania, wyszczególnione w art. 7 Decyzji 681/2005/WSiSW:

- szkolenia dla wyższych rangą funkcjonariuszy policji oparte na wspólnych standardach,
- opracowywanie zharmonizowanych programów szkolenia dla funkcjonariuszy policji,
- upowszechnianie rezultatów prac naukowo-badawczych,
- szkolenia dotyczące cywilnego zarządzania w sytuacjach kryzysowych,
- szkolenia dla funkcjonariuszy policji państw kandydujących,
- organizację wymiany funkcjonariuszy policji państw członkowskich i partnerstwa wschodniego,
- rozwój platformy elektronicznej spełniającej standardy bezpieczeństwa,
- podnoszenie umiejętności językowych funkcjonariuszy policji.

Współpraca o charakterze szkoleniowym obejmuje szerokie spektrum zagadnień związanych przede wszystkim z realizacją poszczególnych komponentów oferty szkoleniowej CEPOL. Jej najistotniejszym i podstawowym przejawem są specjalistyczne przedsięwzięcia szkoleniowe (kursy, seminaria, warsztaty oraz konferencje) dotyczące zagadnień o charakterze paneuropejskim, kluczowych z punktu widzenia UE oraz zgodnych z potrzebami szkoleniowymi państw członkowskich. Podstawowymi wymogami, jakie muszą spełniać osoby delegowane, są: właściwość merytoryczna, doświadczenie w przedmiotowym zakresie oraz dobra znajomość języka angielskiego.

Cyberprzestępczość – międzynarodowa wymiana danych

W celu prawidłowej interpretacji przepisów prawa krajowego oraz międzynarodowego w pierwszej kolejności należy wyjaśnić różnicę między dwoma pojęciami ICP (Internet Content Provider) a ISP (Internet Service Provider). Internet Content Provider to zewnętrzny dostawca oferujący usługę dostępu do treści internetowych. Zaś Internet Service Provider to zewnętrzny dostawca oferujący usługę dostępu do Internetu. Odróżnienie to ma ogromne znaczenie dla późniejszej interpretacji przepisów.

W obecnej sytuacji nasilenia istniejących zagrożeń z wykorzystywaniem komputerów, urządzeń mobilnych oraz szeroko pojętej sieci teleinformatycznej zwalczanie cyberprzestępstw nie jest możliwe w pojedynkę, bez wymiany doświadczeń, dobrych praktyk oraz rozwijania intensywnej współpracy pomiędzy poszczególnymi organami ścigania pastw UE. Transgraniczny charakter działania przestępców stawia wyzwania zarówno technologiczne, jak i dotyczące dostosowania instrumentów prawnych do efektywnego eliminowania i ograniczania tejże aktywności w Internecie.

Istotnym elementem dotyczącym umożliwienia skutecznego zwalczania zagrożeń o charakterze kryminalnym jest Konwencja Rady Europy o cyberprzestępczości[13], sporządzona w Budapeszcie dnia 23 listopada 2001 r., zwana Konwencją Budapesztańską (ratyfikowana została przez Polskę w dniu 1 czerwca 2015 r.). Ujednolica ona oraz wytycza standardy międzynarodowe, będąc jednocześnie skutecznym narzędziem wykorzystywanym do zwalczania cyberprzestępczości społeczeństwa informacyjnego.

Jednym z efektów Konwencji (poza dostosowaniem przepisów prawa krajowego poszczególnych państw, które ratyfikowały przedmiotowy akt prawny) jest wyznaczenie (zgodnie z zapisami art. 35 Konwencji) punktów kontaktowych funkcjonujących w systemie „24/7", mających za zadanie udzielanie wsparcia partnerom zagranicznym (tj. organom ścigania) w realizacji m.in. spraw niecierpiących zwłoki bądź wypełniających przesłanki z kategorii zagrożenia życia i zdrowia, a związanych

z niezwłocznym zabezpieczeniem przechowywanych przez danego Providera danych teleinformatycznych, zgodnie z art. 29 i 30 Konwencji. W warunkach polskich rolę tę odgrywa Sekcja Obsługi Całodobowej Wydziału Rozpoznania BdWzC KGP jako oficjalny punkt kontaktowy realizujący nałożone na nią zadania z zakresu omawianej współpracy międzynarodowej.
W ramach prowadzonej sprawy każdy polski policjant realizujący czynności może wystąpić z odpowiednim wnioskiem (opracowanym na potrzeby powyższych działań przez Wydział Rozpoznania BdWzC KGP), po uprzednim zaakceptowaniu przez odpowiedniego kierownika komórki organizacyjnej polskiej Policji, o zwrócenie się do organów ścigania państwa, które przystąpiło do realizacji zapisów Konwencji, o zabezpieczenie danych teleinformatycznych oraz internetowych na potrzeby prowadzonego postępowania. Każdorazowo wniosek zostaje skierowany drogą elektroniczną na wskazany adres poczty elektronicznej, do odpowiedniego punktu kontaktowego, w celu zabezpieczenia niezbędnych danych. Następnie, w ramach międzynarodowej pomocy prawnej (MLA – Mutual Legal Assistance), strona występująca z wnioskiem o zabezpieczenie danych zobowiązana jest dostarczyć, stosując instrumenty międzynarodowe, odpowiedni dokument będący postanowieniem, na mocy którego ujawnione zostaną zabezpieczone dane.

Cyberprzestępczość – oddziaływanie

Trzy główne zagrożenia zidentyfikowane w 2017 r. przez Unię Europejską w walce z cyberprzestępczością stanowią:
- cyberprzestępstwa popełniane przez zorganizowane grupy, generujące duże zyski poprzez oszustwa internetowe,
- cyberprzestępstwa powodujące poważne szkody dla ofiary, np.: wykorzystywanie seksualne dzieci on-line,
- cyberprzestępstwa (w tym cyberataki) wpływające na krytyczne systemy infrastruktury i informacji w Unii Europejskiej.

PODSUMOWANIE

Wraz z postępującym rozwojem technologicznym wszystkie tradycyjne rodzaje przestępstw ewoluują i coraz częściej znajdują swoje odpowiedniki w cyberprzestrzeni. Mowa tu o takich zjawiskach, jak: cyberprzemoc, cyberkradzież, cyberhejt i wiele innych spenalizowanych już zachowań, np. stalking.
Są one bardzo niebezpieczne, gdyż dotyczą często setek, a nawet tysięcy osób (np. atak phishingowy). Niestety, obecnie stosunkowo niska znajomość technologii informatycznych przez starsze pokolenie, a jednocześnie dosyć lekceważące (zbyt ufne) podejście młodego pokolenia do problematyki cyberprzestępczości prowadzą często do nieodwracalnych skutków. Nie można lekceważyć zjawisk związanych z cyberprzestępczością, dlatego też w grudniu 2016 r. zostało powołane Biuro do Walki z Cyberprzestępczością Komendy Głównej Policji. Jako jedyne Biuro w KGP ma charakter realizacyjny − w praktyce oznacza to, iż funkcjonariusze pełniący w nim służbę biorą czynny udział w realizacji spraw związanych ze zwalczaniem przedmiotowej działalności przestępczej. W mijającym roku, niespełna parę miesięcy po powstaniu Biura, dzięki bezpośredniemu zaangażowaniu policjantów zatrzymano m.in. osobę, która zajmowała się handlem danymi osobowymi. W wyniku tej działalności zostało sprzedanych co najmniej 56 tys. rekordów z bazy danych wartej około 110 mln zł. Natomiast w październiku 2016 r. zatrzymano 4 osoby zamieszane w wykradanie, a następnie odsprzedawanie danych osobowych konkurencyjnej firmie telekomunikacyjnej.
Nie można zapomnieć, iż ważnym elementem w walce z nowymi trendami jest ustawiczne podnoszenie wiedzy i umiejętności, dlatego też BdWzC KGP zostało włączone do Międzynarodowego Stowarzyszenia Edukacyjnego ECTEG (European Cybercrime Training and Education Group), dzięki czemu polska Policja będzie miała dostęp do materiałów szkoleniowych wykorzystywanych w policji niemal całego świata.
Bez względu na podjęte do tej pory działania należy mieć na uwadze fakt, iż cyberprzestępczość to zjawisko dynamiczne i bardzo szybko dostosowujące się do nowych osiągnięć w informatyce. Tylko dzięki zdecydowanym działaniom i specjalistycznym wydziałom, powołanym specjalnie w tym celu, mamy możliwość prowadzenia skutecznej walki i eliminacji zagrożeń płynących z sieci.

[1] *Moore's law*, https://en.wikipedia.org/wiki.Moore's-law [dostęp: 16.11.2017 r.].
[2] *Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011–2016,* https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ness-map/Poland_Cyber_Security_Strategy.pdf [dostęp: 16.11.2017 r.].
[3] *Strategia Bezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020,* https://www.gov.pl/documents/31305/0/strategia_v_29_09_2016.pdf/b621e7df-dca7-ad54-210c-5d58eec650f0 [dostęp: 16.11.2017 r.].
[4] Konwencja Rady Europy o cyberprzestępczości, Budapeszt, 23 listopada 2001 r. (Dz. U. z 2015 r. poz.728).
[5] *Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015,* w: http://en.bbn.gov.pl/ftp/dok/01.DCB.pdf [dostęp: 16.11.2017 r.].
[6] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 [dostęp: 16.11.2017 r.].
[7] https://epe.europol.europa.eu.
[8] *Global Airlines Action Day*, https://www.europol.europe.eu/activities-services/europol-in-action/global-airline-action-day [dostęp: 16.11.2017 r.].
[9] *The European Money Mule Action*, https://europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling [dostęp: 16.11.2017 r.].
[10] *Analysis Project Cyborg*, https://www.europol.europa.eu/activities-services/crime-areas-trends/europol-analysis-projects [dostęp: 16.11.2017 r.].
[11] *European Union Agency for Law Enforcement Training*, www.cepol.europa.eu [dostęp: 16.11.2017 r.].
[12] Dz. Urz. UE L 336/1 z 30.12.2000 r.
[13] Konwencja Rady Europy o cyberprzestępczości, Budapeszt, 23 listopada 2001 r. (Dz. U. z 2015 r. poz. 728).

Summary

Introduction to cybercrime

The article discusses the issues related to problems with cybercrime. The first part of the text focuses on differences between cybercrime and cybersecurity. Into the author's opinion we have some problems with distinguish these two definitions. But they relate to different levels of IT technology. In the middle of the article we try to present the internationale organisation which cooperates with Poland especially with Police department. With no doubt one of the most important document which creates IT relations between Poland and other UE countries is Budapest convention. We try to interpretate IP-procedure. Cybercrime inter aspects are – law definitions, threat, challenges. I hope that readers will find in this article the primary answers about the cybercrime.

ARTYKUŁ NAUKOWY

BANKOWOŚĆ ELEKTRONICZNA – zagrożenia

mł. insp. dr inż. Robert Maciejczyk

zastępca kierownika
Zakładu Służby Kryminalnej CSP

W czasach, kiedy środki płatnicze, takie jak drukowane banknoty i wybijane monety, są sukcesywnie wypierane przez nowoczesne metody płatnicze, przy użyciu Internetu lub smartfona, bezpieczeństwo tych transakcji staje się jednym z nadrzędnych celów w ochronie mienia należącego do klientów banków. Niniejsze opracowanie ma na celu przybliżenie problematyki działania sprawców dokonujących przejęcia środków płatniczych oraz sposobów zabezpieczenia się przed tego rodzaju przestępstwami, zarówno w obszarze działań usługodawcy, jakim jest bank, jak i klienta, którego nieostrożne działania mogą ułatwić sprawcom dokonanie na jego mieniu przestępstwa.

WSTĘP

Bankowość elektroniczna, jako forma dostarczania usług bankowych do klientów, stanowi obecnie najszybciej rozwijający się obszar bankowości. Jest to w dużej mierze podyktowane postępującą informatyzacją społeczeństwa, jak również rosnącą świadomością udogodnień płynących z korzystania z tego typu rozwiązań. Jeszcze kilkadziesiąt lat temu w Polsce trudno było szukać w sklepach terminali umożliwiających płatność kartą, pojedyncze bankomaty znajdowały się tylko w największych miastach, a o bankowości internetowej nikt nie słyszał. Dziś rzeczywistość wygląda inaczej, niemal każdy obywatel posiada kartę płatniczą, a większość sklepów umożliwia regulowanie należności za jej pomocą, widok bankomatów nikogo nie dziwi, a transakcje w ramach bankowości internetowej realizujemy już nie tylko za pośrednictwem komputerów, ale wprost z ekranu smartfona. Niewiele dzieli nas od czasów, kiedy większość transakcji przeniesie się docelowo do świata wirtualnego pieniądza.

Niestety, wraz ze wzrostem liczby klientów bankowości elektronicznej, a – co za tym idzie – ze wzrostem liczby realizowanych transakcji oraz zaangażowanych kwot, wzrasta zagrożenie ze strony grup przestępczych. Rozwój technologiczny, nowe narzędzia informatyczne, a także coraz większa łatwość ich stosowania idą w parze z rosnącymi umiejętnościami i atakami cyberprzestępców. Zagrożenia ciągle ewoluują, trzeba zatem umieć się przed nimi bronić[1].

Niniejsze opracowanie podejmuje problematykę takich właśnie zagrożeń, jego celem jest wskazanie głównych zagrożeń występujących w poszczególnych obszarach bankowości elektronicznej oraz odpowiedź na pytanie, jakie czynniki wpływają na wzrost ryzyka popełnienia przestępstw związanych z płatnościami elektronicznymi.

Tak sformułowany cel pozwala na realizację problemów badawczych w obszarze zagrożeń przestępczością. W niniejszym opracowaniu problem badawczy ogranicza się do zagrożeń przestępstwami wobec środków płatniczych, obejmując tylko elektroniczne transakcje. Określenie problemu badawczego pozwala na zbudowanie następujących hipotez badawczych:

– jaki wpływ na bezpieczeństwo transakcji elektronicznych ma sam użytkownik, a w jakim zakresie bezpieczeństwo jego środków płatniczych zapewnia usługodawca (bank)?
– czy organy ścigania posiadają narzędzia umożliwiające rozpoznawanie przestępstw w sieci wobec środków płatniczych i zapobieganie ich popełnianiu?

Jako metodę badawczą przyjęto analizę źródeł literaturowych w omawianym obszarze, tj. w zakresie przestępstw przeciwko środkom płatniczym.

JAK PŁACIMY? FORMY PŁATNOŚCI

Bankowość elektroniczna może być postrzegana jako zjawisko współczesnego świata, które oznacza specyficzny sposób prowadzenia działalności bankowej w ramach społeczeństwa informacyjnego. Stanowi zatem element elektronicznej gospodarki globalnej, której cechą charakterystyczną jest wymiana

dóbr i usług na odległość, z wykorzystaniem elektronicznych środków komunikacji. Oznacza to szybki i niemal nieograniczony geograficznie czy też czasowo dostęp do usług bankowych. Wykorzystanie nowoczesnych technologii pozwala zarówno na świadczenie przez banki nowych usług, jak i na przeniesienie tradycyjnych produktów do elektronicznych kanałów dystrybucji. Skutkuje to umożliwieniem klientom szybkiego dostępu do własnych środków zgromadzonych na rachunku bankowym czy też natychmiastowego zlecenia operacji bez konieczności wizyty w oddziale banku.

Aby przeprowadzić analizę ryzyka i zagrożeń w bankowości elektronicznej, konieczne jest zapoznanie się z usługami i kanałami dystrybucji oferowanymi przez instytucje sektora bankowego. W zależności od przyjętych kryteriów można dokonać rozmaitych podziałów i klasyfikacji usług bankowości elektronicznej. Przyjmuje się, że bankowość elektroniczna obejmuje wszelkie elektroniczne kanały dystrybucji usług i produktów bankowych. Zaliczymy zatem do niej płatności z fizycznym wykorzystaniem kart płatniczych i kredytowych, transakcje realizowane w bankomatach, płatności terminalowe POS oraz szeroko pojętą bankowość internetową. Zwłaszcza w przypadku tej ostatniej należy zwrócić uwagę na tempo postępu technologicznego oraz mnogość nowych urządzeń, umożliwiających zdalny dostęp do usług bankowych z wykorzystaniem Internetu. Pod pojęciem bankowość elektroniczna należy zatem rozumieć nie tylko klasyczną e-bankowość, ale również wszelkiego rodzaju usługi mobilne, obsługiwane przez klientów za pośrednictwem aplikacji na telefonach, smartfonach, tabletach, telewizorach itp.[2]

KARTY

Karty płatnicze są potocznie określane jako „plastykowy pieniądz", umożliwiający dokonanie zapłaty za nabywane towary lub świadczone usługi[3]. Jednakże ww. termin ma znaczenie tylko symboliczne, ponieważ w ścisłym rozumieniu karty nie są pieniądzem, lecz jedynie nośnikiem pieniądza bezgotówkowego[4]. Pierwsze karty (w niewielkim stopniu przypominające ich dzisiejszą postać) miały kształt papierowych książeczek, metalowych płytek lub kartoników z wytłoczonymi danymi okaziciela. Dziś karta płatnicza występuje jako płytka wykonana z tworzywa sztucznego PCV. Standardowe wymiary karty zostały określone w 1985 r. przez ISO (International Organization for Standarization). Według tej standaryzacji karty powinny mieć następujące wymiary: wysokość – 53,98 mm, szerokość – 85,6 mm, grubość – 0,76 mm. Każda karta ma nadany numer, w którym pierwsze sześć wytłoczonych lub wydrukowanych cyfr stanowi numer identyfikacyjny wydawcy karty, zwany często także numerem identyfikacyjnym banku[5].

Na karcie znajduje się również wiele elementów służących do identyfikacji okaziciela. Na awersie możemy znaleźć między innymi: cechy systemów, takie jak logo, hologram, numer początkowy, data ważności karty, dane okaziciela, opcjonalnie – zdjęcie. Rewers natomiast to: pasek magnetyczny z naniesionymi danymi o karcie i jej okazicielu, pasek, na którym posiadacz karty składa wzór swojego podpisu, dane wystawcy karty, czyli informacja, czyją własnością jest karta, a także numer telefonu, pod którym uzyska się pomoc od pracowników banku w kwestiach związanych z kartą. Przed wydaniem karty posiadaczowi jest ona personalizowana przez wytłoczenie lub nadruk płaski imienia i nazwiska, numeru karty oraz kodowanie paska magnetycznego. W ten sposób karta jest jednoznacznie powiązana z określoną osobą i rachunkiem bankowym[6]. Karta płatnicza została zdefiniowana w art. 4 Prawa bankowego, który określa ją jako kartę identyfikującą wydawcę i upoważnionego posiadacza, uprawniającą do wypłaty gotówki lub dokonywania zapłaty, a w przypadku karty wydanej przez bank lub instytucję ustawowo upoważnioną do udzielania kredytu – także do dokonywania wypłaty gotówki lub zapłaty z wykorzystaniem kredytu[7].

Karta płatnicza jest to forma płatności bezgotówkowych mająca z punktu widzenia klienta duże zalety: jest niewątpliwie bardzo wygodną formą dokonywania płatności i pozyskiwania środków zgromadzonych na koncie.

Pojedyncza karta posiada najczęściej wiele funkcjonalności – pozwala na wypłatę pieniędzy w bankomacie, dokonanie zapłaty w sklepie czy płatności przez Internet. Zapewnia przy tym duże bezpieczeństwo rozliczeń i mniejsze narażenie na kradzież. Nie wolno jednak zapominać, że bardzo często używanie kart płatniczych zmniejsza hamulce przy wydawaniu pieniędzy[8]. Obecnie polskie banki konkurują ze sobą, emitując różnego rodzaju karty, które różnią się m.in. zasięgiem, sposobem rozliczania transakcji lub liczbą podmiotów biorących udział w rozliczeniach. Biorąc pod uwagę liczbę podmiotów uczestniczących w rozliczeniach za pomocą kart, możemy wyróżnić karty[9]: **dwustronne** – wydawane zazwyczaj przez instytucje niebankowe typu biura podróży, linie lotnicze, duże domy towarowe i akceptowane jedynie przez ich emitenta, **trójstronne** – ich cechą charakterystyczną jest to, że w transakcjach nimi dokonywanych uczestniczą trzy osoby, a mianowicie: emitent, przedsiębiorstwo, które wyraziło zgodę na to, aby można w nim było dokonywać płatności taką kartą, oraz posiadacz karty, **czterostronne** – w przypadku tych kart oprócz podmiotów wymienionych powyżej, w rozliczeniu transakcji bierze również udział właściciel systemu, w którym emitowana jest dana karta. System czterostronny jest obecnie najbardziej popularny w Polsce i na świecie.

Karty dzielimy też ze względu na **nośnik informacji** zapisanych na nich elektronicznie[10]. Zgodnie z tym podziałem można wyodrębnić karty mikroprocesorowe i magnetyczne. Cechą wyróżniającą **kart mikroprocesowych**, potocznie znanych jako „chipowe", jest możliwość przechowywania dużej ilości danych, zdolność do przetwarzania danych i przede wszystkim nieporównywalnie skuteczniejszy od innych poziom zabezpieczeń, o których będzie mowa dalej. Istnienie mikroprocesora w układzie scalonym karty decyduje o funkcjonalności, a przez to i przeznaczeniu karty. Karta z mikroprocesorem, nadal najczęściej 8-bitowym, jest de facto mikrokomputerem. Typowe wartości pamięci karty to: 64 KB pamięci ROM przeznaczonej na system operacyjny, 8 KB RAM i do 2–16 KB pamięci EEPROM, pełniącej rolę twardego dysku. W części rozwiązań, w których wymaga się dużej ilości obliczeń kryptograficznych, kartę wyposaża się dodatkowo w koprocesor kryptograficzny. Ze względu na sposób komunikacji karty ze środowiskiem zewnętrznym, karty dzieli się na karty **stykowe** i **bezstykowe**. Karty stykowe wymagają bezpośredniego

kontaktu z czytnikiem w celu odczytania jej zawartości. Karty bezstykowe posiadają wbudowaną antenę, umożliwiającą bezprzewodową transmisję danych na niewielkie odległości (do kilku centymetrów). Karty bezstykowe znajdują zastosowanie przede wszystkim w transporcie miejskim i systemach kontroli dostępu. Istnieją też karty dualne, w których w tym samym kawałku tworzywa zatapia się układ stykowy i bezstykowy lub jeden układ stykowo-bezstykowy. **Karty magnetyczne** są obecnie jednym z najbardziej rozpowszechnionych nośników informacji. Ich podstawowym elementem jest występująca w postaci paska magnetycznego pamięć. Umożliwia ona zapis informacji, które mogą być następnie odczytywane za pomocą czytników kart magnetycznych. Dzięki takiej możliwości karty te znajdują szerokie zastosowanie w różnorodnych systemach, np. kontroli dostępu, rejestracji czasu pracy, systemach lojalnościowych, a także jako karty płatnicze[11].

Kolejnym kryterium podziału kart jest **funkcjonalność**[12]. Według niego karty dzielą się na: płatnicze, bankomatowe, identyfikacyjne i wstępnie opłacone. **Karty płatnicze** (ang. *payment card*) umożliwiają regulowanie płatności w sposób bezgotówkowy w punktach handlowo-usługowych, telefonicznie lub przez Internet. Według międzynarodowego standardu ISO obecnie funkcjonujące karty płatnicze muszą być wykonane z tworzywa sztucznego. Karty płatnicze są wygodne dla klientów, którzy nie muszą nosić ze sobą gotówki, ale także dla sprzedawców, ponieważ, jak wykazały badania, klienci płacący kartami, wydają dużo więcej pieniędzy niż ci płacący gotówką. **Karty bankomatowe** (ATM card, cash card) służą wyłącznie do dokonywania wypłat gotówki oraz innych transakcji, które możliwe są do wykonania z użyciem bankomatu, np. sprawdzenia stanu rachunku, wydrukowania historii transakcji, zmiany kodu PIN czy dostępu do funkcji depozytowych w bankomacie. Karta bankomatowa nie posiada żadnych funkcji płatniczych, nie można zatem z jej wykorzystaniem wykonać transakcji bezgotówkowej – nawet jeżeli bankomat udostępnia możliwość wykonania takiej transakcji, np. doładowania konta telefonu komórkowego. Ponieważ funkcjonalność kart bankomatowych jest bardzo ograniczona, większość banków nie decyduje się na ich wydawanie. W zamian banki wydają karty płatnicze, które jednocześnie wyposażone są w funkcje karty bankomatowej. Karty bankomatowe mogą być wydane jako karty lokalne (czyli akceptowane wyłącznie przez określoną sieć bankomatów jednego lub kilku współpracujących ze sobą banków) bądź mogą być wydane w ramach jednego z międzynarodowych systemów kart bankomatowych (np. PLUS lub Cirrus), wówczas akceptowane są przez wszystkie bankomaty na świecie oznaczone symbolem danego systemu. **Karty identyfikacyjne** są szeroko stosowane w naszym codziennym życiu, np. jako karty kontroli dostępu do określonych budynków czy pomieszczeń, karty biblioteczne czy karty stałego klienta – ich zastosowanie można podawać niemalże w nieskończoność. Posiadają często również różne dodatkowe funkcje, np. rabatowe. Podstawowym celem kart identyfikacyjnych jest szybka identyfikacja jej posiadacza, dlatego jest na nich numer, zapisany w sposób umożliwiający jego elektroniczne odczytanie (poprzez zapis w postaci kodu kreskowego bądź zakodowanie na pasku magnetycznym lub mikroprocesorze). Karta identyfikacyjna może również posiadać kod PIN (bądź inny sposób weryfikacji, oparty np. na metodach biometrycznych), dzięki czemu jej zastosowanie umożliwia rezygnację z innych metod sprawdzenia tożsamości posiadacza takiej karty. Dodatkowo na karcie identyfikacyjnej można umieścić także zdjęcie jej posiadacza oraz wzór jego podpisu. **Karty wstępnie opłacone**, przedpłacone, wstępnie ładowane (prepaid card, preloaded card), to karty wydawane w dwóch podstawowych typach: jako karty z oddzielnym kontem technicznym, który można wielokrotnie zasilać, oraz karty z określonym nominałem. Karty z możliwością doładowywania są wykorzystywane przez firmy i instytucje do przekazywania środków pieniężnych, np. do wypłacania różnego typu świadczeń, takich jak: zasiłki socjalne, stypendia, wynagrodzenia dla pracowników sezonowych czy pracowników nieposiadających rachunku bankowego; są również stosowane w programach nagradzania pracowników czy w programach lojalnościowych, do wypłat nagród pieniężnych w programach promocyjnych czy do rozliczania delegacji pracowników. Klienci indywidualni używają kart przedpłaconych jako formy wypłaty kieszonkowego dla młodzieży, do bezpiecznych transakcji w Internecie czy też jako wygodnego sposobu przekazania określonej kwoty jako podarunku z możliwością łatwego doładowania rachunku karty przelewem lub gotówką[13].

Ze względu na sposób rozliczenia transakcji kart, dzielimy je na[14]: debetowe, obciążające i wstępnie opłacone.

Karty debetowe (ang. *debit card*) funkcjonują na zasadzie rozliczenia transakcji wykonanej z użyciem karty natychmiast po otrzymaniu przez bank informacji o jej przeprowadzeniu.

Oznacza to, że rachunek posiadacza karty, który wykonał transakcję z użyciem karty debetowej, zostanie obciążony przez bank natychmiast, gdy tylko informacja o transakcji dotrze do banku. Okres ten zależy jednak od wielu czynników, np. od tego, gdzie była wykonana transakcja, od sposobu jej rozliczania oraz od systemu informatyczno-księgowego stosowanego przez bank. Okres ten może wynosić zatem od niemalże kilku sekund od przeprowadzenia transakcji aż do kilku lub nawet kilkunastu dni.

Karty obciążające umożliwiają posiadaczowi zaciągnięcie u emitenta karty kredytu kupieckiego, czyli odroczenia terminu płatności za nabyte towary i usługi. Uiszczenie należności następuje na koniec okresu rozliczeniowego na podstawie specjalnego zestawienia wydatków.

Karta obciążeniowa posiada zbliżone zasady funkcjonowania do karty kredytowej. Może posiadać określony limit wydatków, bank może ją również wydać bez górnego limitu wydatków (pod warunkiem, iż posiadacz terminowo reguluje wszelkie swoje zobowiązania). Raz w miesiącu bank wysyła zestawienie transakcji wykonanych z użyciem karty. Posiadacz karty zobowiązany jest do spłaty całości zadłużenia (nie można spłacić tylko części) w określonym czasie, np. w ciągu dwóch tygodni od daty otrzymania zestawienia. Posiadacz karty może w ciągu miesiąca wykonywać transakcje do wysokości limitu (niezależnie od kwoty, która znajduje się na jego rachunku). Określonego dnia bank sumuje wszystkie transakcje wykonane z użyciem karty i samodzielnie obciąża kwotą transakcji rachunek posiadacza karty.

Karty kredytowe umożliwiają posiadaczowi karty dokonywanie płatności bezgotówkowych na podstawie umowy kredytu bez konieczności posiadania bieżących środków na rachunku bankowym. Zaciągnięty kredyt spłaca się na zasadach ustalonych wcześniej przez bank wydający kartę.

Posiadacz karty może np. spłacić tylko część zaciągniętego kredytu, ale wtedy bank pobiera odsetki od niespłaconej kwoty. Bank ustala limit kredytowy, do którego wysokości posiadacz karty może dokonywać płatności w punktach handlowo-usługowych, dokonywać płatności zdalnych (przez telefon czy Internet), podejmować gotówkę z bankomatu. Każda z tych czynności rozliczana jest przez bank inaczej, w zależności od jej klasyfikacji, i skutkuje np. różnym oprocentowaniem transakcji gotówkowej (wypłata z bankomatu) i bezgotówkowej (płatność kartą w POS). Wydanie karty jest uzależnione od dochodów konsumenta i oparte jest na analizie zdolności kredytowej (jak przy zaciąganiu kredytu). Często nie wymaga się posiadania przez klienta rachunku oszczędnościowo-rozliczeniowego w danym banku. Karty wstępnie opłacone są powszechnie stosowane w życiu codziennym. Każdy z nas z pewnością posiada niejedną taką kartę – są one bowiem wykorzystywane masowo jako karty telefoniczne, karty parkingowe, karty z biletami komunikacji czy karty do telefonów komórkowych.

Systemy kart płatniczych to organizacje wydawców kart płatniczych, użyczające ich emitentom (najczęściej bankom) prawa do używania znaku tej organizacji. Wspomniany system zapewnia honorowanie swoich kart płatniczych w sieci punktów handlowo-usługowych oznaczonych znakiem organizacji oraz nadzór nad rozliczeniami i sposobem emisji[15].

Pierwsze karty płatnicze zaczęły być wydawane przez banki w Stanach Zjednoczonych pod koniec lat 40. Były to karty o zasięgu lokalnym, które miały charakter kredytowych. Pierwszą kartę o zasięgu ponadstanowym wydał Franklin National Bank z Nowego Jorku w roku 1951. Równocześnie, oprócz kart wydawanych przez banki, rozpoczęto wydawanie kart o charakterze klubowo-podróżniczym, powszechnie nazywane T&E (typu „Travel And Entertainment"). Pierwszą kartę tego typu wydał działający do dziś Diners Club. W 1959 r. wydawanie karty T&E rozpoczął American Express. Międzynarodowy zasięg osiągnęła również karta klubowa organizacji Carte Blanche wchłoniętej przez Diners Club. Poza wydawanymi lokalnie kartami banki zaczęły wydawać karty o zasięgu krajowym, a później międzynarodowym. Tak właśnie powstały w latach 60. dwa duże systemy zajmujące się emisją, obsługą, rozliczeniem i rozwojem kart, znane dziś jako VISA i MasterCard[16]. Do największych funkcjonujących obecnie systemów kart płatniczych zaliczają się: VISA International, MasterCard/EuroCard/Access, JCB (Japanese Credit Bureau), American Express, Europay International/Diners Club.

BANKOMATY

Bankomaty to samoobsługowe urządzenia, które są wyposażone w czytniki paska magnetycznego/mikroprocesora i umożliwiają przeprowadzenie operacji bankowych z użyciem kart płatniczych. Wykorzystywane są przede wszystkim do wypłaty pieniędzy, choć dają również możliwość wykonywania innych operacji, jak np. wpłaty pieniędzy na rachunek w dowolnym banku, przelewów środków na inny rachunek, otwierania lub likwidowania zleceń stałych, zmian terminów i kwot zleceń stałych, otwierania lub likwidowania lokat, sprawdzania stanów konta, załadowania kart telefonii komórkowej itp.[17]

Bankomaty można sklasyfikować według różnych kryteriów. Ze względu na funkcję dzielimy je na: **CD – Cash Dyspenser – bankomat jednofunkcyjny** służący tylko i wyłącznie do wypłaty gotówki; **ATM – Automated Teller Machine – bankomat wielofunkcyjny**, który służy zarówno do wypłat pieniędzy z bankomatu, jak i do wykonywania przelewów, sprawdzania stanu konta, prześledzenia historii dokonywanych operacji itp.; **Cash Recycler** – to złożona maszyna, która obsługuje kilka prostych, a zarazem ważnych zadań – przyjmuje, wydaje oraz bezpiecznie przechowuje gotówkę, utrzymuje uporządkowaną księgowość gotówki w kasie i automatyzuje cykl gotówkowy. Według miejsca lokalizacji wyróżniamy bankomaty: wewnętrzne – usytuowane wewnątrz pomieszczeń, np. banków; przyścienne – które posiadają panel operacyjny (umożliwiający dokonywanie transakcji – monitor, klawiatura) na zewnątrz budynku, zaś ich pozostała część znajduje się w banku; zewnętrzne – usytuowane poza budynkiem banku, często jako urządzenia wolno stojące; mobilne bankomaty – odpowiednio przystosowane samochody ustawione w pobliżu banku, w których są zainstalowane bankomaty. Przez aplikację w telefonie klient kontaktuje się z takim pojazdem, po czym ten specjalny samochód przyjeżdża w wyznaczone miejsce, pozwalając na wypłatę bądź wpłatę gotówki. Według trybu komunikacji z bankiem podział kształtuje się następująco: bankomaty działające w systemie offline, które nie są bezpośrednio połączone z bankami i nie mogą dokonywać autoryzacji bezpośrednio po zawarciu transakcji; autoryzacja dokonywana jest na podstawie limitów wypłat z bankomatu; limity wypłat wynikają z tego, że bankomat „nie wie", ile klient posiada pieniędzy na koncie, bo bankomat nie jest podpięty do bazy danych; większość banków rozpoczęła instalację bankomatów pracujących w trybie offline, a wybór ten był głównie podyktowany względami ekonomicznymi oraz ówczesnymi możliwościami technicznymi banków; bankomaty działające w systemie online – to takie, w których wypłata gotówki powoduje natychmiastowe przekazanie informacji do banku, w którym znajduje się konto klienta; w systemie tym bankomat po otrzymaniu od klienta dyspozycji wypłaty gotówki dokonuje autoryzacji karty, po czym przesyła dane o dokonanej transakcji do banku wydawcy karty[18].

Obecnie poza wypłatami gotówki bankomaty umożliwiają również m.in.: wpłaty gotówki, sprawdzanie bieżącego stanu rachunku klienta, wydruk historii rachunków, zmianę numeru PIN karty, możliwość zapoznania się z informacjami i ogłoszeniami banku, przyjmowanie gotówki w depozyt, obsługę czeków podróżnych itp. Podstawowe elementy składowe bankomatu to: klawiatura, okienko wprowadzania karty, monitor, oświetlenie, klawisze funkcyjne, sejf, logo banku, okienko drukarki, wskaźnik świetlny miejsca wprowadzania karty, okienko dyspensera. Pierwszy bankomat na świecie został uruchomiony 1964 r. przez First Pennsylvania Bank w Stanach Zjednoczonych. Od tego czasu bankomaty bardzo szybko rozpowszechniły się, a ich liczba stale wzrastała (w 2001 r. na świecie było ponad 800 tys. bankomatów). Sieci bankomatów mogą być prywatne lub współdzielone, czyli stanowią wów-

czas wspólne przedsięwzięcie wielu instytucji finansowych, dla których są dostępne, i wspólnie ponoszą koszty, a klienci mają łatwiejszy dostęp do większej liczby urządzeń[19]. W Polsce pierwszy bankomat został zainstalowany przez Bank Pekao SA w 1990 r. Od lat dziewięćdziesiątych XX w. rozpoczęła się w Polsce konkurencja banków w zakresie wydawanych kart płatniczych i zainstalowanych bankomatów. Obecnie mają je już wszystkie banki komercyjne oraz większość banków spółdzielczych. Liczba bankomatów w kraju dynamicznie wzrastała. W szczególności szybki przyrost następował w okresie do 2001 r., natomiast w kolejnych latach tempo wzrostu nieco osłabło, zaś od 2008 r. przyrost roczny bankomatów wynosił ponad 1000 sztuk. Spośród banków na pierwszym miejscu pod względem posiadanych bankomatów znajduje się największy bank detaliczny – PKO BP SA[20], a spośród operatorów komercyjnych – Euronet SA.

Pomimo szybkiego tempa wzrostu nadal wyprzedza nas pod względem liczby bankomatów przypadającej na jeden milion mieszkańców większość krajów UE. O ile w Polsce przypadało na jeden milion mieszkańców 416 bankomatów, o tyle średnia UE wynosi 867, zaś w wielu krajach, takich jak: Belgia, Niemcy, Hiszpania, Portugalia, Austria czy Wielka Brytania, wskaźnik ten przekracza 1000. Za nami uplasowała się jedynie Szwecja i Czechy. Niemniej Polska jest pierwszym krajem w Europie, który wprowadza bankomaty z identyfikacją biometryczną. Bankomaty te będą wyposażone w czytniki rozpoznające układ naczyń krwionośnych w palcu klienta bankowego[21].

BANKOWOŚĆ INTERNETOWA I MOBILNA

Bankowość elektroniczna (ang. *e-banking*) to forma usług oferowanych przez banki, polegająca na umożliwieniu dostępu do rachunku za pomocą urządzenia elektronicznego: komputera, bankomatu, terminalu POS, telefonu (zwłaszcza telefonu komórkowego) i linii telekomunikacyjnych, w tym Internetu. Usługi bankowości elektronicznej są także określane jako telebanking (bankowość zdalna). Zależnie od wykorzystanych rozwiązań umożliwia wykonywanie operacji pasywnych (np. sprawdzanie salda i historii rachunku) oraz aktywnych (np. dokonanie polecenia przelewu, założenie lokaty terminowej). Bankowość elektroniczna jest kluczowym elementem bankowości transakcyjnej[22]. Jest rozumiana jako forma komunikacji klienta z bankiem i zarazem świadczenia usług bankowych z wykorzystaniem elektronicznych urządzeń, takich jak komputer (home/corporate banking, Internet banking – e-banking), telefon, elektroniczne terminale do akceptowania kart płatniczych czy terminale multimedialne[23].

Bankowość elektroniczna ma kilka form nazywanych potocznie kanałami. Część z nich jest wygaszana ze względu na postęp technologiczny oraz wypieranie/zastępowanie przez inne usługi/kanały. **Home banking** to rozwiązanie umożliwiające obsługę rachunków bankowych bez konieczności wychodzenia z domu. Obsługa rachunku bankowego odbywa się z użyciem publicznej sieci telefonicznej, telefonii komórkowej lub innego łącza dostępowego oraz komputera wyposażonego w odpowiednie oprogramowanie. Bezpieczeństwo systemu zapewniają m.in. generowane hasła, a transmitowane dane są kodowane. Wadą home bankingu jest to, że dostęp do konta jest możliwy tylko z komputera, na którym jest zainstalowany odpowiedni program. Bankowość internetowa to komunikacja z bankiem za pośrednictwem Internetu. Witryna internetowa banku umożliwia klientom dokonywanie online różnorodnych operacji na ich rachunkach. Klient banku internetowego powinien mieć dostęp do komputera z zainstalowaną przeglądarką stron www podłączonego do sieci Internet. Kluczową ideą bankowości internetowej jest przede wszystkim wirtualna obsługa klienta, tj. włączenie klienta jako fizycznego użytkownika do skomputeryzowanego systemu bankowego. Istotą jej jest zaś możliwość korzystania z usług bankowych niezależnie od czasu i miejsca. Jest to aktualnie najpopularniejsza forma udostępniania usług bankowych swoim klientom.

Bankowość telefoniczna i mobilna – usługi bankowe dostępne za pośrednictwem telefonu nazywamy bankowością telefoniczną lub phone bankingiem. Usługi te, dostępne dzięki urządzeniom przenośnym, głównie telefonom komórkowym, określamy jako bankowość mobilną lub mobile banking. Operacje bankowe przez telefon mogą być realizowane na kilka sposobów: poprzez kontakt z operatorem (call center) lub automatyczny serwis telefoniczny IVR oraz z użyciem telefonu komórkowego za pomocą SMS lub technologii WAP. O ile kontakt telefoniczny z operatorem lub IVR (Interactive Voice Response) nadal jest dostępny w większości działających na polskim rynku banków, o tyle technologia WAP jest zastępowana przez usługi mobilne wykorzystujące dedykowane aplikacje, uruchamiane z poziomu telefonu komórkowego, co spowodowane jest głównie ułatwionym dostępem do Internetu mobilnego oraz smartfonów. Sam zakres usług pozostaje zbliżony. Operacje wykonywane za pomocą bankowości telefonicznej możemy podzielić na pasywne i aktywne. Pasywne to te, w których klient odbiera jedynie informacje dotyczące rachunku. Najprostszą i najczęściej wykonywaną operacją pasywną jest sprawdzenie salda rachunku. Inne, dostępne w większości serwisów telefonicznych, usługi to sprawdzanie historii rachunku bądź uzyskiwanie informacji o aktualnych stopach oprocentowania lub kursach walut. Usługi aktywne bankowości telefonicznej to takie, które powodują zmianę salda i historii rachunku. Do typowych operacji aktywnych zaliczyć możemy przelewy oraz dyspozycje dotyczące lokat terminowych. Usługa WAP oraz bankowość mobilna umożliwia dostęp do rachunku bankowego poprzez telefon komórkowy. Jest odmianą bankowości internetowej, która pozwala na korzystanie z usług bankowych za pośrednictwem telefonu bezprzewodowego. W ramach usług możliwe są m.in. następujące operacje bankowe: dostęp do informacji o saldzie rachunku, uzyskanie informacji o obrotach na rachunku, weryfikacja listy odbiorców dla przelewów, wgląd do historii operacji, wykonanie przelewu na obce rachunki, definiowanie zlecenia stałego, sporządzenie listy rachunków, na które ma być zrealizowany przelew, dokonanie przelewu z przyszłą datą realizacji, anulowanie przelewu, realizacja przelewu na rachunki ZUS, zakładanie i zrywanie lokat terminowych, zmiana hasła dostępu.

Pierwszym bankiem wykorzystującym Internet do świadczenia usług bankowych był kalifornijski Bank Wells Fargo, zaś wirtualnym – amerykański Security First Network Bank (SFNB), który powstał w 1995 r. w Stanach Zjednoczonych[24].

Bankowość internetowa w Polsce ma dość krótką historię. Jej początek datuje się na 14 października 1998 r. W tym dniu

Powszechny Bank Gospodarczy SA w Łodzi oficjalnie uruchomił internetowy oddział dla klientów detalicznych i małych przedsiębiorstw. Od tego momentu, w ciągu niespełna dwudziestu lat, bankowość internetowa przeszła ogromną ewolucję, co dokumentują odpowiednie statystyki. O ile na koniec 2000 r. zaledwie osiem banków udostępniało usługi bankowe przez Internet, o tyle na początku 2016 r. wśród 37 banków działających w formie spółki akcyjnej nie było ani jednego, który nie korzystałby tej formy dystrybucji usług. Potwierdzeniem ogromnej dynamiki rozwoju bankowości internetowej w segmencie klientów detalicznych jest przyrost liczby klientów aktywnie z niej korzystających, tj. logujących się na koncie przynajmniej raz w miesiącu. Według danych Związku Banków Polskich ich liczba wzrosła w ciągu 10 lat o 237%[25].

Bankowość internetowa przeszła zmiany nie tylko o charakterze ilościowym, ale także jakościowym. W pierwszej fazie interakcja pomiędzy bankiem i klientem była oparta na stronie www z okresowo aktualizowaną zawartością informacyjną, ale o bardzo słabej interaktywności ze względu na brak możliwości wykonania operacji bankowych. Strona internetowa banku była więc początkowo wykorzystywana jako źródło informacji o jego ofercie i działalności oraz dostarczała informacji teleadresowych. W drugiej fazie rozwoju bankowości internetowej wprowadzona została ograniczona forma interakcji z klientem, poprzez udostępnienie różnego rodzaju kalkulatorów, formularzy dostępnych online i aplikacji umożliwiających sprawdzanie stanu konta. Wykonywanie poprzez serwis www zarówno pasywnych operacji bankowych, czyli niezmieniających salda, jak i operacji dostępnych w oddziałach stało się możliwe dopiero w fazie trzeciej, nie bez przyczyny określanej jako „prawdziwa bankowość internetowa". Wpisując unikatowy login i hasło, klient banku uzyskuje dostęp do indywidualnego zbioru stron internetowych powiązanych tematycznie i umieszczonych na serwerze banku, czyli serwisu transakcyjnego. Immamentną cechą tego serwisu są wbudowane w niego aplikacje internetowe postrzegane przez użytkowników jako funkcje serwisu www, które umożliwiają realizację operacji bankowych. Charakterystyką czwartej i do tej pory ostatniej wyróżnionej fazy rozwoju bankowości internetowej jest strategiczne wykorzystanie Internetu przez banki. Upowszechnienie internetowego kanału dystrybucji usług bankowych spowodowało, że banki zaczęły aktywnie wykorzystywać informacje o zachowaniu klientów, w tym analizować ich zyskowność i dostosowywać ofertę do cech poszczególnych segmentów. Oprócz usług bankowych poprzez serwis transakcyjny stały się dostępne także inne produkty finansowe, na przykład ubezpieczenia, fundusze inwestycyjne, co doprowadziło do jego przekształcenia w portal finansowy[26].

Lista usług udostępnianych przez banki poprzez bankowość internetową stale wzrasta. Podstawowymi i najczęściej wykorzystywanymi przez użytkowników (klientów) są następujące operacje: sprawdzanie salda rachunku, przeglądanie historii operacji, wykonywanie przelewów jednorazowych wewnętrznych i zewnętrznych (w tym zagranicznych), przelewy do ZUS, definiowanie przelewów stałych, dokonywanie płatności w sklepach internetowych z ROR, zakładanie i zrywanie lokat terminowych, składanie wniosku o kredyt/kartę kredytową, ustanowienie zlecenia stałego, zamawianie kart bankowych i czeków, usługi maklerskie, ustanowienie pełnomocnictwa.

Jednym z kluczowych elementów bankowości internetowej są jego zabezpieczenia. Można je podzielić na dwa obszary: zabezpieczenie połączenia między komputerem/terminalem klienta (zabezpieczenie sesji) oraz autoryzacja zleceń/operacji klienta.

Pierwsza grupa zabezpieczeń zawiera w sobie wszelkie zasady dotyczące logowania, tj. wymogi dotyczące loginu i hasła, za pomocą których klient łączy się z serwisem transakcyjnym, oraz zabezpieczenia samych stron internetowych, jakie są udostępniane z serwera banku. Jeśli chodzi o sam mechanizm logowania się, banki stosują różne rozwiązania, od wprowadzania samego loginu i pełnego hasła, poprzez kombinację login oraz pojedyncze – wskazane losowo – litery z hasła, aż po kombinację loginu, hasła i pytania kontrolnego lub/i tzw. Captcha – Completely Automated Public Turing test to tell Computers and Humans Apart – rodzaj techniki stosowanej jako zabezpieczenie na stronach www, celem której jest dopuszczenie do przesłania danych tylko wypełnionych przez człowieka. Celem jest upewnienie się, iż samo logowanie się do serwisu transakcyjnego, choćby celem jedynie wyświetlenia informacji o saldzie, jest zainicjowane przez osobę do tego upoważnioną.

Zabezpieczenia związane z bezpiecznym połączeniem z bankiem realizowane są na poziomie aplikacyjnym. Ich celem jest zadbanie, aby wymiana informacji między serwerem a klientem nie mogła zostać „podsłuchana", tj. widoczna i czytelna dla osób trzecich. Są one konieczne, jako że samo połączenie odbywa się poprzez Internet, a nie osobne/wydzielone łącze. Najpopularniejszym sposobem zabezpieczania sesji jest szyfrowanie połączenia z wykorzystaniem protokołu HTTPS (ang. Hyper Text Transfer Protocol Secure). Za implementację protokołu odpowiedzialny jest dostawca usługi/strony, czyli bank.

Druga grupa zabezpieczeń stosowanych w bankowości internetowej dotyczy mechanizmu autoryzacji operacji, jakie poprzez serwis transakcyjny zleca użytkownik. Najczęściej stosowany jest model podwójnego uwierzytelniania, tj. poza koniecznością prawidłowego zalogowania się do serwisu, wypełnienia stosownego zlecenia w formularzu www, konieczne jest podanie hasła jednorazowego, celem potwierdzenia dyspozycji. Ma to na celu uniemożliwienie wykonania operacji bankowych osobom trzecim, które weszłyby w posiadanie zestawu danych (np. loginu i hasła). Same hasła jednorazowe mogą być dostarczane do klienta na kilka sposobów. Do niedawna najpopularniejszym były listy haseł jednorazowych. Były to papierowe arkusze zawierające ponumerowane sekwencje znaków, np. cyfr, drukowane najczęściej w formie kart-zdrapek. Użytkownik przy każdorazowym zlecaniu transakcji w serwisie bankowym proszony był o podanie hasła/sekwencji znaków znajdujących się na wspomnianej karcie. Każde hasło mogło być wykorzystane tylko raz. Po wyczerpaniu całej listy kodów/haseł klient mógł zamówić kolejną, która dostarczana była pocztą na wskazany przez niego adres. Rozwiązanie to jest wypierane przez rozwiązania elektroniczne. Aktualnie najpopularniejszym są hasła jednorazowe dostarczane w formie wiadomości SMS na wskazany przez klienta numer telefonu komórkowego. Sam mechanizm autoryzacji w serwisie www jest zbliżony – klient proszony jest o podanie hasła, jakie otrzymał na swój telefon. Alternatywnym rozwiązaniem są hasła generowane przez tzw. tokeny, czyli

generatory kodów jednorazowych. Ich działanie polega na generowaniu ciągów cyfr za pomocą funkcji jednokierunkowej wykorzystującej dwa parametry – jeden stały dla konkretnego egzemplarza urządzenia, drugi zmienny – wprowadzany za pomocą klawiatury, wczytywany z ekranu monitora bądź generowany na podstawie czasu. Tokeny występują w formie generatorów haseł jednorazowych (One Time Password – OTP) oraz w formie bardziej zaawansowanej wyzwanie-odpowiedź (challenge-response). Tokeny OTP wyświetlają kod zmieniany zwykle co 60 sekund i nie posiadają przycisku lub posiadają tylko jeden przycisk wywołujący wyświetlenie kodu, natomiast tokeny challenge-response przypominają niewielkie kalkulatory i zazwyczaj są chronione kodem PIN. Rozwinięciem tokenów challenge-response są czytniki kart obliczające kody na podstawie klucza zapisanego na mikroprocesorze karty płatniczej. Najnowszym rozwiązaniem są jednak tokeny OTP oraz challenge-response wbudowane w kartę formatu karty płatniczej (może to być zarówno karta Visa lub Mastercard z wbudowanym tokenem, jak i oddzielny token służący jedynie do uwierzytelniania). Ze względu na stosunkowo wysoką cenę tokenów banki częściej stosują karty kodów jednorazowych lub hasła SMS. Urządzenie może też być zastąpione przez telefon komórkowy używający dedykowanej aplikacji spełniającej funkcję generatora haseł.

Bankowość elektroniczna we wszelkich swych formach ciągle ewoluuje. Funkcjonując już od niemal pół wieku, na stałe wpisała się w nasze codzienne życie. Ciężko sobie obecnie wyobrazić brak możliwości dokonywania zakupów przez Internet czy też płatności kartami kredytowymi. Tak intensywna ekspansja wykorzystywania tych kanałów realizacji transakcji pociągnęła za sobą pojawienie się przestępstw skierowanych przeciwko użytkownikom bankowości elektronicznej. Mimo rozlicznych zabezpieczeń wykorzystywanych do zapewnienia bezpieczeństwa transakcji realizowanych za jej pośrednictwem obszar ten charakteryzuje się coraz większą dynamiką wzrostu przestępczości. Wynika to zarówno z rosnącej popularności poszczególnych instrumentów wśród klientów banków, jak i pojawienia się wyspecjalizowanych grup przestępczych, oraz popularyzacji Internetu, umożliwiającego działanie tychże na całym świecie. W kolejnej części opracowania zostanie przedstawiona typologia prawnokarna rodzajów przestępstw w obszarze bankowości elektronicznej, opis stosowanych metod oraz przykłady przestępstw.

RODZAJE PRZESTĘPSTW

Na szczególną uwagę zasługują metody, jakimi posługują się przestępcy, charakterystyka poszczególnych technik z podziałem na kanały bankowości elektronicznej, w których znajdują zastosowanie, oraz kwalifikacje czynów według przepisów kodeksu karnego. Opisy zostały podzielone zgodnie z kanałem bankowości elektronicznej, który jest wykorzystywany dla danego typu przestępstwa. Istnieją techniki wykorzystujące lub wykorzystywane w więcej niż jednym kanale bankowości[27].

Karty płatnicze

Biorąc pod uwagę szerokie zastosowania kart płatniczych, zdefiniowanie przestępczości kartowej jest skomplikowane. Można ją rozumieć jako wszelkiego rodzaju działalność podejmowaną przez osoby nieuprawnione lub uprawnione do użycia karty płatniczej, mającą na celu uzyskanie dostępu do środków finansowych, w oparciu o które funkcjonuje karta, przez osobę nieuprawnioną lub niezgodne z prawem dokonanie transakcji z wykorzystaniem tych środków[28].

Przestępstwa związane z wykorzystaniem kart płatniczych są zróżnicowane i nie istnieje jeden uniwersalny katalog, pozwalający jednoznacznie je usystematyzować. Można je podzielić na trzy główne kategorie: przestępstwa skierowane jedynie na uzyskanie dostępu do środków finansowych posiadacza karty, przestępstwa skierowane na dokonanie nieuprawnionej transakcji w oparciu o te środki, przestępstwa skierowane na uzyskanie dostępu do środków finansowych i jednorazowego dokonania nieuprawnionej transakcji w oparciu o te środki.

Zgodnie z decyzją ramową Rady 2001/413/WSiSW z dnia 28 maja 2001 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi[29] do przestępstw odnoszących się do kart płatniczych, które nakazuje penalizować, są zaliczane: kradzież lub innego rodzaju bezprawne uzyskanie instrumentu płatniczego, podrabianie lub fałszowanie instrumentu płatniczego do użycia go w celu oszustwa, przyjmowanie, otrzymywanie, transportowanie, sprzedaż lub przekazanie innej osobie albo posiadanie ukradzionego, uzyskanego w inny nielegalny sposób, podrobionego lub sfałszowanego instrumentu płatniczego do użycia go w celu dokonania oszustwa, użycie ukradzionego, uzyskanego w inny nielegalny sposób, podrobionego lub sfałszowanego instrumentu płatniczego w celu dokonania oszustwa.

Jako najczęściej popełniane przestępstwa z wykorzystaniem instrumentów płatniczych, do których zaliczamy również karty płatnicze, wymienić możemy[30]: wyłudzenia kart na podstawie wniosku z fałszywymi danymi, posługiwanie się zgubionymi lub skradzionymi kartami przez osoby nieuprawnione, posługiwanie się kartami niedoręczonymi, fałszowanie kart, kopiowanie kart na rachunkach obciążeniowych, nielegalne wykorzystanie numeru karty, wykorzystanie karty zgłoszonej jako utracona, wyłudzenie towarów i usług przez legalnego posiadacza, włamywanie się do systemów informatycznych i telekomunikacyjnych, manipulowanie bankomatami (tzw. skimming), phishing.

Wyłudzenie karty płatniczej jest – analogicznie jak większość tego typu przestępstw – oparte na podaniu nieprawdziwych danych osobowych podczas składania wniosku o wydanie takiej karty, jak również podanie fałszywych danych dotyczących zarobków. Ma to na celu spełnienie minimalnych kryteriów kwalifikujących zdolność kredytową osoby do przyznania takiego produktu bankowego. Po wydaniu takiej karty sprawca dokonuje licznych transakcji bezgotówkowych bez zamiaru uregulowania płatności z bankiem-emitentem karty.

Kolejnym przestępstwem z wykorzystaniem kart, które stanowi również fałszowanie dokumentów, jest kopiowanie kart na dokumentach obciążeniowych. Popełniają je przestępcy we współpracy z nieuczciwymi sprzedawcami. Liczba transakcji, które są aktualnie przetwarzane przez centra autoryzacyjnie, stale i znacząco wzrasta, nie jest zatem możliwe sprawdzanie każdej z nich. Fakt ten wykorzystują przestępcy do wykonywania transakcji kradzionymi kartami płatniczymi. Omijają w ten sposób zabezpieczenie w postaci wymaganego zgodnego podpisu użytkownika karty.

Innym przykładem działalności przestępczej z wykorzystaniem transakcji kartowych, gdzie następuje manipulacja przy

dokumentach obciążeniowych, jest podrabianie potwierdzeń dokonania transakcji. Spotykane jest to głównie w punktach usługowych, w których zwyczajowo dodawane są napiwki. Jeśli klienci pozostawiają to pole puste, może ono zostać dowolnie wypełnione przez nieuczciwego kelnera czy sprzedawcę. Taka transakcja jest następnie wprowadzana do terminala, a klient jest obciążany podwyższoną kwotą. Co prawda istnieje zabezpieczenie w formie ograniczenia wysokości napiwku (20%), niemniej ryzyko nadal istnieje.

Nielegalne używanie numeru karty, czyli dokonywanie zakupów na odległość (przeważnie w Internecie) z wykorzystaniem danych cudzych kart (nazywany zwyczajowo cardingiem), polega na wykorzystaniu przez przestępców danych karty uzyskanych nielegalnie od jej właściciela. Jest to odmiana kradzieży tożsamości. Przestępca może wejść w posiadanie wspomnianych danych poprzez fizyczny kontakt z kartą lub też wykradzenie tych danych np. podczas korzystania z niej przez właściciela do zakupu przez Internet. Możliwe jest również wykorzystanie narzędzi socjotechnicznych w celu nakłonienia użytkownika do przekazania tych danych. Bez względu na sposób uzyskania danych karty, dalsze kroki przestępcy wyglądają podobnie, tj. są one wykorzystane do dokonania zakupów w Internecie. Do niedawna zabezpieczeniem przed tego typu przestępstwem było ograniczenie w wysyłce towaru wyłącznie na adres dostępny w bazie wystawców danej karty. Obecnie większość działających w Internecie sklepów pozwala na pełną dowolność, jeśli chodzi o dane osoby dokonującej płatności, jak i adres odbiorcy towaru. Dodatkowe zabezpieczenie, które jest coraz częściej stosowane, stanowi weryfikacja w systemie bankowym wystawcy karty kodu CVV2/CVC2, który znajduje się na odwrocie karty i nie jest co do zasady przechowywany w żadnych bazach. Ostatnio wprowadzane są również mechanizmy podwójnego uwierzytelniania, tj. hasła jednorazowe dostarczane na telefon komórkowy właściciela karty płatniczej. Usługa ta nie jest jeszcze powszechnie stosowana, ale pozwala na znaczące ograniczenie ryzyka nielegalnego wykorzystania numeru karty płatniczej.

Innym rodzajem przestępstwa z wykorzystaniem karty płatniczej jest skimming. Polega on na przechwyceniu przez przestępców danych z paska magnetycznego karty oraz kodu PIN. Następuje to podczas dokonywania przez użytkownika transakcji w terminalu płatniczym lub w bankomacie. Uzyskane dane wykorzystywane są do wykonania duplikatu karty, którym sprawcy posłużą się następnie do wypłacenia pieniędzy z rachunku posiadacza karty.

Kolejnym przestępstwem popełnianym przez oszustów internetowych jest phishing. Jest to forma wyłudzenia mająca na celu uzyskanie przez sprawcę numeru karty płatniczej wraz z numerem PIN. Wykorzystuje się w tym celu fałszywe wiadomości e-mail, mające udawać korespondencję z banku, w których przesyła się prośbę o jak najszybsze zalogowanie na stronę banku. Wiadomość zawiera najczęściej link mający przenieść na stronę banku. W rzeczywistości strona ta jest fikcyjna i jedynie przypomina stronę internetową banku. Nieświadomy użytkownik podaje login, hasło, numer karty, numer konta, numer PIN i inne dane, które przestępcy mogą później wykorzystać.

Według danych opublikowanych przez NBP liczba oszukańczych operacji dokonanych z użyciem kart płatniczych wynosi ok. 70 tys. rocznie (dane przekazywane są przez banki)[31]. Analizując zaprezentowane dane, można stwierdzić, iż stworzenie jednolitego katalogu przestępstw kartowych jest bardzo trudne. W przypadku tego typu przestępstw celem działania sprawców jest zawsze osiągnięcie korzyści majątkowej, rozumianej jako zwiększenie aktywów lub zmniejszenie pasywów. Korzyścią majątkową jest zarówno korzyść dla siebie, jak i dla innej osoby (art. 115 § 4 kk).

Kradzież karty płatniczej jest jednym z przestępstw związanych z wykorzystaniem karty, która została uzyskana przez sprawcę w sposób nielegalny. Przy tego typu przestępstwach istotną czynnością sprawczą jest fizyczne wejście w posiadanie oryginalnej karty płatniczej stanowiącej własność innej osoby. Niekiedy sprawca uzyskuje również dostęp do kodu PIN (np. jeśli został on zapisany na rewersie karty lub był przechowywany wraz z kartą płatniczą w portfelu) lub do podpisu legalnego posiadacza karty. Szacuje się, że obecnie ta kategoria przestępstw stanowi największy odsetek nielegalnych transakcji spośród dokonywanych za pomocą kart płatniczych.

Najpowszechniejszym obecnie sposobem kradzieży kart płatniczych jest kradzież kieszonkowa. Jeszcze kilka lat temu złodzieje kieszonkowi wyrzucali karty znalezione w skradzionym portfelu. Obecnie karty stają się coraz częściej przedmiotem kradzieży[32]. Po dokonaniu kradzieży karty sprawca nie zmienia danych na niej zawartych, lecz podszywając się pod posiadacza karty, dokonuje transakcji – najczęściej poniżej limitu autoryzacyjnego. Przy dokonywaniu transakcji za pośrednictwem karty kredytowej sprawca musi jeszcze tylko sfałszować podpis na rachunku obciążeniowym według wzoru na pasku karty[33].

Kradzież karty płatniczej w obecnym stanie prawnym, jako przestępstwo, penalizowana jest w art. 287 § 5 kk, zgodnie z którego brzmieniem przepisy dotyczące zaboru w celu przywłaszczenia cudzej rzeczy ruchomej „stosuje się odpowiednio do kradzieży energii lub karty uprawniającej do podjęcia pieniędzy z automatu bankowego".

Kolejnym przestępstwem, którego przedmiotem może być karta płatnicza, jest fałszerstwo. Polega ono generalnie na przerabianiu i podrabianiu samych kart płatniczych, stosowaniu tzw. białego plastiku oraz generowaniu numerów kart. Przestępstwa przerabiania karty płatniczej najczęściej są realizowane poprzez: zmianę tłoczenia numerów kart, zmianę daty ważności karty, zaprasowanie starego numeru karty i wbicie nowego, wycinanie i doklejanie odpowiednich elementów kart, zmiany w pasku przeznaczonym na podpis posiadacza karty.

Podrabianie polega na wyprodukowaniu nowych fałszywych kart z wykorzystaniem kompletu lub części informacji zdobytych z karty autentycznej.

Obecnie brak jest jednoznacznego zakazu fałszowania kart płatniczych. Możliwe jest jego penalizowanie na podstawie wykładni językowej art. 310 § 1 kk, tj. fałszowania pieniędzy i innych środków płatniczych. Zgodnie z obowiązującym orzecznictwem karta płatnicza, jako instrument dostępu do środków pieniężnych na odległość, umożliwiający elektroniczną identyfikację posiadacza niezbędną do dokonania zapłaty, jest „innym środkiem płatniczym" w rozumieniu ww. artykułu.

PRZESTĘPSTWA W OBSZARZE BANKOWOŚCI ELEKTRONICZNEJ

Jednym z najpopularniejszych przestępstw z wykorzystaniem kart płatniczych jest skimming, czyli działanie polegające na nielegalnym skopiowaniu zawartości paska magnetycznego karty płatniczej bez wiedzy jej posiadacza w celu wytworzenia kopii i wykonywania nieuprawnionych płatności za towary i usługi lub wypłat z bankomatów. Skimmingu można dokonać zarówno w placówkach handlowych (terminale płatnicze), jak i bankomatach. Operacja w punkcie handlowo-usługowym polega na tym, że pasek magnetyczny karty płatniczej jest skanowany przez przestępcę za pomocą specjalnych czytników. Dane zeskanowane z karty płatniczej są następnie przez przestępców wykorzystywane do podrabiania danej karty płatniczej lub jej przerabiania. Skimming w bankomacie jest o tyle groźniejszy od dokonywanego w POS, iż sprawca poza danymi zapisanymi na karcie uzyskuje również kod PIN osoby korzystającej z bankomatu.
W celu wejścia w posiadanie danych kart płatniczych przestępcy wykorzystują różne sposoby i różnego rodzaju sprzęt specjalistyczny, np. tzw. skimmery oraz mikrokamery lub fałszywe klawiatury bankomatowe przy transakcjach autoryzowanych (sprawcy uzyskują kody PIN kart), wykorzystują też skimmery do uzyskania danych z karty (kieszonkowcy, włamywacze, w pokojach hotelowych), chipy umieszczone w oryginalnych terminalach POS – do uzyskania kodów PIN kart. Innymi sposobami są: włamania crackerów do serwerów sklepów internetowych z danymi kart tych sklepów, podłączanie do sieci celem uzyskania danych (tzw. tapping), wykorzystanie podmiotów posiadających i gromadzących dane kart płatniczych (akceptanci, banki, centra personalizacyjne kart płatniczych).

Skimming – zwłaszcza bankomatowy – jest wyjątkowo groźnym przestępstwem z wykorzystaniem karty płatniczej. Daje on sprawcy prawie nieograniczony dostęp do środków znajdujących się na powiązanym rachunku. Samo kopiowanie danych trwa zaledwie kilka sekund. Może być wykonane przez osoby pracujące w punkcie handlowo-usługowym niemal na oczach właściciela. Warto zauważyć, że dane odczytane z naszej karty płatniczej mogą być wykorzystane także za granicą, co skutecznie może utrudnić ściganie potencjalnych sprawców.

W tym miejscu warto zaznaczyć, że skimming bankomatowy wymaga odpowiednich przygotowań. Niezbędne jest przygotowanie bankomatu: zainstalowanie nakładki skimmingowej, której zadaniem będzie odczytanie danych z karty, oraz miniaturowej kamery, która ma posłużyć do zarejestrowania wprowadzanego numeru PIN. Opcjonalnie możliwe jest zastosowanie nakładki na klawiaturę bankomatu, która pozwala na zdobycie przez przestępców PIN-u. Każde z zainstalowanych urządzeń posiada swoje źródło zasilania oraz pamięć pozwalającą na zapisanie zebranych informacji. Umożliwia to ich nieprzerwaną pracę do kilkudziesięciu godzin. Po tym czasie urządzenia są demontowane, a informacje kopiowane na komputer, skąd przenosi się je na duplikat karty. Wraz z zapisem wideo wpisywanego numeru PIN pozwalają na bezproblemowe podejmowanie środków z bankomatów. Wystarczy tu zastosowanie tzw. białego plastiku, czyli „czystych" kart pozbawionych grafik nanoszonych przez poszczególne banki-emitentów.

Pozyskiwanie przez sprawcę danych z paska magnetycznego oraz kodu PIN w celu wytworzenia kopii karty płatniczej może być kwalifikowane jako przestępstwo przygotowania do fałszerstwa karty, a więc jako czyn z art. 310 § 4 kk. Jeśli pozyskane dane zostaną naniesione na nośnik, to jest to uznawane za podrabianie karty płatniczej.

Innym typem przestępstw z wykorzystaniem kart płatniczych jest użycie kart niedoręczonych. Polega ono na przejęciu karty płatniczej, zanim zostanie ona dostarczona pocztą do klienta. Sprawca po wejściu w posiadanie karty dokonuje transakcji płatniczych i bankomatowych. Aby wejść w posiadanie cudzej karty, przestępcy usiłują zmienić w banku, w którym prowadzony jest rachunek karty, dotychczasowy adres dostarczenia.
Czyn taki kwalifikowany jest zgodnie z art. 278 § 1 lub 5 kk, art. 275 § 1 kk lub art. 284 § 1 kk. Warto tu zaznaczyć, że posłużenie się kartami płatniczymi niedoręczonymi może być kwalifikowane jako przywłaszczenie tylko wtedy, gdy sprawca wejdzie w jej posiadanie w wyniku błędnego zaadresowania przesyłki, a następnie nie zwróci jej właścicielowi ani bankowi, natomiast zacznie jej używać.

Przestępstwa z wykorzystaniem bankomatów

Jednym z przestępstw należących do grupy przestępstw bankomatowych jest umieszczanie na nośniku informacji (którym jest najczęściej pasek magnetyczny karty płatniczej, ale może być to również mikroprocesor) odpowiedniego programu pozwalającego na wprowadzenie do systemu poprzez bankomat, z użyciem karty bankomatowej, programu – wirusa[34]. Zadaniem takiego programu jest przechwycenie i przesłanie do sprawców danych karty przetwarzanej przez bankomat, jak również numeru PIN. Podczas korzystania z bankomatu, który został zarażony tego typu wirusem, autoryzacja użytkownika inicjuje przechwycenie numeru karty, daty jej ważności oraz unikatowego, trzyznakowego kodu usługi powiązanego z kartą, który określa sposób rozliczania transakcji, a także kodu PIN wpisywanego przez użytkownika. Warto wspomnieć, że współczesne trojany bankomatowe potrafią omijać zabezpieczenia bankomatów polegające na szyfrowaniu transmisji kodów PIN wprowadzanych do bankomatu. Kolejnym krokiem jest odczytanie przez sprawcę informacji poprzez wprowadzenie do bankomatu odpowiednio spreparowanej karty, która pozwala na przejęcie kontroli nad urządzeniem. Skradzione informacje są następnie wyświetlane na ekranie bankomatu lub zapisywane na używanej karcie. Wykrycie tego typu działań jest o tyle skomplikowane, iż brak jest jakiejkolwiek fizycznej ingerencji w urządzenie. Co więcej, najnowsze wersje tego typu trojanów potrafią „wyczyścić" zainfekowany bankomat poprzez skasowanie plików logu i zainfekowanych plików. Potrafią też same się aktualizować, restartować urządzenie lub zmieniać tryb jego pracy. Najczęstszym celem zainfekowania bankomatu takim wirusem jest doprowadzenie do niezależnej wypłaty pieniędzy z bankomatu, np. opróżnienie zasobnika pieniędzy z użyciem jak największych nominałów. Powyższe działanie może być – poza kradzieżą – również zakwalifikowane jako przestępstwo z art. 268 § 2 kk (niszczenie informacji na informatycznym nośniku danych) lub też art. 287 § 1 kk (oszustwo komputerowe).

Innym przestępstwem bankomatowym jest fizyczne oddziaływanie na bankomat, polegające na włamaniu się do zasobów finansowych znajdujących się wewnątrz. Jest to najbardziej prymitywna metoda kradzieży. Sprawcy stosują do tego ciężki sprzęt budowlany lub samochody ciężarowe. Bankomat jest następnie przewożony w ustronne miejsce w celu otwarcia sejfu i kradzieży jego zawartości.
Inną metodą fizycznego oddziaływania na bankomat jest jego wysadzenie. Sprawcy wtłaczają do wnętrza urządzenia łatwopalny gaz i wywołują zapłon.
Istnieją również bardziej wyrafinowane formy fizycznego oddziaływania na bankomat. Przykładem jest tzw. wenezuelski śrubokręt: za pomocą kleju sprawca blokuje klapkę zasłaniającą szufladę, do której przekazywane są z zasobnika banknoty. Następnie oczekuje on na użytkowników, którzy będą chcieli dokonywać wypłat z danego bankomatu. Kiedy po nieudanych próbach dokonania wypłaty gotówki użytkownicy oddalają się, sprawca wydobywa zgromadzone wewnątrz pieniądze za pomocą śrubokręta.
W przypadku przestępstw z fizycznym oddziaływaniem na bankomat kwalifikacja czynu jest jednoznaczna – zgodnie z art. 279 § 1 kk stanowi on kradzież z włamaniem, natomiast metoda „wenezuelskiego śrubokręta" kwalifikowana jest jako kradzież (art. 278 kk).
Innym przestępstwem zaliczanym do grupy bankomatowych jest uzyskanie karty płatniczej za pomocą fałszywego bankomatu. Osoba korzystająca z takiego urządzenia nieświadomie wprowadza swoją kartę do czytnika i wprowadza numer PIN w celu wypłaty określonej kwoty. Fałszywe urządzenie nie wypłaca żądanej sumy pieniędzy, a dodatkowo uniemożliwia odbiór karty i rejestruje wpisany numer PIN. Sprawcy, będąc w posiadaniu skradzionej karty i numeru PIN, mogą zarówno realizować transakcje w prawdziwych bankomatach, jak i dokonywać zakupów.
Szczególnym przypadkiem działania, które ma na celu uzyskanie przez sprawcę karty płatniczej, jest zastosowanie metody „libijskiego oczka". Sprawcy blokują otwór bankomatu za pomocą folii plastikowej, a następnie oczekują w pobliżu na swoją ofiarę. Klient wprowadza do bankomatu kartę, którą bankomat przyjmuje, a następnie wypłaca żądaną kwotę. Nie następuje jednak wydanie karty, którą bankomat zatrzymał w wyniku zastosowanej blokady. W tym momencie do bankomatu podchodzi sprawca oferujący swoją pomoc, próbując zdobyć zaufanie klienta. Celem jest zdobycie numeru PIN, aby sam go wpisał i spróbował odzyskać kartę. Karta nadal pozostaje zablokowana. Sprawca czeka, aż zniechęcony nieudanymi próbami klient oddali się, pozostawiając kartę w bankomacie. Następnie demontuje on blokadę i wchodzi w posiadanie karty wraz z kodem PIN. Metoda ta podlega pod art. 275 § 1 kk (używanie cudzych dokumentów), art. 278 § 1 i 5 kk (kradzież) oraz art. 284 § 1 kk (przywłaszczenie).

Przestępstwa z wykorzystaniem bankowości internetowej

Bankowość internetowa to forma świadczenia usług za pośrednictwem sieci internetowej, z wykorzystaniem standardowego oprogramowania (przeglądarka internetowa) lub oprogramowania dotykowego do komunikacji z bankiem[35]. Oznacza to, że dokonywanie transakcji odbywa się za pomocą urządzeń elektronicznych i łączy telekomunikacyjnych. Same transakcje są realizowane w środowisku wirtualnym, które, co do zasady, zapewnia stronom wysoki stopień anonimowości, a konsekwencją tego jest duży margines możliwości pozyskania przesyłanych podczas transakcji danych przez osoby trzecie. Stąd też bankowość internetowa nie jest wolna od zagrożeń przestępczością.
W powiązaniu z przestępstwami związanymi z wykorzystaniem kart płatniczych, sprawcy popełniają również inne przestępstwa dotykające obszaru bankowości elektronicznej. Jednym z nich jest włamanie się do komputerowych systemów informatycznych i telekomunikacyjnych, mające na celu uzyskanie danych kart płatniczych, tj. ich numerów, kodów PIN itp.
Takie działanie sprawcy wyczerpuje znamiona czynu opisanego w art. 267 § 1 kk – tzw. naruszenia tajemnicy informacji („Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne informatyczne lub inne szczególne zabezpieczenie") zagrożonego karą grzywny, ograniczenia wolności lub pozbawienia wolności do lat 2. Brzmienie wspomnianego artykułu zostało znowelizowane[36] w związku z implementacją do polskiego prawa karnego decyzji ramowej Rady Europejskiej 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[37]. Decyzja ta nakłada na kraje członkowskie Unii Europejskiej zobowiązania do podjęcia kroków mających na celu kryminalizację następujących zachowań: nielegalnego dostępu do systemów informatycznych, nielegalnej ingerencji w system, nielegalnej ingerencji w dane, kierowania, pomagania i podżegania oraz usiłowania w zakresie wyżej wymienionych czynów.
Jednym z najpopularniejszych przestępstw popełnianych w obszarze bankowości internetowej jest tzw. phishing. Jest to metoda oszustwa, w której przestępca podaje się za inną osobę lub instytucję w celu wyłudzenia określonych informacji np. danych logowania, szczegółów karty płatniczej lub nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.
Termin ten powstał w połowie lat 90. na określenie działań crackerów próbujących wykraść konta w serwisie AOL. Atakujący udawał członka zespołu AOL i wysyłał wiadomość do potencjalnej ofiary. Wiadomość zawierała prośbę o ujawnienie hasła, np. dla „zweryfikowania konta" lub „potwierdzenia informacji w rachunku". Gdy ofiara podawała hasło, napastnik uzyskiwał dostęp do konta i wykorzystywał je w przestępczym celu, np. do wysyłania spamu.

Termin phishing jest niekiedy tłumaczony jako password harvesting fishing (łowienie haseł). Inni utrzymują, że termin pochodzi od nazwiska Briana Phisha, który miał być pierwszą osobą stosującą techniki psychologiczne do wykradania numerów kart kredytowych.

Najczęściej sprawcy wykorzystują wiadomości email rozsyłane w dużej liczbie (analogicznie jak spam), próbując nakłonić potencjalne ofiary do odwiedzenia odpowiednio spreparowanej strony internetowej, która ma przypominać stronę danego banku. Treść samej wiadomości najczęściej sugeruje konieczność niezwłocznego dokonania logowania przez użytkownika celem zweryfikowania swoich danych, wstrzymania nieautoryzowanej płatności, potwierdzenia operacji bankowej lub też – paradoksalnie – zabezpieczenia się przed zagrożeniem ze strony przestępców. Znacząca większość odbiorców tego typu

wiadomości nie daje się oszukać. Niemniej aktualne badania wskazują, że skuteczność tej metody oscyluje w okolicach 5%, czyli ponad pięciokrotnie więcej niż średnia odpowiedzi na zwykły spam. Oznacza to, że przy stosunkowo niewielkich nakładach (przygotowanie wiadomości i spreparowanie strony) nadal możliwe jest uzyskanie korzyści majątkowej.
Metoda przestępstwa phishingu występuje w kilku wariantach, ale najczęściej polega na nakłonieniu użytkownika do samodzielnego wpisania poufnych danych na specjalnie spreparowanej stronie internetowej mającej imitować oryginalną stronę instytucji (np. banku internetowego, serwisu aukcyjnego, internetowego systemu płatności etc.), pod którą podszywają się oszuści. Zazwyczaj stosowaną przez phisherów techniką jest wysyłanie spreparowanego listu elektronicznego, zawierającego odnośnik do fałszywej strony internetowej. Aby oszukać odbiorcę i uwiarygodnić przesłaną wiadomość i adres strony, na którą przekierowywana jest ofiara, wykorzystywane są błędy w przeglądarkach lub inne triki. Jeden z nich to **typosquatting**. Polega na rejestrowaniu domen z zastosowaniem prostych błędów literowych, które mogą zostać popełnione przez internautów podczas wpisywania nazwy strony w pasku adresu przeglądarki. Przykładem mogłoby być pominięcie jednej z liter lub wprowadzenie takiej, która sąsiaduje z daną literą na klawiaturze. Inne proste zastosowania tej techniki to: wwwnazwadomeny (bez kropki pomiędzy „www" a nazwą domeny); www-nazwadomeny (kreska pomiędzy „www" a nazwą domeny); nazwadomeny-dowolnanazwa (kreska pomiędzy nazwą oryginalnej domeny a nazwą domeny). Warto dodać, że w przeszłości najpopularniejsze było umieszczanie na „przejętej" przez atakującego domenie katalogu z nazwą domeny, pod którą chciał podszyć się atakujący. Innym sposobem jest **Homoglyph & homograph**. Atak polega na wykorzystaniu podobieństw w wyglądzie danej litery, cyfry bądź znaku, poprzez użycie zestawu innych znaków, m.in. cyfr i liter. Często stosowaną metodą jest używanie tych samych liter z innych języków bądź kodowań. Najprostszą techniką tego typu jest łączenie liter oraz znaków i ich zamiana na inne. Do najpopularniejszych przykładów możemy zaliczyć poniższe (w nawiasie przedstawiono czytelniejszą wersję): **rn** jako m (małe litery R i N jako mała litera M), **cl** jako d (małe litery C i L jako mała litera D), **q** jako g (mała litera Q jako mała litera G), **cj** jako g (małe litery C i J jako mała litera G), **vv** jako w (podwójna litera V jako litera W), **ci** jako a (małe litery C oraz I jako mała litera A), **I** jako l (duża litera i jako mała litera L), **l** jako I (mała litera L jako duża litera i), **1** jako l (cyfra 1 jako mała litera L), **1** jako I (cyfra 1 jako duża litera i), **l** jako 1 (mała litera L jako cyfra 1), **I** jako 1 (duża litera i jako cyfra 1). **Punycode** natomiast to specjalne kodowanie, które jest wykorzystywane w celu konwersji Unicode na zestaw dozwolonych znaków w nazwie (tj. litery ASCII, cyfry i myślniki). Domenę, która zawiera znaki spoza ASCII, nazywamy Internationalized Domain Name (IDM) – dzięki Punycode jesteśmy w stanie przedstawić jej nazwę w wersji obsługiwanej przez serwery DNS.
Z kolei **bitsquatting** to technika polegająca na rejestracji domeny różniącej się o jeden bit od tej „popularnej", pod którą chciałby się podszyć atakujący. Całość opiera się na oczekiwaniu na losowe błędy spowodowane sprzętem komputerowym (najczęściej RAM-em)[38].
Do phishingu wykorzystywane są coraz bardziej wyrafinowane techniki, czego przykładem może być złośliwy kod zaszyty w plikach graficznych, keyloggery pobierane w chwili otwierania przez ofiarę wiadomości email czy też spreparowane strony nieróżniące się niczym od oryginalnych, włącznie z certyfikatem bezpieczeństwa – tzw. kłódką – widoczną obok adresu strony lub w prawym dolnym rogu ekranu, mającą zaświadczyć o autentyczności danej strony internetowej.
Podstawowe ataki phisingowe polegają na przekierowaniu odwołań użytkowników do fałszywych stron internetowych. Przez odpowiednio spreparowane formularze użytkownik jest odpytywany o dane do uwierzytelnień, numery kart płatniczych, jednorazowe kody autoryzacyjne, numery PIN. W zaawansowanych przypadkach atakujący posługują się bardziej wyszukanymi metodami. Mogą np. używać złośliwego oprogramowania do zainfekowania stacji klienta. Najczęściej dochodzi do tego w sposób całkowicie dla użytkownika niezauważalny, np. podczas przeglądania stron internetowych. Takie złośliwe oprogramowanie może funkcjonować na zasadzie tzw. tylne wejście (backdoor) i rejestrator aktywności klawiatury (keylogger). Jego zadaniem może być także śledzenie odwołania do serwisów bankowości internetowej i wtedy takie odwołanie stwierdza, rejestruje i loguje aktywność klawiatury. Skutkiem tego takie dane jak nazwy użytkowników oraz hasła dostępowe, a także ewentualnie numery PIN i kody autoryzowania transakcji przestają być poufne, mimo że połączenia do systemów bankowości internetowej są szyfrowane[39].
Można wyszczególnić pięć sposobów przeprowadzenia ataku phishingowego.

1. Phishing z wykorzystaniem wiadomości e-mail

Najstarszy spośród ataków phishingowych, nadal najpopularniejszy. Polega na wysłaniu potencjalnemu klientowi odpowiednio spreparowanej wiadomości email, której treść ma nakłonić atakowanego do kontaktu z fałszywym serwerem, który udaje serwer jego banku. Wiadomość zawiera link do strony udającej witrynę banku z formularzem do wpisania żądanych informacji poufnych. Warto zaznaczyć, że przesłane wiadomości posiadają najczęściej treść i wygląd bardzo zbliżony do oficjalnego szablonu korespondencji email wysyłanej przez bank.

2. Phishing z wykorzystaniem stron internetowych i mechanizmów usług webowych

Strony internetowe, które wykorzystywane są do przeprowadzenia ataków phishingowych, mogą być publikowane na serwerach zarządzanych przez atakującego lub na zaatakowanych serwerach internetowych, które są własnością innych organizacji. Typowe metody przeprowadzenia ataków wykorzystujących strony internetowe i mechanizmy usług webowych to: zamieszczanie – często w postaci zakamuflowanej – na często odwiedzanych stronach internetowych odnośników do fałszywych serwisów bankowych; wykorzystanie w charakterze graficznej reprezentacji odnośników do fałszywych stron, bannerów z elementami graficznymi charakterystycznymi dla banku, którego klienci są na celu ataków phishingowych; wykorzystanie pozbawionych ramek okienek typu pop-up dla ukrycia prawdziwego adresu pochodzenia komunikatów od atakującego; osadzenie na często odwiedzanych stronach lub na stronach, których adres, na ogół w zamaskowanej postaci, propaguje atakujący, obiektów aktywujących w środowisku przeglądarek internetowych podatności skutkujące umożliwieniem atakującemu przejęcie zdalnej kontroli nad stacją roboczą użytkownika lub zainstalowanie dowolnego złośliwego oprogramowania (na przykład keylogger, screen-grabber, backdo-

or, koń trojański); nadużycie – zdefiniowanych w środowisku przeglądarki internetowej – relacji zaufania w celu podszycia się pod autoryzowaną domenę lub zaufany serwer uprawniony do uruchamiania określonych skryptów lub odwołań do określonych źródeł danych; przeszukanie historii odwiedzin stron w celu spersonalizowania ataku (na przykład dostosowania formy i treści spamu phisingowego do konkretnego banku, z którego korzysta klient)[40].

3. Phishing z wykorzystaniem złośliwego oprogramowania

Złośliwe oprogramowanie może być przez atakującego wykorzystywane na dwa sposoby. Pierwszym z nich jest infekowanie komputera użytkownika, wykorzystywanego następnie do celów dystrybucji spreparowanej wiadomości poczty lub komunikatorów, albo też infekowanie innych stacji. Komputer, który został zainfekowany, staje się elementem tzw. botnetu, czyli licznego zbioru zainfekowanych stacji, które mogą być kontrolowane przez atakującego. Drugi sposób wykorzystania złośliwego oprogramowania to przeprowadzenie ataku phisingowego sprowadzającego się do infekowania stacji użytkowników, tj. przechwytywania danych poufnych, takich jak hasła i loginy do systemów bankowości internetowej, danych autoryzacji transakcji (haseł jednorazowych) i innych ważnych danych, np. numerów kart kredytowych. W tym celu najczęściej wykorzystywane są wirusy nazywane trojanami i programami szpiegującymi.

4. Phishing z wykorzystaniem popularności komunikatorów internetowych

Wraz ze wzrostem popularności komunikatorów internetowych wśród użytkowników Internetu, stały się one również celem przestępców działających w obszarze bankowości elektronicznej, a w szczególności bankowości internetowej. Rozwój funkcjonalności tych komunikatorów, tj. dodanie możliwości przesyłania grafik, elementów multimedialnych, rozwijania odnośników i aktywnych linków, powoduje, iż wszelkie techniki stosowane do przeprowadzania ataków phishingowych dla kanałów webowych znajdują zastosowanie także tu.

5. Phishing realizowany za pośrednictwem ataków man-in-the-middle

Skierowany jest na realizowane przez użytkownika połączenia z serwerami bankowości internetowej. Jego celem jest naruszenie poufności danych transmitowanych przez użytkownika, w tym zwłaszcza danych potwierdzających tożsamość użytkownika lub stanowiących podstawę autoryzacji dokonywanych przez niego transakcji. Atak tego typu polega na interaktywnej komunikacji przestępcy z klientem i wykorzystaniu wyłudzonych informacji w czasie rzeczywistym[41]. Atak man-in-the-middle wykorzystuje dodatkowy serwer, który łączy klienta z serwerem docelowym. Jego ideą jest przejmowanie pakietów, ich modyfikacja i wykorzystywanie w celu osiągnięcia własnych korzyści. W praktyce atak ten jest trudny do wykrycia, zwłaszcza po stronie użytkownika. Atakujący może nie tylko przechwycić pakiety, ale także wykradać informacje, przechwycić aktualną sesję i dowolnie ją modyfikować. Większość działań opiera się na sniffingu (podsłuchu). Pewnym minusem w stosunku do „typowego" phishingu jest fakt, że nie można go stosować masowo. O ile wysyłając maile ze sfałszowanymi stronami, atakujący otrzymuje wiele numerów kont i haseł, o tyle w tego rodzaju ataku musi się skupić na jednym, ewentualnie kilku klientach, którzy w dodatku niekoniecznie muszą na koncie mieć sumę rekompensującą wysiłek włożony w tego typu atak. Dlatego właśnie atak typu man-in-the-middle najczęściej stosuje się w celu kradzieży tożsamości i danych[42].

Zbliżoną do man-in-the-middle metodą jest man-in-the-browser (w skrócie MinB).

Jest to atak skierowany przeciwko przeglądarce, z której korzysta klient banku. Polega na modyfikacji danych, które wprowadza użytkownik podczas korzystania z usług bankowości internetowej. Ataki tego typu stanowią obecnie jedno z najpoważniejszych zagrożeń dla internetowego bezpieczeństwa, tak prywatnych internautów, jak i dużych instytucji, a ich celem są najczęściej serwisy bankowości internetowej. Pierwszym etapem tego typu ataku jest zainfekowanie przeglądarki internetowej końcowego użytkownika specjalnym rodzajem złośliwego oprogramowania. Mogą to być infekcje przeprowadzane w czasie przypadkowego odwiedzenia złośliwej strony internetowej (ataki typu drive-by download) lub w wyniku otwarcia odnośników zawartych w skierowanych wiadomościach poczty elektronicznej.

Drugim etapem ataku jest wykorzystanie agenta w przeglądarce do kontrolowania jej zachowania oraz modyfikowania i przechwytywania treści wyświetlanych oraz wprowadzanych przez końcowego użytkownika. W tym wypadku przed udaną modyfikacją treści oraz przechwyceniem danych nie uchroni już ani stosowanie do zabezpieczania stron przez banki protokołu SSL, ani dwuskładnikowe uwierzytelnianie stosowane coraz częściej przez wiele serwisów internetowych. Warto podkreślić, że ataki man-in-the-browser nie mają nic wspólnego ze słabościami samych systemów bankowych – są jedynie wynikiem lokalnych infekcji komputerów należących do użytkowników końcowych[43].

Odmiennym niż przesyłanie wiadomości email zawierających link odsyłający na fałszywe strony bankowe sposobem dokonywania przestępstwa typu phishing jest przesyłanie klientowi banku, za pośrednictwem poczty, przesyłki zawierającej CD lub inny nośnik danych przeznaczony do użytku na komputerze. Nośnik taki oznaczony jest stosowną grafiką zawierającą logo banku i inne tego typu elementy mające wskazywać jego oryginalne pochodzenie. Na nośniku znajduje się informacja, iż może on zostać wykorzystany na komputerze w celu zapoznania z najnowszą ofertą banku lub obejrzenia filmu. W rzeczywistości po włożeniu nośnika do czytnika w komputerze, uruchamia się złośliwe oprogramowanie służące do wykradania danych. Wykradzione w ten sposób dane, przesyłane są następnie do przestępcy za pośrednictwem Internetu[44].

Jako że mechanizm phishingu polega na umyślnym wprowadzaniu w błąd innej osoby, a jego celem jest uzyskanie poufnych danych dotyczących możliwości zalogowania się do internetowej witryny banku oraz dokonywanie nieuprawnionych operacji, działanie takie jest ingerencją w dane teleinformatyczne, a jego cel to osiągnięcie korzyści majątkowej. Tym samym czyn taki nosi znamiona czynu opisanego w art. 287 § 1 kk, czyli oszustwa komputerowego („Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, groma-

PHARMING

dzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5").

Pharming to bardziej zaawansowana i niebezpieczna dla użytkowników odmiana phishingu.

Cel w przypadku obu przestępstw jest ten sam – wyłudzenie poufnych danych. Różnica natomiast polega na tym, że w przypadku pharmingu nie jest wysyłana informacja nakłaniająca użytkownika do podania swoich poufnych informacji, zaś w momencie odwiedzania przez użytkownika witryny internetowej (np. strony internetowej swojego banku) następuje niezależnie od wiedzy i udziału użytkownika przekierowanie połączenia do fałszywej strony cyberoszusta, zamiast na właściwą stronę, mimo że użytkownik wpisał prawidłowy adres strony. Jednym słowem pharming polega na przekierowaniu użytkownika Internetu do spreparowanej strony internetowej, która wyglądem może przypominać witrynę banku internetowego, serwisu aukcyjnego, sklepu internetowego czy innej instytucji, w celu osiągnięcia przez hakera korzyści finansowych. Strony takie są tworzone najczęściej w celu zdobycia danych, takich jak login, hasło, numer karty kredytowej, PIN i innych – mogą one zostać wykorzystane do kradzieży pieniędzy z konta bankowego[45].

Przestępcy, dokonując pharmingu, najczęściej manipulują „pytaniami o kierunek" zgłaszanymi przez komputer w celu odnalezienia żądanej strony internetowej, co w konsekwencji powoduje dyskretne przekierowanie użytkownika do fałszywej witryny stworzonej przez sprawcę. Skutek ten możliwy jest do osiągnięcia na dwa sposoby. Pierwszy sposób polega na ingerencji w pamięć podręczną DNS komputera lokalnego, drugi na ingerencji w pamięć adresów DNS na serwerze[46].

Modyfikacja pamięci podręcznej DNS komputera lokalnego (zwana inaczej „zatruwaniem" adresów DNS) jest możliwa dzięki wykorzystaniu konia trojańskiego. Są to dodatkowe instrukcje dopisane najczęściej do załączników wiadomości poczty elektronicznej lub bezpłatnego oprogramowania dostępnego w Internecie (takich jak gry, wygaszacze ekranu, programy użytkowe). Po ich instalacji koń trojański zaczyna wykonywać pewne dodatkowe funkcje, umożliwiając hakerom np. zdalny dostęp do zainfekowanego komputera.

O wiele bardziej atrakcyjne może być uzyskanie dostępu do pamięci podręcznej serwera używanego przez usługodawcę internetowego, gdyż również tam są przechowywane wzory najczęstszych translacji adresu stron www na postać numerycznego adresu IP. Samo tłumaczenie następuje poprzez sprawdzenie adresu w tabelach, dostępnych w bazach danych 13 głównych serwerów DNS na świecie (tzw. gold standard DNS). W przypadku zainfekowania serwera dostawcy Internetu wszyscy użytkownicy, którzy z niego korzystają, a próbują zalogować się do swojego bankowego konta internetowego są przekierowywani na stronę sprawców i proszeni o zalogowanie się. Z uwagi na stosowane zabezpieczenia zatruwanie pamięci DNS serwerów jest trudne i nieczęste, natomiast w stosunku do użytkowników prywatnych tego typu ataki stają się coraz bardziej popularne. Warto podkreślić, że poza najstarszym i najpopularniejszym sposobem infekowania komputerów użytkowników koniem trojańskim, coraz częściej wykorzystywaną techniką jest tzw. drive-by pharming. Polega on na zagnieżdżaniu w kodzie tworzonych przez przestępców stron skryptów. W przypadku odwiedzenia tak spreparowanej strony zaimplementowany skrypt zmieni ustawienia DNS na jego routerze lub w punkcie dostępu bezprzewodowego. Może do tego dojść, jeśli router nie będzie chroniony hasłem albo hasło okaże się łatwe do odgadnięcia.

Modyfikując pamięć DNS, sprawca dokonuje zamachu na integralność danych informatycznych. Działanie takie wpisuje się w opis przestępstwa ujętego w art. 268 § 1 kk („Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2"). W przypadku, gdy czyn dotyczy zapisu na informatycznym nośniku danych, zagrożony jest karą pozbawienia wolności do lat 3. Natomiast zgodnie z art. 268a § 1 kk („Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3") ochronie podlega dostęp do danych, a nie integralność. Niemniej modyfikacja pamięci DNS wyczerpuje znamiona tego czynu, jako że proces przetwarzania danych nie zostaje zatrzymany, lecz przebiega w sposób odmienny od zamierzonego, a więc zakłócony. Podobnie sprawa przedstawia się w przypadku art. 269a kk („Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5"), który penalizuje zmianę danych informatycznych w istotnym stopniu zakłócających pracę systemu komputerowego lub sieci teleinformatycznej. Należy zauważyć, że wymienione powyżej przepisy odnoszą się do samego faktu modyfikacji zapisów w systemie komputerowym, co jest – jak wynika z opisu sposobu przeprowadzania pharmingu – jedynie środkiem do celu sprawcy, jakim w konsekwencji stanowi uzyskanie danych uwierzytelniających niezbędnych do przejęcia środków zgromadzonych na koncie użytkownika. Z tego powodu i mając na uwadze, iż celem działania sprawcy pharmingu w przypadku ataków na klientów bankowości internetowej jest osiągnięcie korzyści majątkowej, może być ono również penalizowane na gruncie art. 287 kk (oszustwo komputerowe).

Kolejnym z grupy przestępstw dokonywanych w obszarze bankowości internetowej jest sniffing. Nazwa pochodzi od angielskiego słowa *sniff*, które oznacza wąchanie, obwąchiwanie[47]. Technika ta początkowo została stworzona na potrzeby administratorów i polegała na podsłuchiwaniu wszystkich pakietów, które krążyły po sieci komputerowej. Celem takiego działania było dokonywanie analiz tych pakietów w poszukiwaniu nieprawidłowości funkcjonowania sieci. Pozwalało to na zidentyfikowanie słabych stron danej sieci i odpowiednią jej modyfikację. Tego typu narzędzie diagnostyczne jest nadal szeroko wykorzystywane w codziennej pracy zespołów IT administrujących sieciami teleinformatycznymi na całym świecie. Przestępcy/hakerzy wykorzystują do sniffingu specjalnie stworzone oprogramowanie, pozwalające wychwycić spośród pakietów informacji konkretne dane, takie jak numery kart, dane logowania – hasła i loginy czy też dane osobowe.

Przestępstwo sniffingu pozwala osobom postronnym na uzyskanie danych przesyłanych przez sieć, ale nie wpływa na ich zawartość. Informacja niezmieniona i kompletna dociera do odbiorcy. Metoda ta ma, jak zatem widać, bierny charakter, nie stanowi w sposób bezpośredni zagrożenia.

Jest jedynie narzędziem, które pozwala snifferowi na uzyskanie niezbędnych danych do realizacji innych przestępstw, bardziej niebezpiecznych i stanowiących bezpośrednie zagrożenie – przykładowo numer karty kredytowej zdobyty przez podsłuch sieci może zostać następnie wykorzystany przez osoby nieuprawnione do realizacji płatności. Sprawca sniffingu swoim zachowaniem wyczerpuje znamiona czynu określonego w art. 267 § 3 kk („Kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem") zagrożonego karą grzywny, karą ograniczenia wolności albo karą pozbawienia wolności do lat 2. Sniffing jest przestępstwem umyślnym, które można popełnić tylko w zamiarze bezpośrednim, zaś osoba, która instaluje urządzenie podsłuchowe, np. na cudze zlecenie, ponosi odpowiedzialność karną na podstawie 267 § 3 kk tylko wówczas, jeżeli ma świadomość, iż nie jest uprawniona do zakładania tego rodzaju urządzeń. Osoba zlecająca takiego rodzaju działania odpowiadać będzie natomiast za sprawstwo kierownicze w zakresie polecenia popełnienia czynu z art. 267 § 3 kk[48].

Spoofing (ang. *spoof* – naciąganie, szachrajstwo) – grupa ataków na systemy teleinformatyczne polegających na podszywaniu się pod inny element systemu informatycznego. Efekt ten osiągany jest poprzez umieszczanie w sieci preparowanych pakietów danych lub niepoprawne używanie protokołów[49]. Innymi słowy, technika ta polega na oszukiwaniu komputera-odbiorcy, który błędnie identyfikując nadawcę, wszystkie pakiety informacji wysyła do agresora, co następnie pozwala na udostępnienie poufnych danych, a finalnie może doprowadzić do ich wykorzystania celem przejęcia środków zgromadzonych na koncie bankowym ofiary.

Sposób popełnienia spoofingu w bankowości internetowej można podzielić na dwie fazy – pierwsza polega na udawaniu banku przez przestępców. Podobnie jak w przypadku sniffingu, etap ten służy głównie do uzyskania danych potencjalnych ofiar, takich jak imię, nazwisko, numer karty kredytowej, a przede wszystkim do zdobycia tajnego identyfikatora i hasła, które klienci wykorzystują podczas logowania się do systemu bankowości internetowej z portalu transakcyjnego banku. Sprawcy w tym wypadku wykorzystują nieuwagę klientów oraz błędy programowe przeglądarek internetowych. Mogą przykładowo rozsyłać do klientów emaile z informacją o otwarciu nowego serwisu transakcyjnego z prośbą o jak najszybsze logowanie. Znajdujący się w treści maila link będzie prowadzić do fałszywego serwera, kontrolowanego przez przestępców. W ten sposób wchodzą oni w posiadanie autentycznych danych logowania klientów. Drugi etap spoofingu to wykorzystanie zdobytych danych i dokonanie przelewu pieniędzy na swoje konta.

Sprawca spoofingu swoim zachowaniem wyczerpuje znamiona czynu z art. 267 § 1 kk (kradzież informacji), zagrożonego karą grzywny, karą ograniczenia wolności albo karą pozbawienia wolności do lat 2.

PODSUMOWANIE

W przedmiotowym opracowaniu zawarto opis zagrożeń związanych z korzystaniem z usług bankowości elektronicznej, a także rodzaje przestępstw w obszarze bankowości elektronicznej oraz metody stosowane przez sprawców w przypadku wszelakich transakcji realizowanych za pomocą kart zarówno płatniczych, jak i kredytowych, bankomatów oraz coraz popularniejszej bankowości internetowej. Zaprezentowane metody ukazują duże zróżnicowanie w działaniach przestępczych w poszczególnych usługach bankowości elektronicznej. Determinuje to profil potencjalnego przestępcy. W przypadku bankomatu, gdy w grę wchodzi wykorzystanie oddziaływania fizycznego na urządzenie, lub w przypadku kart płatniczych, gdy kluczowe jest wejście w posiadanie fizycznej karty, np. w drodze kradzieży kieszonkowej, możliwe jest działanie przez sprawców niemających specyficznych umiejętności czy narzędzi. Inaczej sytuacja wygląda w przypadku bardziej wyrafinowanych metod, takich jak np. skimming kart lub skimming bankomatowy, gdzie niezbędne jest posiadanie dedykowanych, specjalnie przygotowanych urządzeń służących do pozyskania danych zapisanych na karcie. W przypadku bankowości internetowej można zaryzykować stwierdzenie, iż konieczne jest posiadanie odpowiedniej, specjalistycznej wiedzy z zakresu informatyki, by móc przeprowadzić skuteczny atak.

Potencjalna ofiara musi zachować czujność na każdym kroku – przykładowo używając tej samej karty kredytowej w bankomacie, płacąc nią w sklepie czy dokonując transakcji przez Internet. Każdy z tych kanałów wymaga zastosowania odmiennych zasad ostrożności, aby uniemożliwić lub przynajmniej utrudnić potencjalnym sprawcom dokonanie przestępstwa.

Same grupy przestępcze, mając świadomość efektu synergii pomiędzy poszczególnymi kanałami bankowości elektronicznej, skrzętnie go wykorzystują. Według kwalifikacji czynów w obowiązujących przepisach potencjalne ryzyko, którego miernik stanowi wymiar kary przewidziany aktualnie w kodeksie karnym, jest zdecydowanie niższe niż potencjalnie uzyskiwane korzyści. Kwoty, w posiadanie których mogą wejść przestępcy np. po uzyskaniu dostępu do konta internetowego ofiary, na którym zgromadzone są wszystkie posiadane przez niego środki, mogą być dla przestępców dużą zachętą. Dodatkowo ryzyko bycia przyłapanym w momencie popełniania danego czynu jest niewielkie, jako że – ze względu na specyfikę bankowości elektronicznej – może być on dokonany na odległość.

Zagrożenia związane z korzystaniem z usług świadczonych w bankowości elektronicznej będą się dynamicznie zmieniać, tak jak zmieniają się nowoczesne technologie. Najważniejsze będzie świadome działanie użytkownika, ponieważ nawet najbardziej skomplikowane i zaawansowane technologicznie zabezpieczenia nie zastąpią rozwagi i zdrowego rozsądku podczas korzystania z usług bankowych dostarczanych kanałami elektronicznymi. Na nic się zdadzą wszelkie zabezpieczenia, jeśli użytkownik nie zadba o przestrzeganie podstawowych zasad bezpieczeństwa. Oczywiście w świetle obowiązujących przepisów banki i inne instytucje biorące udział w realizacji

transakcji są zobowiązane do zapewnienia bezpieczeństwa operacji wykonywanych przez swoich klientów zarówno od strony operacyjnej, jak i technicznej. Różnorodność potencjalnych rozwiązań stosowanych przez banki i operatorów utrudnia dokonanie przestępstwa, nieustający postęp technologiczny otwiera nowe możliwości zapewnienia bezpieczeństwa transakcji, a jednak mimo wszystko nadal istotnym elementem będzie użytkownik końcowy, który musi w sposób umiejętny i świadomy posługiwać się dostarczonymi mu rozwiązaniami. Analizowany obszar bezpieczeństwa pozwala stwierdzić, że w zagrożeniach nad ochroną środków płatniczych jednym z najważniejszych elementów jest działanie człowieka. W jednym z zachowań użytkownika niezbędne będzie jego przemyślane, usystematyzowane i zgodne z regulaminem usługodawcy, postępowanie w trakcie transakcji. Z drugiej zaś strony będzie prawidłowy system ochrony usługodawcy (banku) i jego administratorów bezpieczeństwa. Niemniej jednak należy stwierdzić, że zachowanie wymogów bezpieczeństwa obu stron może jednak jedynie utrwalić działanie sprawcy czynu przeciwko środkom płatniczym. Dlatego konieczne staje się właściwe przygotowanie służb porządku publicznego do przeciwdziałania, zapobiegania i wykrywania sprawców tego rodzaju czynów zabronionych. Ich umiejętności, doświadczenie i narzędzia prawne w pełni pozwolą na zapewnienie prawidłowego procesu ochrony przedmiotu przestępstwa, jakim są elektroniczne środki płatności.

Słowa kluczowe: przestępstwo, środki płatnicze, proces wykrywczy, bezpieczeństwo klienta bankowego

Keywords: crime, legal tenders, detection process, security of the bank client

[1] T. Sławek, *Zagrożenia w płatnościach bankowych*, UTH im. H. Chodkowskiej, Warszawa 2017.
[2] T. Sławek, *Zagrożenia w płatnościach bankowych*.
[3] J. Kukulski, *Aspekty prawne bankowych kart płatniczych w polskim systemie płatniczym*, Wydawnictwo Kodeks Sp. z o.o., Warszawa 2002, s. 13.
[4] A. Bury, *Karty płatnicze w Polsce*, Wydawnictwo CeDeWu Sp. z o.o., Warszawa 2001, s.14.
[5] A. Myczkowska, T. Dąbrowski, *Karty płatnicze. Przewodnik po świecie plastykowego pieniądza*, Wydawnictwo Rzeczpospolita, Warszawa 1997, s. 8.
[6] J. Kukulski, *Aspekty prawne bankowych kart płatniczych w polskim systemie płatniczym*, s. 46–47.
[7] Art. 4 ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2017 r. poz. 1876).
[8] Z. Dobosiewicz, *Podstawy bankowości*, Wydawnictwo Naukowe PWN, Warszawa 2002, s. 163.
[9] W. Grzegorczyk, *Produkty bankowe: rozwój i sprzedaż*, Wydawnictwo Biblioteka Menedżera i Bankowca, Warszawa 2001, s. 93–94.
[10] J. Grzywacz, *Podstawy bankowości. System bankowy kredyty i rozliczenia, ryzyko i ocena banku, marketing*, Wydawnictwo Difin, Warszawa 2002, s. 8.
[11] http://www.karty-plastikowe.pl/karty-magnetyczne.html; www.podsystem.pl/oferta_katy_magn.pkp [dostęp: 22.11.2017 r.].
[12] W. Grzegorczyk, *Produkty bankowe: rozwój i sprzedaż*, s. 93–94.
[13] B. Świecka, *Detaliczna bankowość elektroniczna*, CeDeWu, Warszawa 2007, s. 50–52.
[14] Z. Dobosiewicz, *Podstawy bankowości*, Wydawnictwo Naukowe PWN, Warszawa 2002, s. 164.
[15] D.T. Dziuba, *Systemy informatyczne w obsłudze banków detalicznych*, wyd. Uniwersytetu Warszawskiego, Warszawa 2002, s. 130.
[16] A. Bury, *Karty płatnicze*, CeDeWu, Warszawa 1999, s. 39.
[17] B. Świecka, *Detaliczna bankowość elektroniczna*, CeDeWu, Warszawa 2007, s. 232.
[18] A. Borcuch, *Bankowość elektroniczna w Polsce*, CeDeWu, Warszawa 2011, s. 65.
[19] P. Niczyporuk, A. Talecka, *Bankowość – podstawowe zagadnienia*, wyd. Temida 2, Białystok 2011, s. 200.
[20] Tamże, s. 202.
[21] KNF, *Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia*, Warszawa 2010, s. 58.
[22] www.wikipedia.org [dostęp: 30.09.2017 r.].
[23] B. Świecka, *Detaliczna bankowość elektroniczna*, s. 33.
[24] Tamże, s. 53.
[25] M. Kaczmarek, *Użyteczność serwisów internetowych banków – pomiar i ewolucja*, Wyd. UEP, Poznań 2016, s. 7.
[26] Tamże, s. 8.
[27] T. Sławek, *Zagrożenia w płatnościach bankowych*.
[28] R. Kaszubski, Ł. Obzejta, *Karty płatnicze w Polsce*, Wolters Kluwer Polska, Warszawa 2012, s. 378.
[29] Dz. U. UE Nr L149/1 z dnia 2.06.2001 r. wraz ze sprostowaniem do decyzji ramowej Rady z dnia 28 maja 2001 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi (2001/413/WSiSW), Dz. Urz. UE L 282/38 z 25.10.2008 r.
[30] K.J. Jakubski, *Przestępstwa związane z wykorzystaniem kart*, „Prawo Bankowe" 1998, nr 2, s. 84–87.
[31] *Ocena funkcjonowania polskiego systemu płatniczego*, NBP, Warszawa – dokument cykliczny, http://www.nbp.pl/home.aspx?f=/systemplatniczy/ocena/ocena.html [dostęp: 22.11.2017 r.].
[32] R. Łuczak, *Zagrożenia związane z obrotem przy użyciu kart płatniczych, część II Fałszerstwa związane z obrotem kartami płatniczymi*, „Problemy Kryminalistyki" 2001, nr 212, s.10.
[33] K.J. Jakubski, *Przestępstwa związane z wykorzystaniem kart*, s. 89.
[34] J. Gąsiorowski, P. Podsiedlik, *Przestępstwa w bankowości elektronicznej w Polsce*, WSB, Dąbrowa Górnicza 2015, s. 55.
[35] A.J. Grandys, *Usługi finansowe w rzeczywistości wirtualnej – kartowe doświadczenia*, „Bank" 1999, nr 9, s. 4.
[36] Ustawa z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. Nr 214, poz. 1344).
[37] Decyzja ramowa Rady Unii Europejskiej 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz. Urz. UE L 69/67 z 16.03.2005 r.).
[38] https://sekurak.pl/nietypowe-metody-wykorzystywane-w-atakach-phishingowych [dostęp 30.09.2017 r.].
[39] J. Gąsiorowski, P. Podsiedlik, *Przestępstwa w bankowości elektronicznej w Polsce*, s. 150.
[40] J. Nawrat, *Phishing i antyphishing w bankowości internetowej*, „Boston IT Security Review" 2017, nr 4, s. 50.
[41] G. Szwajkowska, P. Kwaśniewski, K. Leżoń, W. Woźniczka, *Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia*, UKNF, Warszawa 2010, s. 35.
[42] M. Ziarek, *Phishing, pharming i sieci. Zombie i to, czego nie wiesz o swoim komputerze*, http://securelist.pl [dostęp: 22.11.2017 r.].
[43] https://sekurak.pl/jak-wyglada-atak-typu-man-in-the-browser/.
[44] R. Kaszubski, Ł. Obzejta, *Karty płatnicze w Polsce*, Wolters Kluwer Polska, Warszawa 2012, s. 402.

[45]M. Jelesiński, *Pharming – nadchodzi nowe zagrożenie?*, http://pc-centre.pl/ [dostęp: 4.02.2006 r.].
[46]A. Kiedrowicz, *Wywiad. Pharming i jego penalizacja*, „Prokuratura i Prawo" 2011, nr 6, s. 24.
[47]J. Fisiak, A. Adamska-Szałaciak i in., *Słownik współczesny angielsko-polski, polsko-angielski*, Longman, Bergamo 2006, s. 408.
[48]A. Adamski, *Nadużycia związane z kartami płatniczymi i ich karalność – przestępczość gospodarcza z perspektywy Polski i Unii Europejskiej*, TNOiK Dom Organizatora, Toruń 2003.
[49]www.wikipedia.org [dostęp: 30.09.2017 r.].

Bibliografia

Adamski A., *Nadużycia związane z kartami płatniczymi i ich karalność – przestępczość gospodarcza z perspektywy Polski i Unii Europejskiej*, TNOiK Dom Organizatora, Toruń 2003.
Bury A., *Karty płatnicze w Polsce*, Wydawnictwo CeDeWu Sp. z o.o., Warszawa 2001.
Bury A., Karty płatnicze, CeDeWu, Warszawa 1999.
Dobosiewicz Z., *Podstawy bankowości*, Wydawnictwo Naukowe PWN, Warszawa 2002.
Dziuba D.T., *Systemy informatyczne w obsłudze banków detalicznych*, wyd. Uniwersytetu Warszawskiego, Warszawa, 2002.
Fisiak J., Adamska-Szałaciak A. i in., *Słownik współczesny angielsko-polski, polsko-angielski*, Longman, Bergamo 2006.
Gąsiorowski J., Podsiedlik P., *Przestępstwa w bankowości elektronicznej w Polsce*, WSB, Dąbrowa Górnicza 2015.
Grandys A.J., *Usługi finansowe w rzeczywistości wirtualnej – kartowe doświadczenia*, „Bank" 1999, nr 9.
Grzegorczyk W., *Produkty bankowe: rozwój i sprzedaż*, Wydawnictwo Biblioteka Menedżera i Bankowca, Warszawa 2001.
Grzywacz J., *Podstawy bankowości. System bankowy kredyty i rozliczenia, ryzyko i ocena banku, marketing*, Wydawnictwo Difin, Warszawa 2002.
Jakubski K.J., *Przestępstwa związane z wykorzystaniem kart*, „Prawo Bankowe" 1998, nr 2.
Kaczmarek M., *Użyteczność serwisów internetowych banków – pomiar i ewolucja*, Wyd. UEP, Poznań 2016.
Kaszubski R., Obzejta Ł., *Karty płatnicze w Polsce*, Wolters Kluwer Polska, Warszawa 2012.
Kiedrowicz A., *Wywiad. Pharming i jego penalizacja*, „Prokuratura i Prawo" 2011, nr 6.
KNF, *Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia*, Warszawa 2010.
Kukulski J., *Aspekty prawne bankowych kart płatniczych w polskim systemie płatniczym*, Wydawnictwo Kodeks Sp. z o.o., Warszawa 2002.
Łuczak R., *Zagrożenia związane z obrotem przy użyciu kart płatniczych, część II Fałszerstwa związane z obrotem kartami płatniczymi*, „Problemy Kryminalistyki" 2001, nr 212.
Myczkowska A., Dąbrowski T., *Karty płatnicze. Przewodnik po świecie plastykowego pieniądza*, Wydawnictwo Rzeczpospolita, Warszawa 1997.
Nawrat J., *Phishing i antyphishing w bankowości internetowej*, „Boston IT Security Review" 2017, nr 4.
Niczyporuk P., Talecka A., *Bankowość – podstawowe zagadnienia*, wyd. Temida 2, Białystok 2011.
Sławek T., *Zagrożenia w płatnościach bankowych*, UTH im. H. Chodkowskiej, Warszawa 2017.
Szwajkowska G., Kwaśniewski P., Leżoń K., Woźniczka W., *Usługi bankowości elektronicznej dla klientów detalicznych. Charakterystyka i zagrożenia*, UKNF, Warszawa 2010.
Świecka B., *Detaliczna bankowość elektroniczna*, CeDeWu, Warszawa 2007.

Akty prawne

Dz. Urz. UE L 149/1 z dnia 02.06.2001 r. wraz ze sprostowaniem do decyzji ramowej Rady z dnia 28 maja 2001 r. w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi (2001/413/WSiSW), Dz. Urz. UE L 282/38 z 25.10.2008 r.
Decyzja ramowa Rady Unii Europejskiej 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz. Urz. UE L 69/67 z 16.03.2005 r.).
Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz. U. z 2017 r. poz. 1876).
Ustawa z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. Nr 214, poz. 1344).

Netografia

http://www.karty-plastikowe.pl/karty-magnetyczne.html; www.podsystem.pl/oferta_katy_magn.pkp [dostęp: 22.11.2017 r.].
https://sekurak.pl/jak-wyglada-atak-typu-man-in-the-browser/ [dostęp 30.09.2017 r.].
https://sekurak.pl/nietypowe-metody-wykorzystywane-w-atakach-phishingowych [dostęp 30.09.2017 r.].
Jelesiński M., *Pharming – nadchodzi nowe zagrożenie?*, http://pccentre.pl/ [dostęp: 4.02.2006 r.].
Ocena funkcjonowania polskiego systemu płatniczego, NBP, Warszawa – dokument cykliczny, http://www.nbp.pl/home.aspx?f=/systemplatniczy/ocena/ocena.html].
Spoofing, w: https://pl.wikipedia.org/wiki/Spoofing [dostęp: 30.09.2017 r.].
Ziarek M., *Phishing, pharming i sieci. Zombie i to, czego nie wiesz o swoim komputerze*, http://securelist.pl [dostęp 30.09.2017 r.].

Summary

E-banking – threats

In times when legal tenders, such as printed banknotes and minted coins, are successively replaced by modern payment methods with the use of the Internet or smart phones, security of these transactions becomes one of overarching objectives in the protection of property belonging to bank client. The present study is aimed at moving closer the issues of actions of perpetrators taking over legal tenders and ways of protecting ourselves against that kind of crimes, both in the area of bank contractor's actions and the ones of a client, whose careless actions can facilitate the perpetration of this kind of property crimes.

Tłumaczenie: Renata Cedro, WP

RANSOMWARE
– wymuszanie okupu w sieci

Jarosław Sordyl

Zastępca Dyrektora ds. Cyberbezpieczeństwa Departamentu Bezpieczeństwa PSE S.A., audytor wiodący ISO 27001, ekspert informatyki śledczej, trener i wykładowca z zakresu bezpieczeństwa systemów teleinformatycznych, posiadacz m.in. tytułów CDFE, CISSO. W latach 2011–2013 członek zarządu Europolu.
Deputy Director of Cybersecurity Security department, PSE S.A. lead auditor of ISO 27001, Computer Forensics expert, trainer and lecturer of IT system security, holder of CDFE, CISSO certificates. 2011–2013 member of Management Board of Europol.

W ostatnich latach doświadczyliśmy ogromnego wzrostu ataków z wykorzystaniem programów „złośliwych" ransomware* – wymuszających okup. Cyberprzestępcy w bardzo krótkim czasie „wypuszczali" w świat coraz to nowe programy blokujące, z wersji na wersję bardziej zaawansowane w metodach blokowania dostępu – aż do wykorzystania kryptograficznych algorytmów eliptycznych szyfrujących informacje/dane włącznie.

W 2017 r. bardzo dynamicznie rozwija się oprogramowanie ransomware, atakujące zasoby informacyjne firm. NotPetya czy WannaCry to tylko niektóre z odmian tego bardzo niebezpiecznego oprogramowania. Jego wprowadzenie do sieci firmowej może skutecznie zablokować działanie przedsiębiorstwa na okres aż do opłacenia okupu, przy czym około 75% ataków nie kończy się tak dobrze. Celem NotPetya/Expetya – jak się okazuje po analizach – jest niszczenie danych, a nie wymuszanie okupu.

Od początku pojawienia się ataków typu Ransomware obserwujemy nie tylko rozwój samego oprogramowania, ale także wektorów ataków. W najbliższym okresie nie należy się spodziewać osłabienia samych ataków, ale trzeba wziąć pod uwagę nowe podatności, wektory ataków oraz to, że każdy może się stać celem ataku. W związku z tym warto upowszechniać wiedzę na temat ransomware.

*programowe blokowanie dostępu do informacji z wykorzystaniem kryptografii oraz żądanie okupu

WSTĘP

Dynamiczny rozwój sieci Internet, który rozpoczął się w połowie lat 90. ubiegłego wieku, doprowadził do wielu nieodwracalnych zmian. Świat stał się dostępny na wyciągnięcie ręki, postępujące procesy globalizacji umożliwiają prowadzenie każdej działalności w prawie każdym miejscu na świecie. Mamy nieograniczone możliwości w nawiązywaniu kontaktów, wykonywaniu pracy czy w dostępie do informacji. Niemniej jednak codziennie media informują o rożnych nadużyciach, które miały miejsce w sieci internetowej, ktoś został okradziony z pieniędzy, kolejnej osobie skradziono dane personalne i wykorzystano w działaniach przestępczych czy też wykradziono ważne dokumenty z bazy firmy, która w wyniku takich działań utraciła klientów czy też wiarygodność. Scenariuszy związanych z postępowaniem cyberprzestępców jest wiele. W ciągu ostatnich lat „koalicja" antycyberprzestępcza, składająca się z przedstawicieli organów ścigania, m.in. Policji, agencji unijnych oraz organizacji zajmujących się problematyką bezpieczeństwa sieci, informowała użytkowników o różnych zagrożeniach, jakie czyhają na każdego z nich. O ich złożoności, skali czy też sposobach prowadzenia ataków i ich celach napisano wiele publikacji i artykułów. Jednym z takich zagrożeń, które skutecznie „atakuje" i naraża na straty finansowe, jest „ransomware" – wymuszanie okupu w cyberprzestrzeni.

RANSOMWARE – definicja zjawiska

Czym jest ransomware? Jest to typ wymuszenia w cyberprzestrzeni, stosowany przez przestępców posługujących się specjalnie przygotowanym oprogramowaniem, mającym na celu zablokowanie użytkownikowi dostępu do systemu operacyjnego komputera lub zaszyfrowanie danych i informacji. Dostęp ten może zostać odzyskany po opłaceniu odpowiedniej wysokości „okupu" za pośrednictwem różnego rodzaju systemów płatności elektronicznej „pre-paid", a ostatnio – coraz bardziej popularnych kryptowalut, np. bitcoin.

Ransomware stanowi jeden z wielu sposobów wykorzystywanych przez cyberprzestępców do przeprowadzania ataków, których bezpośrednim celem jest uzyskanie środków finansowych. Trudno oszacować, ile na świecie zostało zaatakowanych użytkowników oraz ilu z nich zapłaciło okup, ale jak pokazują raporty firm zajmujących się bezpieczeństwem systemów teleinformatycznych, są to dochody liczone w milionach USD. Metoda ta ciągle się rozwija, a jej popularność powodują m.in. następujące uwarunkowania:

- anonimowe płatności, które utrudniają bądź uniemożliwiają identyfikację atakującego;
- łatwy dostęp w sieci Internet do zasobów i programów pozwalających na przeprowadzenie ataku ransomware;
- w dalszym ciągu bardzo niski poziom świadomości wśród użytkowników na temat tego zagrożenia[1].

Obecnie najczęściej spotyka się zagrożenia, które w swoim działaniu wykorzystują szyfrowanie zasobów na danym komputerze wraz z wyświetlaniem na ekranie informacji o wyznaczonym czasie na opłacenie „okupu". Po upływie tego czasu kwota wzrasta, np. dwukrotnie, lub kasowane są wybrane losowo pliki/foldery na zaszyfrowanym zasobie.

O tym typie zagrożenia dystrybuowanego poprzez sieć Internet, ukierunkowanego na użytkownika końcowego, głośno stało się w latach 2005–2006 w Rosji, gdzie grupy hakerskie przypuściły atak na użytkowników[2]. Początkowy schemat ataku był następujący: do użytkownika docierała przesyłka e-mail wskazująca na konieczność odwiedzenia strony internetowej, np. w celu potwierdzenia swojej tożsamości w banku, lub też wydrukowania załączonej do wiadomości „superoferty". Po kliknięciu w załącznik użytkownik instalował najczęściej „kod złośliwy" z tzw. elementem kontroli i zarządzania (command and control), a następnie za jego pośrednictwem był przekierowany na stronę, z której był pobierany program wykonawczy, mający za zadanie blokowanie dostępu do pulpitu systemu operacyjnego, co uniemożliwiało wykonanie jakiejkolwiek operacji. Na ekranie była wyświetlana informacja, z której wynikało, iż w celu odblokowania komputera należy wysłać na wskazany numer SMS-a o określonej treści. Były to oczywiście numery „Premium", z których cyberprzestępcy czerpali zyski. Takie były początki działalności cyberprzestępczej związanej z ransomware – wymuszaniem okupu w sieci.

Kolejną odsłoną tego typu metody był „Winlocker", mający charakter ataku socjotechnicznego[3], który to oprócz blokowania ekranu użytkownika i informacji wymuszającej okup za odblokowanie wyświetlał ekran z wiadomością łudząco przypominającą informację ze strony policyjnej. Zawierała ona komunikat o popełnionym przez użytkownika przestępstwie, za które musi zapłacić grzywnę poprzez wskazany system płatności, np. Ukash lub Paysefecard. Kwota, której żądano za odblokowanie komputera, zależała od miejsca pobytu zaatakowanego użytkownika, była jednocześnie zdecydowanie większa niż koszt SMS-a „Premium" i wynosiła odpowiednio od 100 USD do 100 funtów. Ten typ ataku uzyskał specyficzną nazwę – „Police Ransomware" – czyli wymuszanie okupu przez „policję". Jego charakterystycznym elementem był wizerunek oznaczeń policyjnych na ekranie, który pojawiał się po zablokowaniu dostępu do komputera wraz z informacjami dotyczącymi popełnionego rzekomo przestępstwa. W polskiej wersji tego ataku oprócz wizerunku policyjnych elementów odnotowano także wykorzystanie wizerunku Prezydenta RP.

W 2011 r. pojawiły się zagrożenia wymuszające, które były dystrybuowane jako fałszywe antywirusy. Komunikat towarzyszący temu oprogramowaniu informował, iż komputer użytkownika nie jest chroniony i wymagana jest instalacja odpowiedniego oprogramowania, do którego wskazywano link. Nie był to oczywiście prawdziwy program antywirusowy, lecz program typu ransomware.

Najnowszym rozwiązaniem i zarazem kolejnym wariantem ransomware dystrybuowanym przez cyberprzestępców są różne odmiany zagrożenia zwanego „cryptoloker", blokującego dostęp do zasobów użytkownika na komputerze oraz szyfrującego je, najczęściej szyfrowaniem asymetrycznym[4]. Również tym razem pojawia się komunikat wyświetlany na monitorze komputera, informujący o konieczności zapłacenia okupu poprzez systemy płatności on-line, aby otrzymać klucz, tzw. prywatny, niezbędny do odblokowania zasobów. W przypadku niezapłacenia okupu program atakujący kasuje wszystkie zablokowane zasoby lub też niszczy klucz prywatny, który jest wymagany do odszyfrowania plików. Przy czym czas, w którym należy opłacić okup, jest zdefiniowany i wynosi najczęściej od 48 do 72[5] godzin. Do ostatnich programów tego typu należą m.in. WannaCry, NotPetya, BadRabit.

Sposoby dystrybucji ataku

Pierwszym i najczęściej spotykanym sposobem dystrybucji ataku typu ransomware były przesyłki e-mail kierowane do przypadkowych osób, najczęściej wykradzionych z zaatakowanych systemów pocztowych. Oczywiście program atakujący jest załączony w takim przypadku do głównej wiadomości, która mogła mieć taką treść: *W załączeniu przesyłamy bilet lotniczy – nagrodę, która została wylosowana dla Pana/Pani w naszym systemie podróży*. Schemat dalszego scenariusza jest prosty. Zainteresowany użytkownik otwiera załącznik, tym samym instalując program szkodliwy – „agenta", który łączy się z zasobami w sieci Internet z C&C (Command and Control – zarządzanie i kontrola), najczęściej z serwerem dystrybuującym oprogramowanie złośliwe. Program ten informuje o lokalizacji użytkownika, zainstalowanych programach i ich wersjach i ściąga program blokujący dostęp. Sposób dalszego postępowania już znamy. Aby odblokować dostęp, trzeba zapłacić „okup". Taki rodzaj ataku był identyfikowany przez organizacje oraz niezależne laboratoria zajmujące się bezpieczeństwem jako Troj/ransom-JO[6].

Atak poprzez rozsyłanie e-maili wymagał dodatkowego nakładu pracy, m.in. pozyskania listy e-mail, następnie przygotowanie scenariusza ataku socjotechnicznego, w wyniku którego użytkownik końcowy np. otwierał załącznik przesłany wraz z wiadomością. Wraz z rozwojem zagrożenia cyberprzestępcy sięgnęli po bardziej efektywny sposób ataku użytkowników,

tzw. *wathering hole* – studnia wody[7]. Polega to na przygotowaniu odpowiedniej „zainfekowanej" oprogramowaniem wymuszającym strony w sieci internetowej, na którą przekierowywani są użytkownicy np. wybranej korporacji, którzy zostali nakłonieni do akceptacji tzw. pop-up, okienka z odpowiednio przygotowaną „atrakcyjną" informacją, która pojawia się podczas przeglądania różnych serwisów www. Cyberprzestępcy mogą też w wyniku rekonesansu dowiedzieć się, jakie strony są najczęściej odwiedzane przez pracowników, i taką stronę infekują w celu przeprowadzenia ataku.
Kolejnym sposobem atakowania użytkowników są różnego rodzaju exploity[8], które miały za zadanie wykrycie słabości systemu użytkownika i dobranie odpowiedniego ataku powodującego blokadę dostępu do komputera. Przykładem takiego zestawu programów typu exploit może być „Blackhole", który wykorzystuje podatności występujące w plikach typu PDF oraz programach opartych na Javie. Mając taki exploit, należy tylko dostarczyć spreparowany program do użytkownika – potencjalnej ofiary.

Pranie pieniędzy pochodzących z ransomware

Każdy z systemów płatniczych wykorzystywanych przy okazji ataku ransomware ma za zadanie ukrycie bądź uniemożliwienie dotarcia do cyberprzestępcy lub jego bezpośredniego wskazania. Dlatego najczęściej w tego typu działaniach są wykorzystywane systemy płatności on-line bądź też systemy pre-paid, które w zamian za wpłaconą gotówkę lub wykonany przelew elektroniczny generują kod o określonej wartości. Następnie można tymi kodami posługiwać się w systemach kasyn lub gier on-line i – w przypadku wygranej – można swobodnie dokonać przelewów na swoje konto i wypłacić pieniądze uzyskane z gry – całkowicie legalnie. Jest to jeden z systemów pozwalający na tzw. pranie pieniędzy. Innym rozwiązaniem są systemy parabankowe, które za pośrednictwem Internetu pośredniczą w różnego rodzaju anonimowych transakcjach wpłat/wypłat/przelewów/transferów gotówki. Do takich systemów należy m.in. Perfect Money, Web Money, które nie są powiązane z żadnym systemem bankowym, co utrudnia prowadzenie ustaleń organom ścigania. Ponadto systemy te bardzo rzadko weryfikują tożsamość osoby zakładającej konto, więc ustalenie, kto faktycznie jest właścicielem danego konta i kto dokonywał wpłaty/wypłaty środków, jest praktycznie niemożliwe. Jeden z takich systemów − Liberty Reserv − został zajęty przez organy ścigania USA w związku z ustaleniami i potwierdzeniem funkcjonowania na zasadzie prania pieniędzy w systemie. Jak wynika z ustaleń, Liberty Reserv w trakcie swojej działalności wprowadził do legalnego obrotu około 6 bilionów USD. Kolejnym sposobem jest „doładowywanie" kodami kart kredytowych lub debetowych, a następnie wykorzystywanie podstawionych osób w celu wypłaty określonych kwot pieniędzy bezpośrednio z bankomatów[9]. Ten typ działalności przestępczej ukierunkowany jest całkowicie na osiągnięcie zysku. Atak przeprowadzony na użytkowniku ma za zadanie wymusić od niego okup i wpłatę w sposób zadany przez atakującego cyberprzestępcę. W prowadzonych działaniach związanych ze zwalczaniem tego typu działalności przestępczej prowadzi się pewne zestawienia, które pokazują skalę dochodów, jakie płyną do cyberprzestępców. Oczywiście nie są to wszystkie dane, które w sposób całkowity pokazywałyby, z jakim zagrożeniem mamy do czynienia, chociażby ze względu na fakt, iż część osób płaci okup, nie informując organów ścigania czy też firm i organizacji zajmujących się bezpieczeństwem. Z prowadzonych szacunków zakłada się, iż 3% użytkowników dotkniętych atakiem ransomware płaci okup[10]. W jednej z operacji cyberprzestępcy, opisanej przez eksperta ds. bezpieczeństwa wynika, iż w jednym ataku zostało zainfekowanych 25 tys. komputerów. Ponad 800 osób z krajów UE zapłaciło okup w wysokości 70 000 euro. Biorąc pod uwagę transakcje „prania pieniędzy" wymagające dodatkowego zaangażowania podziemia cybernetycznego, tzw. underground, całkowity zysk wynosił ok. 40 000 euro[11]. Inny atak z wykorzystaniem jednej z wersji oprogramowania wykorzystywanego do wymuszenia okupu – „Reventon" – pozwolił na infekcję około 500 tys. komputerów w 18 dni. I w tym wypadku zyski cyberprzestępców musiały być znaczne. Ostatnio coraz częściej wykorzystywane w tym procederze są kryptowaluty – bitcoin. System ten oparty jest na zaufaniu do systemu wymiany peer-to-peer (P2P), gdyż bitcoinów nie emituje żaden bank i nie mają one pokrycia w żadnej walucie, kruszcu czy towarze. Sama waluta jest „kopana", czyli generowana przez komputery w wyniku wykonywania skomplikowanych operacji matematycznych dodatkowo gwarantowanych z użyciem szyfrowania. Sam system bazuje na zaufaniu użytkowników, przez co wartość bitcoina wynosi tyle, ile ludzie/użytkownicy są w stanie za niego zapłacić. Uznaje się, że twórcą (lub grupą twórców) tego systemu wirtualnej waluty jest nieznany nikomu bliżej Satoshi Nacamoto[12].

Analiza trendów i rozwoju zagrożenia

Biorąc pod uwagę łatwość dostępu do programów będących podstawą przeprowadzania ataku oraz szybkość, z jaką uzyskuje się dochody z tego typu działalności – ransomware, nie powinien dziwić fakt, iż jest to obecnie najbardziej dynamicznie rozwijająca się gałąź cyberprzestępczości.
Według szacunków producentów oprogramowania antywirusowego oraz niezależnych ekspertów istnieje duże prawdopodobieństwo utrzymania się trendu ukierunkowanych ataków na małe i duże przedsiębiorstwa oraz ich zasoby, które mogą stanowić ważny element funkcjonowania[13]. Zblokowanie dostępu do krytycznych zasobów mogłoby spowodować bardzo poważne przerwy w działalności organizacji, dlatego przestępcy, przewidując to, próbują znaleźć rozwiązanie i sposób na przeprowadzenie ataku. Dochody z takich działań na pewno będą ogromne, co potwierdzają coroczne raporty na ten temat.
Kolejny bardzo ważny obszar, na który każdy użytkownik powinien zwrócić uwagę, to wszelkie rozwiązania mobilne, zwłaszcza te pracujące na najpopularniejszych platformach systemowych – Android, iOS. Skuteczne ataki są bardzo częste, dlatego cyberprzestępcy nie będą ustawać w ciągłym podejmowaniu działań skutkujących rozwojem oprogramowania ransomware na te platformy. Przykładem może być tutaj podszywanie się cyberprzestępców pod aplikację mobilną do zabezpieczenia przed różnego rodzaju „kodem złośliwym". Pod pozorem skanowania systemu operacyjnego urządzenia i identyfikacji potencjalnych zagrożeń program po uruchomieniu blokował dostęp do urządzenia, wymuszając okup.

Z uwagi na podejmowanie działań zmierzających do odszyfrowywania plików zablokowanych kodem przez cyberprzestępców sięgają oni po bardziej skomplikowane metody szyfrowania i wykorzystują do tego szyfry oparte na krzywych eliptycznych, które pozwalają na uzyskanie bardziej skutecznego efektu szyfrowania bez możliwości skutecznego przeciwdziałania[14]. W dalszym ciągu do obsługi płatności pochodzących z ataków typu ransomware będą wykorzystywane systemy kryptowalut, bądź utrudniające identyfikację końcowego odbiorcy lub utrudniające to organom ścigania w sposób znaczny. Ponadto obecnie oprogramowanie ransomware, po zablokowaniu dostępu do komputera użytkownikowi, wykrada „czas pracy" procesora zainfekowanej stacji PC do tzw. wykopywania bitcoin-ów. Następny krok, jakiego należy się spodziewać ze strony atakujących, to przygotowanie wersji ransomware na platformy dotychczas uznawane za bezpieczne, czyli Linux bądź też platformy przemysłowe. Podobnie jak w przypadku innych zagrożeń ich ewolucja miała zbliżony przebieg. Najpierw były atakowane platformy popularne pod względem liczby użytkowników, a następnie pojawiały się wersje ataków na mniej używane platformy systemowe. Do skutecznego przeprowadzania ataków wykorzystywane są różne schematy pozwalające na wciągnięcie użytkownika w miejsce w sieci, z którego jest przeprowadzany atak. Ten sposób ewoluował od pojedynczych e-maili rozsyłanych do użytkowników, do specjalnie przygotowanych stron www, tzw. studni wody przekierowujących i infekujących komputer „koniem trojańskim". Z uwagi na wysoką skuteczność obecnych ataków z wykorzystaniem szyfrowania plików czy blokowaniem dostępu do komputera ofiary należy się spodziewać coraz wyższych kwot za odblokowanie. Obecnie zdarzają się wymuszenia sięgające ponad 1000 USD. Niejednokrotnie w przypadku ataku z wykorzystaniem oprogramowania typu ransomware „ZeroLocker" za szybką wpłatę otrzymuje się rabat w wysokości ponad 50%. Przy czym płatność może zostać zrealizowana tylko z wykorzystaniem kryptowaluty[15]. Ponadto obserwuje się przypadki bardzo agresywnych technik postępowania cyberprzestępców, które polegają na ataku ransomware z automatycznym przesyłaniem na komputer ofiary zdjęć zawierających treści związane z seksualnym wykorzystywaniem dzieci. Ma to na celu „skłonienie" ofiary do szybkiej wpłaty okupu. Często też w systemach ataku wykorzystywany jest mechanizm ograniczonego czasu przeznaczonego na dokonanie płatności (48 lub 72 h), po którym kwota ulega zwiększeniu lub kasowane są informacje wybrane losowo z dysku ofiary. Odnotowano również ataki ransomware, których celem było zablokowanie/szyfrowanie dostępu do informacji ofiary, ale efektem nie było uzyskanie okupu, lecz usunięcie danych, typowe działanie o charakterze sabotażu np. „NotPetya". Na uwagę zasługuje również fakt występowania pewnego rodzaju konfliktu pomiędzy cyberprzestępcami używającymi ransomware jako źródła dochodu oraz pozostałymi, którzy stosują bardziej dyskretne metody do uzyskiwania interesujących ich informacji, np. grupami zorganizowanymi APT (Advaced Persistent Threat). Przy skutecznym ataku wymuszającym okup użytkownik ma możliwość odtworzenia systemu, a więc usunięcia wszystkich danych wraz z systemem operacyjnym i wgrania ich ponownie na nośnik elektroniczny. Automatycznie są usuwane przy tej okazji inne programy „złośliwe". Powoduje to od pewnego czasu konflikty pomiędzy gangami cybernetycznymi[16].

PODSUMOWANIE

Działalność cyberprzestępców skupiająca się na dostarczaniu, organizowaniu, przeprowadzaniu ataków z wykorzystaniem oprogramowania typu ransomware będzie dalej ewoluować z uwagi na szybkość i skuteczność, zapewniającą efekt w postaci zablokowania/zaszyfrowania ważnych, krytycznych zasobów dla użytkownika stacji komputerowej oraz – co za tym idzie – skuteczne wymuszenie okupu, które stanowi pokaźny dochód przestępczy. Jest to obecnie jeden ze sposobów prowadzenia działań cyberprzestępczych. Stosują je grupy specjalizujące się w tego typu aktywności, które współpracują ze sobą, dzieląc się „obszarami specjalizacji" w przygotowaniu, przeprowadzeniu ataku oraz przekazaniu środków pieniężnych pochodzących od ofiar ataku, a także tzw. praniu pieniędzy w celu legalizacji ich pochodzenia. Zidentyfikowano również systemy „Rasnomware as a Service" w skrócie RaaS, na które bardzo często można się natknąć w sieci DarkNet. Polegają na oferowaniu całego pakietu oprogramowania oraz systemów wspierających takie kampanie dowolnej osobie, która wyrazi chęć infekowania w celu pozyskania środków z okupu. Podział między dostawcą systemu do ataku ransomware a wykonawcą ataków ma najczęściej proporcje 30% do 70% dochodu. Coraz częściej dochodzi również do ataków na kluczowe systemy związane z funkcjonowaniem społeczeństwa, np. szpitale, systemy transportu kolejowego, lotniczego. Efekt jest jeden – właściciel takiego systemu po prostu płaci okup, gdyż skutki braku funkcjonowania mogłyby zagrażać życiu i zdrowiu.

Użytkownicy końcowi, administratorzy, osoby odpowiadające za bezpieczeństwo powinny pamiętać o podstawowych zasadach związanych z utrzymaniem bezpieczeństwa, na które należy zwrócić szczególną uwagę. Należą do nich m.in. aktualizowanie systemu operacyjnego, dbanie o aktualizację i poprawną konfigurację oprogramowania antywirusowego. Otrzymując różnego rodzaju przesyłki e-mail, nie wolno akceptować ani uruchamiać załączników, jeżeli nie jesteśmy pewni ich pochodzenia. Na odwiedzanych stronach internetowych trzeba dokładnie czytać wyświetlane komunikaty i nie akceptować instalacji dodatkowych programów czy też aplikacji, które mogą się wyświetlać. Ponadto należy zadbać o prawidłowy przebieg organizacji oraz przeprowadzenia szkoleń dla użytkowników i uświadamiać im powagę zagrożenia, a także możliwe do realizacji schematy ataków prowadzonych przez cyberprzestępców. Szczególnie trzeba podkreślić skalę zagrożenia oraz jego skutki. Jest to oczywiście pewien zbiór tzw. dobrych praktyk, jednakże należy mieć na uwadze, iż po drugiej stronie znajdują się ludzie poszukujący zysków i ich działania nie stanowią stałego, zamkniętego zbioru schematów do realizacji, co pokazuje analiza zagrożenia, jak również aktualne doniesienia od firm, organizacji, instytucji zajmujących się bezpieczeństwem teleinformatycznym.

Jednocześnie rozwój tego zagrożenia stawia przed organami ścigania nowe wyzwania powodujące konieczność stałego monitorowania i podejmowania wysiłków na rzecz skutecznego zwalczania i eliminowania przestępców. Jednym z głównych wyznaczników skutecznej współpracy jest podejmowanie wspólnych działań na poziomie międzynarodowym z wykorzystaniem Europolu oraz Interpolu[17] oraz przy dużym wsparciu i współpracy ze strony dostawców internetowych oraz producentów oprogramowania, bez których walka z cyberprzestępcami byłaby niemożliwa bądź znacznie utrudniona. Obecnie Centrum Zwalczania Cyberprzestępczości – EC3 przy Europolu może wskazać kilka spraw o zasięgu międzynarodowym związanych z wymuszaniem okupu w sieci Internet, które dzięki współpracy organów ścigania z różnych krajów zakończyły się sukcesem – ujęciem sprawców organizatorów całego procederu. Oczywiście nie eliminuje to całego zagrożenia, nie spowoduje to zaprzestania występowania zagrożenia ransomware w sieci, ale pokazuje, jak skuteczna może być działalność policji oraz współpracujących partnerów w walce z cyberprzestępcami. Ponadto przy wsparciu Europolu EC3 – powstał projekt „No More Ransom", z własną stroną internetową, na której możemy znaleźć m.in. oprogramowanie deszyfrujące, pozwalające na odzyskanie danych i informacji bez konieczności opłacania wysokich kwot okupu cyberprzestępcom.

[1] *Police Ransomware. Threat Assessment*, Europol, 2014, s. 6.
[2] *Trend Micro Incorporated, Police Ransomware Update*, 2012, s. 1.
[3] W bezpieczeństwie teleinformatycznym zestaw metod mających na celu uzyskanie niejawnych informacji przez cyberprzestępcę. Zob. *Inżynieria społeczna*, w: *Wikipedia*, http://pl.wikipedia.org/wiki/Inżynieria_społeczna_(informatyka) [dostęp: 30.11.2017 r.].
[4] Szyfrowanie asymetryczne – szyfrowanie z wykorzystaniem klucza publicznego oraz prywatnego.
[5] Ransomware/cryptolocker, https://suport.kaspersky.com [dostęp: 30.11.2017 r.].
[6] Koń trojański – określenie oprogramowania, które podszywając się pod przydatne lub ciekawe dla użytkownika aplikacje, dodatkowo implementuje niepożądane, ukryte przed użytkownikiem różne funkcje. Zob. *Koń trojański*, w: *Wikipedia*, https://pl.wikipedia.org/wiki/Koń_trojański_(informatyka) [dostęp: 30.11.2017 r.].
[7] *Watering hole attack*, w: *Wikipedia*, http://en.wikipedia.org/wiki/Watering_hole_attack [dostęp: 10.10.2017].
[8] Exploit – złośliwe oprogramowanie wykorzystujące luki programistyczne lub innych podatności w celu przejęcia kontroli nad sprzętem komputerowym lub innym urządzeniem elektronicznym, zob. M. Sawicki, *Cyberprzestępczość*, C.H. Beck, s. 96.
[9] *Police Ransomware threat assessment*, Europol, 2014, s. 11.
[10] Raport: Symantec, *Ransomware: A Growing Menace*, 2012.
[11] http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation.
[12] *Bitcoin*, w: *Wikipedia*, https://pl.wikipedia.org/wiki/Bitcoin [dostęp 10.10.2017].
[13] *Police Ransomware a Threat Assessment*, Europol, 2014, s. 12.
[14] *Kryptografia krzywych eliptycznych*, w: *Wikipedia*, https://pl.wikipedia.org/wiki/Kryptografia_krzywych_eliptycznych.
[15] http://www.zdnet.com/new-zerolocker-crypto-ransomware-offers-discount-for-paying-up-quickly-or-1000-in-bitcoin-7000032779/?utm_source=dlvr.it&utm_medium=twitter#ftag=RSS86a1aa4.
[16] *Ransomware: A Growing Menace* – Symantec 2012, s. 10.
[17] Interpol ICPO – International Criminal Police Organisation, www.interpol.int.

Literatura

Siwicki M., *Cyberprzestępczość*, C.H. Beck, Warszawa 2013.
Ransomware: a growing meanance – Symentec, 2012.
Police Ransomware. Threat Assessment, Europol, 2014.
Trend Micro Incorporated, Police Ransomware Update, 2012.

Netografia

Bitcoin, w: *Wikipedia*, https://pl.wikipedia.org/wiki/Bitcoin.
Interpol ICPO – International Criminal Police Organisation, www.interpol.int.
Inżynieria społeczna, w: *Wikipedia*, http://pl.wikipedia.org/wiki/Inżynieria_społeczna_(informatyka).
Kryptografia krzywych eliptycznych, w: *Wikipedia*, https://pl.wikipedia.org/wiki/Kryptografia_krzywych_eliptycznych.
http://krebsonsecurity.com/2012/08/inside-a-reveton-ransomware-operation.
Koń trojański, w: *Wikipedia*, https://pl.wikipedia.org/wiki/Koń_trojański_(informatyka).
http://www.zdnet.com/new-zerolocker-crypto-ransomware-offers-discount-for-paying-up-quickly-or-1000-in-bitcoin-7000032779/?utm_source=dlvr.it&utm_medium=twitter#ftag=RSS86a1aa4Ransomware/cryptolocker, https://suport.kaspersky.com.
Watering hole attack, w: *Wikipedia*, http://en.wikipedia.org/wiki/Watering_hole_attack.

Summary

Ransomware – forcing ransom in the network

In recent years we experienced the intensive growth of attacks with the use of malicious Ransomware* extorting the ransom. Cybercriminals in a very short time released more and more blocking programs, from one version to another more advanced in methods of blocking the access – up to the use of cryptographic elliptical algorithms encrypting information/data.
In 2017 a ransomware software, attacking information resources of companies, develops dynamically. NotPetya or WannaCry are only some of varieties of this very dangerous software. Its inserting it into the company network can effectively block the operation of the enterprise till the moment the ransom is paid. However about 75% of such attacks does not end so well. The purpose of NotPetya/Expetya – as it turns out after analyses – is the destruction of data rather than the extortion of ransom.
Since the beginning of the appearance of Ransomware attacks we can observe not only a development of the very software, but also attack vectors. In the nearest future one should not expect weakening of these very attacks, but it is necessary to consider new vulnerabilities, attack vectors and the fact that everyone can become a target of the attack. Therefore it is worth to disseminate the knowledge about Ransomware.

* program blocking of the access to the information using the cryptography and ransom demands

Tłumaczenie: Renata Cedro

OSZUSTWA NIGERYJSKIE – próba klasyfikacji

nadkom. Marcin Siwiecki

ekspert Wydziału ds. Odzyskiwania Mienia
Biura Kryminalnego KGP

Absolwent Akademii Górniczo-Hutniczej im. St. Staszica w Krakowie,
były zastępca naczelnika Wydziału dw. z Cyberprzestępczością
Biura Służby Kryminalnej Komendy Głównej Policji

Niniejszy artykuł stanowi próbę usystematyzowania i klasyfikacji bardzo szerokiej i ciekawej grupy przestępstw funkcjonującej pod wspólną nazwą „oszustw nigeryjskich", której na „drugie życie" w nowej i potężniejszej formie pozwolił rozwój Internetu. „Oszustwa nigeryjskie" to zjawisko tak rozpowszechnione, że chyba każdy z nim się spotkał, ale warto o nim od czasu do czasu profilaktycznie przypomnieć, gdyż nadal znajdują się ludzie, którzy padają jego ofiarami.

Oszustwo nigeryjskie lub nigeryjski szwindel (inaczej – afrykański szwindel, z ang. *Nigerian scam*, *419 scam* – ta ostatnia nazwa wywodzi się od artykułu w kodeksie karnym Nigerii, dotyczącym tego przestępstwa) jest to prosty proceder przestępczy – oszustwo, wręcz naiwne, najczęściej zapoczątkowane kontaktem poprzez wykorzystanie poczty elektronicznej. Polega na wciągnięciu (dawniej – przypadkowej, obecnie – coraz częściej typowanej) ofiary w grę psychologiczną, której fabuła jest oparta na fikcyjnym transferze dużej kwoty pieniędzy (często przesadnie wygórowanej – nawet rzędu kilkunastu milionów funtów lub dolarów amerykańskich), z jednego z krajów afrykańskich (najczęściej Nigerii, choć aktualnie może również chodzić o każdy inny kraj – coraz częściej w grę wchodzi Wielka Brytania, Hiszpania) – mającą na celu wyłudzenie pieniędzy od ofiary zaślepionej wizją zbliżającej się fortuny. Przestępstwo to, przeżywające swoją drugą młodość dzięki wszechobecnemu Internetowi, mało ma wspólnego z cyberprzestępczością i zaawansowanymi technologiami. Wykorzystuje głównie socjotechnikę i aż jest niewiarygodne, że ktoś może paść jego ofiarą – przy całej jego prostocie i braku najmniejszego elementu finezji.

Na arenie międzynarodowej powyższą problematykę, nieprzerwanie od ok. połowy lat 90. ubiegłego wieku, bada U.S. Secret Service[1], ale nawet ta służba stoi na stanowisku, że odzyskanie pieniędzy jest praktycznie niemożliwe. Jednak nadal zwraca się z prośbą o przesyłanie, przez pokrzywdzonych takimi przestępstwami, wszelkich informacji otrzymywanych przez oszustów na adres:

The United States Secret Service,
Financial Crimes Division,
950 H Street, NW, Washington, D.C. 20223.

Na gruncie prawa polskiego tego rodzaju przestępstwo zostało spenalizowane w przepisie art. 286 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2017 r. poz. 2204).

„Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania (…)"[2]. Przestępstwo to jest zagrożone karą pozbawienia wolności od 6 miesięcy do 8 lat.

Niestety wykrywalność sprawców tego rodzaju przestępstw jest znikoma, co może być również wynikiem niezadowalającej jakości współpracy z nigeryjskimi organami ścigania. Sytuacja ta pozwala na dużą swobodę działań przestępczych, do tego stopnia, że oszuści dokonujący tego typu czynów niejednokrotnie nawet nie używają narzędzi do ukrywania swojego prawdziwego adresu IP. Z drugiej strony – brak kamuflowania

adresu IP może mieć pozytywne aspekty dla pozostałych użytkowników Internetu, ponieważ często ułatwia to dokonywanie sprawdzeń źródłowego adresu IP otrzymywanej korespondencji dotyczącej oszustw nigeryjskich. Takie sprawdzenia mogą być realizowane np. w serwisach umożliwiających ustalenie miejsca, skąd trafił do nas e-mail, poprzez tzw. serwery „WHOIS Database". W większości przypadków efektem tych poszukiwań jest informacja, że sprawdzany adres IP należy do puli administrowanej z Nigerii, Wybrzeża Kości Słoniowej czy innego zbliżonego geograficznie afrykańskiego państwa.
Wszystko rozpoczyna się od niespodziewanej korespondencji, najczęściej rozesłanej do wielu odbiorców, która ma zainteresować ofiarę możliwością osiągnięcia milionowej fortuny... Poniżej zamieszczono autentyczny „list nigeryjski" (z zachowaną oryginalną pisownią), który krążył po sieci w lipcu i sierpniu 2014 r. i nie różni się od tego typu korespondencji istniejącej w Internecie od ponad dwudziestu lat.

„22 sie 2014 15:46 „Dr. Fredrick Wright" <dr.fredw@hotmail.com> napisał(a):

Witaj przyjacielu,

Jestem dr Fryderyk Wright Przewodniczący Komitetu Audytu grupy Royal Bank of Scotland Plc. Piccadilly Circus w Londynie, w Anglii. Piszę wniosek biznesu będzie acerca To miało ogromne wzajemne korzyści i dla nas obu. To może Cię zainteresować wiedzieć, że w moim departamencie, odkryłem sumę 18,5 mln funtów (osiemnaście milionów pięćset tysięcy Great British Pounds Sterling) na koncie należącym do jednego z naszych zagranicznych klientów Późno Pan John Lambert, amerykański Biznes Mogul, który był ofiarą katastrofie lotniczej w 2012 roku, zabijając go i członków jego rodziny. John Lambert 44, Springfield, i Robin Melton, 46 Ozark, zmarł 2002 Cirrus SR22 Kiedy rozbił się na polu w pobliżu skrzyżowania Farm Road 81 i Missouri 123 Również w płaszczyźnie w momencie katastrofy były Lamberta troje dzieci – McKinley 15; Joshua Grayson 16 i 10; żałujemy wielką stratę.

Jednak wybór kontaktu z tobą budzi z charakter geograficzny, gdzie mieszkasz, w szczególności ze względu na wrażliwość transakcji i poufność w niniejszym dokumencie. Teraz nasz bank-czeka na którykolwiek z krewnymi, aby się-up do roszczenia, bez sukcesu w ciągu roku. Osobiście bezskutecznie lokalizowanie krewnych; Szukam Twojej zgody, aby zaprezentować Państwu jak najbliższych krewnych / Will Beneficjenta do zmarłego tak, że wpływy z tego konta wyceniono na 18,5 mln funtów Great British Pounds Sterling może być wypłacona / Przeniesione do Ciebie tak nazwany najbliższych krewnych / beneficjenta.

To będzie wypłacane lub udostępniane w procentach w oryginalny, 60% do 40% mnie i dla Ciebie. Mam zabezpieczone wszystkie niezbędne dokumenty prawne, które mogą być wykorzystane do wykonania kopii zapasowej tego twierdzenia. All I need to wypełnić swoje nazwiska do dokumentów i zalegalizować go w sądzie, aby udowodnić Ci za prawowitego beneficjenta. All I wymagają teraz jest uczciwy współpracy, poufności i zaufania w celu umożliwienia nam patrz poprzez tę transakcję. Gwarantuję, że będzie to wykonane zgodnie z ambitami prawa i zgodnie z prawem rozwiązanie zabezpieczenia, które będzie chronić komputer z wszelkich przypadków naruszenia prawa.

Proszę dostarczyć mi następujące, jak mamy informacji siedmiu (7) dni, aby uruchomić to przez. To jest bardzo pilne PLEASE.

1 Imię i nazwisko:
2 Bezpośredni Telefon Numer:
3 Twój adres kontaktowy:
4 Zawód:
5 Wiek:
6 Płeć:
7 Narodowość:

Po przejściu przez metodyczne wyszukiwania, postanowiłem skontaktować się z Tobą nadzieję, że „Ta propozycja znajdzie interesujące. Proszę na potwierdzenie tej wiadomości i wskazując zainteresowanie będę dostarczyć Państwu więcej informacji.

Starają się dać mi znać swojej decyzji zamiast trzymać mnie czeka.

Dziękując w oczekiwaniu na swojego pozytywnego i pozytywnej odpowiedzi.

Z poważaniem,
Dr Fryderyk Wright

Prosta, wręcz naiwna forma i fabuła, język wskazujący na wykorzystanie internetowego translatora, niedorzecznie wysoka kwota pieniędzy, adres nadawcy umiejscowiony na darmowym serwerze poczty elektronicznej – to podstawowe cechy listu nigeryjskiego. Istnieje jeszcze jeden niebezpieczny element – usiłowanie wyłudzenia danych osobowych, które służą głównie „opracowaniu" ofiary celem podjęcia z nią gry psychologicznej. Jednakże należy pamiętać, iż takie dane mogą zostać użyte w bardziej niebezpieczny sposób, a mianowicie – mogą posłużyć budowaniu fałszywych tożsamości, być źródłem kolejnych oszustw lub szantaży. Taką wiadomość należy usuwać przed jej przeczytaniem![3]

Najczęściej spotykane odmiany oszustw nigeryjskich

TRADYCYJNA – uchodźca polityczny z Czarnego Lądu

Przestępca kontaktuje się z ofiarą, najczęściej wykorzystując do tego pocztę elektroniczną, rzadziej – łączność telefoniczną. W korespondencji pada propozycja zyskania znacznej kwoty pieniędzy, części fortuny, jaką posiada (czy też odziedziczył) oszust, ale której sam nie może podjąć z banku z różnych przyczyn. Znamienne jest to, iż poziom języka angielskiego, ale częściej języka rodzimego, w którym sprawcy najczęściej się komunikują, jest bardzo niski. Na wczesnym etapie rozwoju tego rodzaju przestępczości oszust najczęściej podawał się za uchodźcę politycznego, dziedzica fortuny utraconej w trakcie przewrotu politycznego, syna obalonego przywódcy jednego

z państw afrykańskich. Kwoty wskazywane w korespondencji oscylują w granicach 20–30 mln USD, a oszust, w zamian za pomoc w jej odzyskaniu, ofiaruje nawet ponad połowę tej kwoty. „Pomoc" ta wiąże się z realnym finansowaniem (oscylującym w granicach kilkuset lub kilku tysięcy USD, funtów brytyjskich czy euro) przez ofiarę kolejnych kroków, jakie oszust musi czynić, by sfinalizować rzekomy przelew majątku na konto wskazane przez ofiarę.

Z sukcesywnie otrzymywanej korespondencji ofiara stopniowo się dowiaduje, że oszust musi np. zarejestrować działalność gospodarczą, posłużyć się kilkoma łapówkami, by przekupić bankierów, skorumpowanych policjantów lub innych urzędników państwowych w jego kraju, lub musi opłacić procedurę wystawienia certyfikatów poświadczających, że pieniądze nie pochodzą z nielegalnego źródła (np. z działalności terrorystycznej lub handlu narkotykami), bo w przeciwnym wypadku przelew zostanie zablokowany itp. Ofiara, która już widzi siebie jako milionera, pokrywa kolejne koszty związane z finalizowaniem całej operacji. Pieniądze przejmuje tylko oszust, który od czasu do czasu uwiarygadnia fabułę oszustwa, przesyłając pocztą elektroniczną kiepsko spreparowane (z wykorzystaniem popularnych edytorów graficznych) certyfikaty, kopie potwierdzeń przelewów itp. W tym momencie rozpoczyna się gra, która ma na celu jak najdłuższe zwodzenie ofiary i wyłudzenie jak najwięcej pieniędzy. Zazwyczaj ofiara na tym etapie zaczyna podejrzewać oszustwo i w pewnym momencie przestaje płacić. Oszust jednak osiągnął zamierzony cel – praktycznie już po otrzymaniu pierwszej wpłaty. Gdy ofiara przerywa finansowanie oszusta, często dochodzi do gróźb, zmiany fabuły gry, oszust teraz może się podawać za inną osobę, ale są to tylko próby wyłudzenia kolejnej kwoty.

SPADEK – najbardziej wyrafinowana wersja oszustwa nigeryjskiego

W ostatnich latach pojawiła się znacznie bardziej zaawansowana odmiana oszustwa nigeryjskiego. Stanowi formę przestępstwa, które jest najprawdopodobniej długo wcześniej zaplanowane, starannie przygotowane, a ofiary są typowane w przemyślany sposób, a nie wybierane losowo lub „atakowane" drogą elektroniczną w sposób zmasowany.

Modus operandi sprawców nie jest jeszcze do końca poznany, jednak pewna powtarzalność w wielu już przypadkach pozwala na sformułowanie ramowego mechanizmu działania oszustów.

Pierwszy kontakt z wytypowaną ofiarą ma sprawiać u niej wrażenie zupełnie przypadkowego. Może to być nieplanowane spotkanie z osobą, która twierdzi, że nosi takie samo nazwisko jak ofiara (bądź nazwisko panieńskie matki ofiary) lub zna kogoś, kto mógł należeć do rodziny ofiary, którą rozdzieliły losy związane np. z zawieruchą wojenną. Scenariuszy może być wiele. Chodzi tylko o to, by w pamięci ofiary utkwił fakt, że gdzieś za granicą żyje ktoś, kto należy do jej rodziny, wie o istnieniu ofiary, mimo że nie utrzymuje stałego kontaktu.

Zazwyczaj właśnie wtedy oszuści zamieszczają taki kontakt w swojej bazie danych potencjalnych ofiar. Teraz śledzą wszystkie informacje, które mogą świadczyć o nagłej śmierci (katastrofa komunikacyjna, pożar lub trzęsienie ziemi itp.) osoby o takim samym nazwisku jak potencjalna wytypowana ofiara oszustwa.

Następnie przestępca kontaktuje się z ofiarą, najczęściej wykorzystując do tego pocztę elektroniczną, rzadziej – telefonicznie. W korespondencji informuje potencjalną ofiarę, że jest jedynym żyjącym spadkobiercą dalekiego krewnego, który niedawno stracił życie, np. w katastrofie lotniczej (dane te najczęściej są ogólnie dostępne, np. w Internecie), i nie pozostawił potomstwa, a swój ogromny majątek postanowił przekazać w testamencie jedynemu znanemu krewnemu, czyli wytypowanej już wcześniej ofierze oszustwa. Fortunę, jaką odziedziczyła ofiara, może podjąć z banku po dopełnieniu kilku formalności i opłaceniu należności, które jednak są niczym w porównaniu z olbrzymim spadkiem. Co typowe – w tej formie oszustwa nigeryjskiego język angielski, w którym jest prowadzona korespondencja – charakteryzuje się wyższym poziomem niż w przypadku tradycyjnych oszustw nigeryjskich. Ofiara zaczyna, na polecenie oszusta, który najczęściej podaje się za prawnika bądź bankiera, finansowanie, z wykorzystaniem kwot oscylujących w granicach kilkuset do kilku tysięcy USD (euro), kolejnych wydatków, jakie muszą być poczynione, by sfinalizować przelew majątku na konto „spadkobiercy". Ze stale napływającej korespondencji ofiara dowiaduje się, że musi opłacić procedurę wystawienia certyfikatów przez bank, poświadczających, że pieniądze nie pochodzą z nielegalnego źródła, gdyż kwota jest ogromna, a w przeciwnym wypadku przelew może zostać zablokowany z różnych przyczyn itp. Oszuści uwiarygodniają całą historię, przesyłając pocztą elektroniczną spreparowane certyfikaty, kopie potwierdzeń przelewów itp. Również w tym przypadku, analogicznie jak w innych odmianach oszustwa nigeryjskiego, rozpoczyna się gra na czas, która ma na celu jak najdłuższe zwodzenie ofiary i wyłudzenie jak najwięcej pieniędzy. Jest więcej niż pewne, że zamiast zyskać fortunę, ofiara sukcesywnie będzie traciła znaczne kwoty pieniędzy, dopóki się nie zorientuje, iż padła ofiarą poczynań oszusta.

KONTO W BANKU BEZ WŁAŚCICIELA

Przestępca, udając najczęściej pracownika banku, kontaktuje się z wytypowaną ofiarą, wykorzystując do tego w pierwszej fazie wyłącznie pocztę elektroniczną. Potencjalna ofiara jest informowana, że jeden z klientów banku zmarł lub zginął w tragicznym wypadku i pozostawił po sobie konto z ogromną sumą pieniędzy, nie wskazując lub nie mając spadkobierców. Bank w sytuacji długoletniej niemożności ustalenia kręgu spadkobierców podjął decyzję o likwidacji „martwego konta" (tj. konta, na którym od dłuższego czasu nie odnotowano żadnej aktywności) i szuka kogoś, kto przejmie jego zawartość. By uprawdopodobnić całą sytuację, oszust śledzi doniesienia mediów o katastrofach w ruchu powietrznym lub morskim, sprawdzając przy tym listę nazwisk tragicznie zmarłych pasażerów, po czym wyszukuje w Internecie osób noszących takie nazwiska. Wydaje się, iż to jest najmniej prawdopodobna wersja przestępstwa nigeryjskiego.

Po wyrażeniu zainteresowania przez ofiarę oszust przysyła kolejną część (bardziej szczegółową) historii. Pojawiają się dokumenty, wytworzone nieudolnie i w kiepskiej jakości graficznej, przesyłane drogą elektroniczną, potwierdzające istnienie przedmiotowego konta należącego do zmarłego milionera. Niewykluczony jest również kontakt telefoniczny. Do całej operacji są włączane kolejne osoby, które mają uwiarygodnić całą historię – dyrektor banku, prawnik lub jeszcze jakiś inny urzędnik, który jest władny wystawiać lub uwiarygodniać dokumenty w przedmiotowej sprawie. Na tym etapie pojawiają się pierwsze informacje dotyczące tego, że ofiara będzie musiała sfinansować kilka „pomniejszych" przedsięwzięć, by w rezultacie mogła przejąć miliony. Pojawiają się np. opłaty za wystawienie certyfikatów przez bank lub inne urzędy,

poświadczających, że pieniądze nie pochodzą z nielegalnego źródła, za usługi prawników oraz koszty operacyjne banku. Oszust podtrzymuje korespondencję, prosząc o kolejne wpłaty tak długo, jak pozwala na to naiwność ofiary.
Zarówno miliony na koncie, jak i to, że informacja pochodzi z banku, są oczywiście fikcją. Nazwiska pracowników banku mogą być prawdziwe, gdyż przeważnie stanowią dane ogólnie dostępne w Internecie. Należy jednak zwrócić uwagę na numery telefonów, których nie można znaleźć w informacjach kontaktowych prawdziwego banku, a adresy e-mail używane przez oszustów często należą do puli adresów serwerów oferujących bezpłatną rejestrację konta poczty elektronicznej, np. Yahoo, Google (Gmail) lub Hotmail.

WYGRANA NA LOTERII

Potencjalna ofiara otrzymuje pocztą elektroniczną spreparowaną wiadomość o wygranej bardzo dużej sumy pieniędzy w jednej z (narodowych) loterii któregoś z europejskich krajów (najczęstsze przypadki to podszywanie się pod loterie hiszpańskie). Do powyższej informacji są załączone certyfikaty (wykonane prostymi narzędziami graficznymi) uprawdopodobniające wygraną oraz istnienie samej loterii. Kwoty są znacznie niższe niż w klasycznym oszustwie nigeryjskim, by bardziej korelowały z wysokościami wygranych na tego typu loteriach. Oszust – by rozwiać wszelkie podejrzenia ofiary − twierdzi, że nagrodę można odebrać osobiście, i podaje dokładny adres oraz telefony kontaktowe. Mało kto decyduje się na coś więcej niż zatelefonowanie, by uwiarygodnić „swoje szczęście". Ofiara, w znakomitej większości przypadków, postanawia więc przyjąć wygraną międzynarodowym przelewem bankowym. Na tym etapie pojawiają się pierwsze opłaty, które jest zobowiązana uiścić, by móc odebrać nagrodę – dla prawnika, za wystawienie kilku nieznanego pochodzenia wewnętrznych dokumentów banku i certyfikatów, opłacenie podatku od wzbogacenia włącznie. Żadna wygrana nie istnieje, a oszust podtrzymuje kontakt tak długo, jak długo ofiara deklaruje kolejne wpłaty.
Charakterystyczne dla tego rodzaju przestępstw jest to, iż oszuści nie obstają przy ścisłych kwotach, jakie należy uiszczać za poszczególne operacje, co byłoby przecież niemożliwe w wypadku konieczności uiszczania opłat przy prawdziwych operacjach bankowych lub podatkowych. Częstokroć ofiara informuje, że obecnie posiada tylko część wymaganej kwoty. Wtedy oszust „wspomaga" ofiarę, wnosząc resztę opłat z własnych środków, które ofiara ma zwrócić w późniejszym terminie. Pozorne działania wspierające utwierdzają ofiarę w przekonaniu o dobrych intencjach kontrahenta, a ponadto wywołują przeświadczenie, iż jest on gwarantem płynnego przeprowadzenia całej procedury.
We właściwym momencie, w celu wzmocnienia przekonania o prawdziwości i rzetelności całego przedsięwzięcia, oszust wysyła pocztą tradycyjną, nie tylko elektroniczną, kolorowe certyfikaty i fałszywe potwierdzenia przyjęcia przez różne instytucje i banki opłat od ofiary. Pieniądze giną gdzieś na Czarnym Lądzie.

INWESTOR

Jest to metoda bardzo zbliżona do metody „tradycyjnej". Przestępca kontaktuje się z ofiarą głównie z wykorzystaniem poczty elektronicznej. Oszust najczęściej podaje się za młodego, wykształconego człowieka, któremu udało się „wybić" w rodzinnym kraju (prawnik, student, modelka), natomiast jego ojciec lub przyjaciel posiada ogromny majątek, który chce zainwestować, lecz z różnych przyczyn sam nie może tego uczynić. Ofiara ma pomóc w inwestowaniu w swoim rodzimym kraju pieniędzy, które zostaną mu powierzone przez oszusta. Należy nadmienić, iż podobnie jak w poprzednim przypadku, poziom języka (sporadycznie już używany język angielski) jest bardzo niski, a wiadomości otrzymywane w języku polskim stanowią tłumaczenie wykonane za pomocą komputerowego translatora, z dużą liczbą błędów. Dalszy przebieg działań jest zbliżony lub analogiczny do wskazanego w poprzednim modelu.

AUKCJA INTERNETOWA

Oszustwa nigeryjskie stale ewoluują, a oszuści szukają ciągle nowych sposobów wyłudzenia pieniędzy. Coraz częściej wykorzystują do tego celu popularne aukcje internetowe; w Polsce tego rodzaju oszustwa zostały popełnione z użyciem portalu aukcyjnego Allegro.pl.
Tym razem ofiara jest wyszukiwana na portalu aukcyjnym, na którym wystawia jakiś wartościowy przedmiot, np. sprzęt elektroniczny – laptop lub sprzęt fotograficzny. Wielokrotnie, co dziwne – były to suknie ślubne. Kontakt pocztą elektroniczną nawiązuje oszust sprawiający wrażenie bardzo zainteresowanego zakupem oferowanego przez ofiarę towaru, który najczęściej ma stanowić jakiś okazjonalny prezent dla bliskiej osoby przebywającej w innym kraju niż oszust, np. w Wielkiej Brytanii.
Oszustowi bardzo zależy na czasie wysyłki, który ma być jak najkrótszy, gdyż prezent musi dotrzeć w konkretnym terminie, więc sprzedaż musi się odbyć poza aukcją, jeżeli nie można zakończyć transakcji za pomocą opcji „kup teraz". Oszust takie niedogodności chce zrekompensować nawet dwukrotnie wyższą kwotą niż żąda sprzedający, który staje się nieświadomą ofiarą.
Oszuści wykorzystują prostą socjotechnikę, kierując się inteligencją emocjonalną i licząc na chciwość potencjalnych ofiar. Wielu sprzedających zgadza się wysłać towar oczywiście po otrzymaniu zapłaty. Tu pojawia się charakterystyczny dla tego rodzaju oszustwa sposób działania sprawcy. Po zakończeniu transakcji, najczęściej drogą elektroniczną, ofiara otrzymuje spreparowany skan potwierdzenia dokonania przelewu bankowego zza granicy, wraz z komentarzem, iż pieniądze z Afryki są przelewane kilka dni, a prezent musi dojść niezwłocznie. Często wpłata ma się odbywać za pośrednictwem takich systemów płatności, jak Bidpay, Money Gram, Western Union. Oszust prosi, by ofiara zawierzyła skanowi potwierdzenia dokonania przelewu i wysłała towar. Zazwyczaj sprzedający godzi się na taki obrót wydarzeń, natomiast w przeciwnym wypadku jest straszony złamaniem umowy, oskarżany o oszustwo, a w skrajnych przypadkach jest straszony nawet zgłoszeniem sprawy do Interpolu.
Podczas każdej innej transakcji z opcją „wpłata na konto bankowe" należy przestrzegać podstawowej zasady – towar wysyła się wyłącznie dopiero po zaksięgowaniu pełnej kwoty na koncie bankowym, w przeciwnym razie nieświadoma ofiara traci towar wystawiany na aukcji.

METODA „WASH-WASH"

Przestępca, podając się najczęściej za pracownika prywatnej firmy, która weszła w posiadanie dużej ilości chemicznie zabezpieczonych banknotów (pokrytych substancją chemiczną, farbą, proszkiem itp.), kontaktuje się z wytypowaną ofiarą, wykorzystując do tego pocztę elektroniczną lub bezpośredni kontakt. Potencjalna ofiara jest informowana, że jakiś czas

temu firma otrzymała zlecenie wykonania pewnej czynności z oznaczonymi banknotami – może to być np. zlecenie przygotowania specjalistycznego opakowania banknotów lub choćby dokonania renowacji czy czyszczenia banknotów, jednak przed odebraniem banknotów urwał się kontakt ze zleceniodawcą. Zresztą fabuła wprowadzająca może być różna i zależy tylko od inwencji twórczej oszusta.

Oszust, w sytuacji wielomiesięcznej niemożności ustalenia właściciela gotówki, nawiązuje kontakt z ofiarą w większości przypadków na jeden z dwóch sposobów – „losowy atak masowy" do wielu odbiorców poprzez e-mail lub typowanie ofiary na podstawie prowadzonego „białego wywiadu" (zbierania wszystkich informacji o potencjalnej ofierze z ogólnie dostępnych źródeł – publikacji internetowych, wydarzeń w lokalnych społecznościach – szkołach, stowarzyszeniach, bractwach, portali społecznościowych, portali randkowych, portali aukcyjnych i ogłoszeniowych itp.), łącznie z obserwacją w przypadku kontaktu bezpośredniego. Kontakt bezpośredni odbywa się najczęściej w środowisku pozwalającym na kilkudniową obserwację potencjalnej ofiary, jej zachowań, nawyków, stylu życia itp. Zwykle takimi miejscami są np. hotele turystyczne, ośrodki wczasowe, kasyna.

Po wyrażeniu zainteresowania przez ofiarę oszust dokonuje prezentacji zabarwionych banknotów, które najczęściej są zaczernionymi kserokopiami dolarów amerykańskich lub wręcz czarnym papierem, jedynie wymiarami odpowiadającym banknotowi amerykańskiego dolara.

Oszust informuje, że jest obecnie w bardzo trudnej sytuacji finansowej i chętnie odsprzeda ofierze walizkę z farbowanymi dolarami (ostatnio coraz częściej mowa też o banknotach euro) za kwotę nawet piętnastokrotnie niższą niż wynosi nominalna wartość banknotów, jednak wcześniej należy je odbarwić – wyczyścić (stąd nazwa metody – z jęz. ang. *wash* – mycie, pranie). Za środek chemiczny, który jest bardzo drogi i trudno go kupić, ma oczywiście zapłacić ofiara – i to stanowi *clue* sprawy. Cena środka chemicznego może wynieść nawet 50 000 euro, ale może być też „płynna" – jak opłaty w innych oszustwach nigeryjskich – czyli oszust „zejdzie" do każdej kwoty, jaką może zapłacić ofiara. Ofiara również może w dalszej kolejności otrzymać wiadomość od firmy dostarczającej taki środek chemiczny, znalezionej przez oszusta, by bardziej uwiarygodnić całą sytuację. Jak nietrudno się domyślić, zarówno firmą dostarczającą środek, jak i dysponentem „zafarbowanych" banknotów jest jeden i ten sam oszust.

UDZIAŁ W KONFERENCJI NAUKOWEJ

Przestępca, udając najczęściej pracownika instytucji naukowo-badawczej, kontaktuje się z wytypowaną ofiarą, którą łatwo wybiera poprzez ogólnodostępne w Internecie publikacje, sprawozdania z sympozjów i konferencji, wykorzystując do tego w pierwszej fazie wyłącznie pocztę elektroniczną. Potencjalna ofiara jest powiadamiana, że jako wybitny i znany naukowiec, specjalista w swojej dziedzinie, jest zapraszana na organizowaną wkrótce konferencję naukową, która rzeczywiście ma się odbyć (a przestępcy podają się za jej współorganizatora) i nie ma problemu ze znalezieniem informacji o tym wydarzeniu w Internecie.

Po wyrażeniu zainteresowania udziału w konferencji przez ofiarę oszust przysyła kolejną część (bardziej szczegółową) informacji, łącznie z agendą konferencji. Pojawiają się dokumenty, wytworzone nieudolnie i w kiepskiej jakości, przesyłane drogą elektroniczną, potwierdzające istnienie przedmiotowego zdarzenia oraz mające na celu uwiarygodnić przestępcę jako pracownika naukowego jakiejś realnie istniejącej instytucji naukowej. Na tym etapie jest niewykluczony również kontakt telefoniczny. Pojawiają się także pierwsze informacje dotyczące tego, że ofiara będzie musiała dokonać nieznacznej wpłaty, by w rezultacie mogła wziąć udział w konferencji. Wpisowe jest niewygórowane, kwota oscyluje w granicach 50–100 dolarów. Oszust podtrzymuje korespondencję, prosząc o kolejne wpłaty tak długo, jak pozwala na to naiwność ofiary. Prośby dotyczą uregulowania drobnych opłat hotelowych, opłat na finansowanie publikacji czy opłat za wpisane w agendę wycieczki po muzeach itp.

Nazwiska pojawiające się w agendzie uczestników konferencji mogą być prawdziwe, gdyż przeważnie są to dane ogólnie dostępne w Internecie. Często też po zweryfikowaniu informacji w Internecie okazuje się, że taka konferencja odbyła się wcześniej. Należy jednak zwrócić uwagę na numery telefonów, których nie można znaleźć w informacjach kontaktowych prawdziwej instytucji badawczej lub organizatora konferencji, a adresy e-mail używane przez oszustów często należą do puli adresów serwerów oferujących bezpłatną rejestrację konta poczty elektronicznej, tj. np. Yahoo, Google (Gmail) czy Hotmail.

LOTERIA WIZOWA

Potencjalna ofiara otrzymuje pocztą elektroniczną spreparowaną wiadomość o wytypowaniu swojej osoby w loterii wizowej, głównie organizowanej przez Stany Zjednoczone. Powyższa wiadomość jest opatrzona szatą graficzną wykonaną w miarę profesjonalny sposób, potwierdzający jej prawdziwość.

Mechanizm samego oszustwa jest bardzo prosty. Wytypowana ofiara, która nieświadoma zagrożeń szukała wcześniej informacji o sposobie uzyskania wizy wjazdowej do USA, podała na stronie internetowej swój adres poczty elektronicznej jako warunek ściągnięcia formularza wizowego lub innego dokumentu związanego z tematem otrzymywania wiz wjazdowych do USA, otrzymuje wiadomość, rzekomo od pracowników administracji rządowej USA, o wytypowaniu do odebrania wizy. Odbiór wizy wjazdowej na teren USA jest uzależniony jedynie od uiszczenia odpowiedniej kwoty na wskazany numer konta bądź przesłanie jej poprzez międzynarodowy system płatności, np. Western Union. Kwoty oscylują w okolicach 600–700 dolarów. Oszust podtrzymuje kontakt tak długo, jak długo ofiara deklaruje kolejne wpłaty, a sprawcy takich przestępstw potrafią mnożyć w nieskończoność powody wpłacania kolejnych sum.

REKOMPENSATA ZA STRATY PONIESIONE W WYNIKU OSZUSTWA NIGERYJSKIEGO

Najbardziej kuriozalna fabuła, jaką mogli wymyślić „oszuści nigeryjscy", jednocześnie sposób bardzo prosty, śmieszny, wręcz bezczelny.

Przestępca, udając najczęściej pracownika administracji państwowej lub organów ścigania Nigerii, ewentualnie upoważnionego przez organy ścigania Nigerii pracownika banku, kontaktuje się z wytypowaną ofiarą, wykorzystując do tego w pierwszej fazie wyłącznie pocztę elektroniczną, w celu sprawdzenia, czy potencjalna ofiara została wcześniej pokrzywdzona w wyniku zaistnienia oszustwa nigeryjskiego lub czy jest na tyle nieuczciwa, by podać się za osobę pokrzywdzoną w wyniku działania „oszustów nigeryjskich" i na tej

podstawie chce wyłudzić nienależne jej odszkodowanie. Istnieje też duże prawdopodobieństwo, iż „oszuści nigeryjscy" zachowują bazę danych osób (ofiar swoich poczynań), z którymi wcześniej prowadzili korespondencję opartą na innym modelu przedmiotowego oszustwa.

Potencjalna ofiara jest informowana, że rząd Nigerii postanowił odzyskać dobre imię i przeznaczył ogromną kwotę pieniędzy na odszkodowania i zadośćuczynienia dla osób pokrzywdzonych w wyniku działalności „oszustów nigeryjskich". W rzeczywistości oszust liczy przeważnie na chciwość i nieuczciwość swojej potencjalnej ofiary wiedzionej wizją uzyskania odszkodowania (w większości przypadków – jej nienależnej rekompensaty) za poniesione straty. Ofiara daje się wciągnąć w grę, w której karty rozdaje oszust.

Po wyrażeniu zainteresowania przez ofiarę oszust przysyła kolejną część (bardziej szczegółową) całej historii. Pojawiają się dokumenty (w kiepskiej jakości) wytworzone w powszechnie dostępnych edytorach graficznych, przesyłane drogą elektroniczną, potwierdzające istnienie przedmiotowego programu rządowego, co ma uprawdopodobnić całą sytuację. Na tym etapie działań sprawcy niewykluczony jest również kontakt telefoniczny. Pojawiają się również informacje dotyczące tego, że ofiara będzie musiała dokonać wpłaty, by w rezultacie mogła przejąć znaczną kwotę rzekomej rekompensaty. Ofiara musi wnieść opłaty za wystawienie certyfikatów przez bank lub inne urzędy, poświadczających, że pieniądze pochodzą ze wskazanego programu rządowego, za usługi prawników oraz koszty operacyjne w banku, który ma sfinalizować przelew. Oszust podtrzymuje korespondencję, prosząc o kolejne wpłaty tak długo, jak pozwala na to naiwność ofiary. Może to trwać bardzo długo, a inwencja twórcza oszustów jest zaskakująca.

Zarówno nazwiska pracowników banku, jak i przedstawicieli administracji rządowej lub organów ścigania bardzo często są prawdziwe, gdyż w większości stanowią dane ogólnie dostępne w Internecie. Jednak nie można znaleźć numerów telefonów tych osób w informacjach kontaktowych infrastruktury rządowej, organów ścigania lub banków, a adresy e-mail używane przez oszustów często należą do puli adresów serwerów oferujących bezpłatną rejestrację konta poczty elektronicznej – tak jak to się odbywa w opisanych wcześniej odmianach tego oszustwa.

Jest to w swej prostocie bardzo wyrafinowana metoda, gdyż ofiara może dobrze zdawać sobie sprawę z faktu, iż sama staje się oszustem, usiłując uzyskać często nienależne jej pieniądze, a faktyczny oszust – inicjator całego zdarzenia – czuje się bezpiecznie, gdyż jego ofiara, która ma świadomość działania nielegalnego i niemoralnego, nie zgłosi procederu Policji…

ZAAWANSOWANE METODY – kryptooszustwo nigeryjskie i złośliwe oprogramowanie – malware[4]

Najbardziej niebezpieczną metodę związaną pośrednio z oszustwami nigeryjskimi stanowi wykorzystanie banalnej treści klasycznego oszustwa nigeryjskiego, wręcz wprost wskazującego na to, iż jest to prymitywny sposób oszustwa, do zainfekowania komputera ofiary złośliwym oprogramowaniem, najczęściej malwarem bankowym.

Scenariusz wydaje się nawiązywać do klasycznego oszustwa nigeryjskiego, z małą, lecz znaczącą modyfikacją. W stopce wiadomości elektronicznej pojawia się informacja, jakoby automatycznie dołączona do korespondencji przez system bezpieczeństwa naszego serwera pocztowego, iż przedmiotowa wiadomość to rodzaj spamu, czyli niechcianych, nieoczekiwanych i irytujących wiadomości elektronicznych, i jeżeli ofiara nie chce otrzymywać więcej tego rodzaju korespondencji, powinna kliknąć odsyłacz (link) znajdujący się poniżej/obok/ lub w tekście. Jest oczywiste, że do korespondencji dołączono złośliwe oprogramowanie, które zostaje aktywowane w momencie kliknięcia, i komputer ofiary oraz wszystkie jego procesy są monitorowane lub modyfikowane zdalnie przez hackerów. Jeśli komputer ofiary został zainfekowany malwarem bankowym, ofiara, która wykorzystuje udogodnienia bankowości elektronicznej, może stracić swoje oszczędności bez szans na ich odzyskanie. Komputer ofiary, nad którym została przejęta kontrola, może się stać narzędziem do popełniania wielu innych przestępstw, jako tzw. komputer zombie połączony w botnet (najpopularniejszą metodą wykorzystania sieci botnet jest tzw. atak DDoS – Distributed Denial of Service – rozproszona odmowa usługi, polegający na zablokowaniu lub spowolnieniu działania całego systemu komputerowego, witryn internetowych e-bankowości lub stron rządowych danego państwa, itp.), ale to już inny temat, na kolejne obszerne opracowanie.

Niniejszy artykuł stanowi rozwinięcie artykułu opublikowanego na stronie internetowej Komendy Powiatowej Policji w Wolsztynie: M. Siwiecki, *Jak uniknąć „oszustwa nigeryjskiego"*, http://www.wolsztyn.policja.gov.pl/w29/prewencja/porady/139469,Jak-uniknac-quotoszustwa-nigeryjskiegoquot.html [dostęp: 16.11.2017 r.].

[1] *Public awareness advisory regarding "4-1-9" or "advance fee fraud" schemes*, w: IWS – The Information Warfare Site, http://www.iwar.org.uk/ecoespionage/resources/4-1-9/secret-service-alert.htm [dostęp: 7.12.2017 r.].

[2] A. Krzyżanowska, *Nowe metody oszustw nigeryjskich. Celem są prawnicy*, http://prawo.gazetaprawna.pl/artykuly/680294,-nowe-metody-oszustw-nigeryjskich-celem-sa-prawnicy.html [dostęp: 16.11.2017 r.].

[3] B. Łącki, *Uwaga na oszustwo Z Mr. Mark Steinert*, http://bothunters.pl/2012/01/10/uwaga-na-oszustwo-z-mr-mark-steinert/ [dostęp: 16.11.2017 r.].

[4] Złośliwe oprogramowanie (z ang. *malware* – zbitka wyrazowa powstała ze słów *malicious* – złowrogi, złośliwy i *software* – oprogramowanie) – wszelkie aplikacje, skrypty itp. mające szkodliwe, przestępcze, groźne lub destrukcyjne działanie w stosunku do użytkownika komputera, https://pl.wikipedia.org/wiki/Złośliwe_oprogramowanie [dostęp: 7.12.2017 r.].

Summary

Nigeria scam – an attempt of classification

The present article constitutes the attempt to systematize and classify a very broad and interesting group of crimes functioning under the shared name "Nigeria scam" for "the second life" of which in a new and more powerful way the Internet allowed. "Nigeria scam" is such a widespread phenomenon that almost everyone met it, but it is worthwhile to remind about it from time to time because there are still people who are its victims.

Tłumaczenie: Renata Cedro

asp. szt. Artur Rogowski

instruktor
Zakładu Służby Kryminalnej CSP

PHISHING – działalność przestępcza mająca na celu kradzież danych, najczęściej bankowych, osobowych oraz innych poufnych informacji. Oszuści za pośrednictwem Internetu rozsyłają nieprawdziwe informacje, aby sprowokować odbiorcę do określonego zachowania, jakim jest na przykład niezamierzone udostępnienie takich danych.

Phishing to oszustwo internetowe, które ma na celu kradzież danych użytkownika, takich jak hasła, loginy, numery kart debetowych i kredytowych, jak również innych poufnych informacji.

Phishing funkcjonuje w Internecie dzięki wykorzystaniu narzędzi komunikacyjnych, m.in. poczty elektronicznej, komunikatorów internetowych oraz niektórych portali społecznościowych. Jedną z metod phishingu jest wysyłanie fałszywych powiadomień z banków, dostawców płatności internetowych lub innych budzących zaufanie instytucji. Przesyłane informacje mają na celu zachęcić lub wręcz przestraszyć odbiorcę tak, aby postępował zgodnie z instrukcjami zawartymi w wiadomości. W rezultacie, nieświadomy oszustwa odbiorca udostępnia swoje dane osobowe. Przykładem takiego działania może być wysłanie za pośrednictwem poczty elektronicznej wiadomości do użytkownika, w której zostanie on poproszony o pilne zalogowanie się na swoje konto bankowe, aby zaktualizować dane, z zastrzeżeniem, iż jeśli tego nie uczyni, straci możliwość logowania na swoje konto bankowe i posługiwania się kartami płatniczymi. Wiadomość, którą otrzyma odbiorca, zawiera

link przekierowujący do fałszywej strony banku, której wygląd odpowiada oryginałowi. Następnie użytkownik wpisuje swoje dane do logowania na stronę banku i otrzymuje informację z podziękowaniem za zalogowanie, a także aktualizację danych, oraz dostaje możliwość wylogowania się z serwisu. Czasem takie strony są tak zaprogramowane, aby wyświetlić użytkownikowi stronę uaktualniającą numer PIN do karty płatniczej. Wiadomość zawiera instrukcję o wprowadzeniu do formularza aktualizacji naszego numeru karty oraz aktualny numer PIN. Dzięki takiemu działaniu sprawca otrzyma dane logowania na konto bankowe oraz karty płatniczej wraz z numerem PIN.

Strony internetowe podszywające się pod bank lub inne instytucję zazwyczaj są wykrywane i usuwane przez administratorów po około 5 dniach. W tym czasie filtry antyphishingowe odnajdują taką stronę i dodają ją do stron zagrożonych, dlatego też oszuści muszą stale tworzyć i konfigurować nowe strony, aby zachować ciągłość swojego procederu.

Sprawcy po uzyskaniu naszych danych poufnych mogą użyć ich np. do wycofywania pieniędzy z kont bankowych, jak również do podrabiania kart płatniczych czy nadawania im numerów identyfikacyjnych odpowiadających oryginalnym kartom i za ich pośrednictwem wypłacać pieniądze.

Wypłata i logowanie na konta bankowe oszukanych użytkowników odbywają sie zazwyczaj w krajach słabo rozwiniętych, jak na przykład Nigeria. Osoby trudniące się phishingiem, które weszły w posiadanie danych użytkowników, aby ograniczyć do minimum identyfikację oraz wykrycie przez organy ścigania, zazwyczaj sprzedają uzyskane dane innym osobom lub organizacjom przestępczym.

Jednym z głównych celów phisherów jest uzyskiwanie danych, dzięki którym otrzymają dostęp do środków finansowych swoich ofiar, ale nie tylko. Bardzo popularna jest również kradzież poświadczeń pocztowych, dzięki którym sprawcy uwierzytelniają swoje działania i mają możliwość rozpowszechniania wirusów lub innych aplikacji, a także tworzenia zainfekowanej sieci informatycznej zwanej botnetem.

Sprawcy chcą za każdym razem dowieść swojej wiarygodności podczas tworzenia fałszywych stron internetowych banków lub też innych organizacji, stale więc aktualizują szablony, szaty graficzne, sposób funkcjonowania stron, aby rozwiać jakiekolwiek wątpliwości logującego się użytkownika co do ich autentyczności.

Działania osób dokonujących oszustw w sieci nie ograniczają się jedynie do uzyskania wiarygodności wizualnej stron, ale również linków i innych odnośników do stron oraz domen internetowych powiązanych z instytucjami lub organizacjami. Sprawcy najczęściej tworzą domeny oraz adresy poczty elektronicznej, które są bardzo podobne do oryginalnych. Na pierwszy rzut oka takie adresy łudząco przypominają te rzeczywiste, jednakże po bliższym prześledzeniu okazuje się, że są to zupełnie inne adresy. Za przykład niech posłuży strona banku ING „www.ingbank.pl" i ich poczta „noreply@ingbank.pl". Fałszywy sposób kodowania to „WWW.lNGBANK.PL" i poczta „NOREPLY@lNGBANK.PL". Różnica między tymi adresami na pierwszy rzut oka jest niewidoczna, jednak po głębszej analizie okazuje się, że w fałszywym sposobie zapisu adresu zamiast dużej litery „I" występuje mała litera „L". Sprawcy mogą w ten sposób zmanipulować użytkownika, który uzna ten adres za zaufany i oryginalny, bo przecież loguje się codziennie na stronę swojego banku i adres ten jest dla niego wiarygodny.

W swych działaniach sprawcy mogą również rozsyłać za pośrednictwem komunikatorów oprogramowanie szpiegowskie lub keyloggery, które na bieżąco wychwytują i przesyłają do użytkowników końcowych wszystkie informacje zapisywane na danym komputerze. Nie tylko dane do logowania mogą więc być narażone na kradzież, ale również dane osobowe, treści komunikatów do innych użytkowników lub też inne dane, które zapisujemy na komputerze.

Jedną z bardziej popularnych metod phishingu w Polsce stała się kradzież danych personalnych osób w celu ich sprzedaży organizacjom przestępczym, a następnie wykorzystania ich do uzyskania środków finansowych.

Przykładem takiego działania jest wystawienie przez sprawców ogłoszenia dotyczącego możliwości podjęcia bardzo dochodowej pracy za pośrednictwem Internetu, polegającej na wypełnianiu ankiet lub też sieciowego call-center. Osoba, wchodząc na stronę z takim ogłoszeniem, które w jej opinii nie budzi żadnej wątpliwości, wysyła kwestionariusz lub też wiadomość za pośrednictwem poczty elektronicznej z informacją, iż chce podjąć taką pracę. Następnie w informacji zwrotnej otrzymuje do wypełnienia formularz rejestracyjny osoby ubiegającej się o pracę, w którym podaje swoje dane osobowe, jak również proszona jest o wysłanie skanu dowodu osobistego lub innego dokumentu potwierdzającego jej tożsamość. Następnie zostaje poinformowana o procesie weryfikacyjnym i konieczności oczekiwania na kontakt ze strony firmy. W tym momencie osoba została już oszukana. Sprawcy, posiadając jej dane oraz skan dokumentu, uzyskują środki finansowe za pośrednictwem firm udzielających kredyty. Po upływie określonego czasu osoba, która została oszukana, próbuje skontaktować się z niedoszłym pracodawcą, jednakże bezskutecznie. Po pewnym czasie otrzymuje informację od firm lub banków o nieterminowej spłacie należności.

Sukces opisanych działań jest możliwy dzięki słabej lub bardzo znikomej wiedzy użytkowników na temat sposobów dokonywania oszustw przez sprawców, jak również dzięki wykorzystaniu ludzkiej ciekawości albo przez zastraszenie. Użytkownicy Internetu nie mają świadomości, że żadna wiarygodna firma, jak bank czy inna instytucja, nie będzie chciała uzyskać od nich danych do logowania, haseł ani innych kodów w zakresie swojej działalności. Należy zatem rozpowszechniać wiedzę o tym, iż bezpieczeństwo naszych danych to w dzisiejszych czasach sprawa priorytetowa i nie należy udostępniać ich osobom postronnym.

Summary

Phishing

Phishing – criminal activity being aimed at a theft of data, most often bank and personal ones, as well as other confidential information. Swindlers, through the Internet, send out false information to provoke the recipient for the determined behavior, which is, for example, unintentional accessibility of such data.

Tłumaczenie: Renata Cedro

WYBRANE ZAGROŻENIA WOBEC DZIECI W INTERNECIE

mł. asp. Tomasz Siemianowski

młodszy wykładowca
Zakładu Służby Kryminalnej CSP

Za szkodliwe treści należy uznać materiały, których skutkiem może być negatywny wpływ na rozwój i psychikę dzieci i młodzieży. Na materiały tego typu mogą one trafiać podczas celowego i konkretnie dokonanego wpisu w wyszukiwarce internetowej, ale także przypadkowo, np. poprzez mylne wyniki wyszukiwania, spam czy reklamę. Najmłodsi polscy internauci przyznają, że mają negatywne doświadczenia związane z korzystaniem z sieci internetowej. Prawie połowa z nich była zastraszana lub miała inne doświadczenia o znamionach zjawiska zwanego cyberprzestępstwem. Dziś już nawet czterolatki swobodnie surfują w Internecie. Czy rodzice zdają sobie sprawę z tego, na co narażają swoje dzieci, udostępniając im bez żadnych ograniczeń komputer czy telefon komórkowy z dostępem do sieci?

Internet to medium, którego dynamiczny rozwój i potencjał są wykorzystywane przede wszystkim przez młodych ludzi. Jest nieodłącznym elementem ich życia społecznego, codziennych aktywności i zabawy. Jednak to nie tylko miejsce rozrywki i nieograniczona przestrzeń, w której ludzie dzielą się zdjęciami czy miejscami, w których bywali. To także strefa, w której miliony ludzi z całego globu ziemskiego poszukują rozwiązania własnego problemu, znalezienia instrukcji czy materiału, który zaspokoi potrzebę ich nauki, ciekawość czy po prostu spełni ich oczekiwania. Nie jest to niestety także miejsce, w którym można czuć się zupełnie bezpiecznie. Pomimo wszelkich zabezpieczeń, systemów, programów czy procedur wdrażanych przez firmy zwalczające przestępczość internetową, sieć internetowa niesie za sobą wiele czyhających zagrożeń gotowych do wyrządzenia człowiekowi szkody w najmniej oczekiwanym miejscu i czasie. Niestety, najbardziej narażone na wszelkie formy zagrożeń są osoby nadmiernie ufne, niemyślące na każdym kroku o konsekwencjach swoich poczynań, osoby niemające zbyt dużo wiedzy o tym, co im grozi. Mowa tu o dzieciach.

Codzienność naszych dzieci, pomimo ich wieku i teoretycznie niewielkiej odpowiedzialności za swoje czyny, składa się z setek decyzji. Często ani dzieci, ani ich rodzice nawet nie zauważają momentu, w którym są one podejmowane. Czasem uważnie rozważają każde za i przeciw, ale często zdarza się też tak, że odczuwają presję wykonania określonej czynności czy zachowania się w odpowiedni, oczekiwany „na zewnątrz" sposób. Niektóre z tych decyzji mają na dzieci niewielki wpływ, czasem wręcz żaden, bo to, czy dziecko obejrzy dwa teledyski ulubionego wykonawcy w Internecie, czy też jeden, tylko skróci bądź wydłuży jego sen o kilka minut. Niestety, konsekwencje innych decyzji, a co gorsza – także decyzji innych osób (dorosłych lub rówieśników), może odwrócić życie dziecka o 180 stopni, często także w tym złym kierunku.

Zjawisko cyberprzemocy czy też innych dramatów − bo cyberprzemoc trzeba kwalifikować jako dramat dla jej ofiary – w których główną rolę odgrywa przemoc z wykorzystaniem nowych technologii, z dnia na dzień, z roku na rok, drastycznie przybiera na sile. Tematyka ta od dawna jest motywem przewodnim programów edukacyjnych, kampanii społecznych lub wszelkiego typu akcji uświadamiających. Oprócz dostępu do treści pojawiła się również możliwość ich tworzenia w formie chociażby zamieszczania zdjęć, filmów czy wpisu odpowiednich komentarzy. Te – obecnie kluczowe w budowaniu zasobów internetowych – funkcjonalności stały się również narzędziem przemocy. Mimo wszelkich podejmowanych działań ukierunkowanych na ograniczenie tego typu zjawisk, problem wciąż narasta, a z ostatnich badań wynika, że co czwarty młody człowiek w wieku 12–15 lat doświadcza cyberprzemocy[1]. Od początku rozważań na temat problemu przemocy w sieci zwraca się uwagę na jego charakter związany ze specyfiką Internetu. Nawet pozornie błahe sytuacje, w związku z powszechną dostępnością kompromitujących materiałów, szybkością ich rozpowszechniania, trudnością usunięcia ich z sieci, a także rangą, jaką młodzi ludzie nadają swojemu sieciowemu wizerunkowi i sieciowej pozycji, potrafią być dla nich bardzo dotkliwe. Coraz liczniejsze, tragiczne w skutkach sytuacje przemocy online nagłaśniane w mediach wskazują, że niewątpliwie borykamy się z problemem dużej wagi. Obraz ten uzupełniają badania prowadzone wśród dzieci i młodzieży pokazujące, że cyberprzemoc jest ich codziennością. W słupkach statystyk górują takie zachowania, jak znieważenia, pomówienia czy też rozbudzanie nienawiści wobec innej osoby bądź grupy osób. Takie zachowania określane są jako mowa nienawiści (*hate speech*) i najczęściej stanowią narzędzie rozpowszechniania uprzedzeń antyspołecznych oraz dyskryminacji na tle rasy, pochodzenia etnicznego, narodowości, płci, tożsamości płciowej, wieku, światopoglądu czy religii. Rozpatrując wskazane powyżej zjawiska, na-

leży jednak zachować ostrożność, ponieważ niezmiernie istotne jest rozgraniczenie języka wrogości między negatywnymi ocenami, często opartymi na uprzedzeniach i stereotypach, a realnej mowy nienawiści, która ma na celu podjęcie określonego działania wobec konkretnej osoby bądź grupy osób. Nawoływanie do nienawiści na tle narodowościowym, rasowym lub etnicznym polskie prawo penalizuje odpowiednio w ustawie z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2017 r. poz. 2204, z późn. zm.) w art. 256 k.k. (propagowanie faszyzmu lub innego ustroju totalitarnego) i art. 257 k.k. (rasizm). W większej mierze polskie organy ścigania zajmują się przestępstwami popełnianymi przez osoby nieletnie, dotyczącymi art. 190 k.k. (groźba karalna), art. 212 k.k. (zniesławienie) czy art. 216 k.k. (znieważenie).

Rasizm, czyli zespół przekonań opierający się na tezie, że różnice rasowe między ludźmi niosą ze sobą niezbywalne odmienności osobowościowe i intelektualne, a także ksenofobia, czyli niechęć i wrogość wobec innych grup etnicznych, wskazują na istniejącą w społeczeństwie ideologię istnienia ras czy grup „wyższych" oraz „niższych". Dzieci same w sobie rodzą się bez negatywnych przekonań tego typu, jednak kształtują się one w trakcie ich rozwoju i wychowania. Zazwyczaj dzieci „przechwytują" tok myślenia i zachowania wobec osób innego koloru skóry lub innej grupy etnicznej od własnych rodziców, bliższej czy dalszej rodziny bądź znajomych, z tą różnicą, że osoby dorosłe najczęściej wyrażają swoje poglądy w rozmowie między sobą, bezpośrednio, natomiast dzieci, nierzadko chcąc „się pochwalić" swoją nowo nabytą ideologią bądź też celowo dokuczyć innej osobie, publikują treści rasistowskie lub ksenofobiczne w Internecie, albo wysyłając wiadomości czy wykonując połączenia głosowe za pomocą telefonii komórkowej.

Nie wszystkie agresywne wypowiedzi w sieci należy jednak klasyfikować jako mowę nienawiści. Zdecydowanie szerszym pojęciem jest tu tzw. hejtowanie, czyli wszelkie wypowiedzi, które w dalszym ciągu są agresywne, jednak nie mają podłoża ideologicznego. Wyraz pochodzi z języka angielskiego od słowa *hate*, które w bezpośrednim tłumaczeniu oznacza wrogość, nienawiść. O ile mowa nienawiści opiera się na negatywnych stereotypach i jest powiązana z poglądami danej osoby, o tyle hejtowanie jest objawem agresji bez ściśle określonego podłoża. Młode osoby korzystające z Internetu coraz częściej skarżą się, że zostały przez kogoś zhejtowane bez jakiegokolwiek powodu. W przypadku hejtu nie mówimy o agresji skierowanej na przykład w kierunku grupy innego wyznania religijnego, lecz po prostu o agresywnym działaniu. Z tematem hejtu są ściśle związani tzw. trolle, czyli osoby przejawiające antyspołeczne zachowanie charakterystyczne przede wszystkim dla wszelkich forów dyskusyjnych, ale także innych miejsc w Internecie, gdzie prowadzi się dyskusje. „Trollowanie" polega na zamierzonym wpływaniu na innych użytkowników w celu ich ośmieszenia lub obrażenia poprzez zamieszczanie napastliwych i kontrowersyjnych, często nieprawdziwych przekazów. Działania takie stosowane są jako prowokacja mająca doprowadzić do wywołania kłótni. Jakie są szanse, że dziecko zostanie „trollem"? Bardzo duże, a wynika to z tego, iż w Internecie zaciera się poczucie indywidualności, w konsekwencji czego użytkownicy tracą kontrolę nad własnym zachowaniem. Taki stan ograniczonej samoświadomości pojawia się w warunkach bycia anonimowym w dużej grupie ludzi. Znikają wtedy hamulce, a dzięki temu osoby czują się wolne od norm i standardów społecznych. Trollowanie na forum w sieci wiąże się z faktem, iż troll zazwyczaj nie wie, kim jest osoba, wobec której się negatywnie wypowiada, nie wie, czym ona się zajmuje i jak wygląda. Troll tworzy wtedy samodzielnie w swojej głowie cały zestaw jej cech, kształtuje jej wygląd, który zazwyczaj nie ma nic wspólnego z rzeczywistym wyglądem i zachowaniem jego rozmówcy. Troll traci wtedy kontakt z rzeczywistością, zaczyna mu się wydawać, że to tylko gra, że jego przeciwnik jest nieokreślony i nierealny, tak jak to bywa w grach komputerowych. Stąd już tylko maleńki krok do uznania, że normalne reguły interakcji nie dotyczą osoby stającej się trollem.

Uporczywe i powtarzające się, a wręcz nękające wiadomości sms, mms, e-mail czy też same połączenia telefoniczne kierowane wobec konkretnej osoby stanowią przestępstwo określane dziś mianem stalkingu. Kodeks karny określa stalking w art. 190a. Sam termin stalking pochodzi z języka angielskiego, a dokładnie od słowa *stalk*, co w bezpośrednim tłumaczeniu oznacza tropić, prześladować, śledzić. Stalking można określić zatem jako celowe, zamierzone i świadome prześladowanie bądź molestowanie ukierunkowane bezpośrednio wobec osoby będącej ofiarą. Działania takie w swoim zakresie obejmują między innymi naruszenie wolności osobistej i prywatności drugiej osoby, zbliżenie się do ofiary w sposób fizyczny lub wirtualny, a także składanie jej niechcianych propozycji i gróźb wywołujących strach i poczucie zagrożenia. Osoba dotknięta przestępstwem określonym jako stalking staje się ofiarą, ponieważ nie chce, aby kontakt ze sprawcą w ogóle istniał, nie życzy sobie zbliżania się do niej, nachodzenia jej w szkole czy w domu, wysyłania jej wszelkiego typu smsów, e-maili czy innych metod kontaktu wirtualnego.

Zjawisko stalkingu coraz częściej jest zauważalne wśród dzieci i młodzieży w wieku szkolnym. Wynika to przede wszystkim z ich rozwoju emocjonalnego, a w szczególności ze zmienności uczuć i emocji towarzyszących procesowi dojrzewania. Młodocianymi sprawcami stalkingu zazwyczaj okazują się osoby płci męskiej, z kolei ofiarami – przedstawicielki płci żeńskiej. Ofiarą stalkingu wśród dzieci i młodzieży jest zazwyczaj była, czasem już dawna miłość, przyjaciel, osoba nielubiana, rywalizująca ze sprawcą w określonej dziedzinie, lub też odwrotnie – osoba bardzo lubiana, z którą każdy chciałby się przyjaźnić, jednak ona zaprasza tylko wybranych do grona swoich znajomych, kierując się trudnymi do osiągnięcia kryteriami, np. do jej grupy mogą należeć osoby pochodzące z tzw. dobrych domów, posiadające określonego rodzaju gadżety szkolne lub ubierające się w specyficzny sposób[2]. Obecnie dominujące do tej pory zjawisko niechcianego kontaktu fizycznego sprawcy z ofiarą jest zastępowane kontaktami wirtualnymi, występującymi w postaci niechcianych połączeń telefonicznych bądź wysyłanych wiadomości sms czy wiadomości internetowych. Stalking nie jest jednostką chorobową, ponieważ nie ma tu problemu medycznego. Trudno jest określić bezpośrednie przyczyny powstawania obsesji na punkcie drugiej osoby i jej prześladowania. Sprawca może się kierować tylko chęcią wyrządzenia ofierze krzywdy, ale może też przyjąć jako cel – nie do końca nawet świadomie – przejęcie kontroli nad ofiarą poprzez doprowadzenie do sytuacji, kiedy odczuwa ona lęk. Zaczyna on wtedy przejawiać potrzebę dominacji nad ofiarą, upajając się poczuciem władzy wynikającej z bezsilności ofiary. Zjawisko obsesyjnego prześladowania wpływa negatywnie na życie i zdrowie ofiary, wywołując liczne negatywne skutki, takie jak poczucie zagrożenia, ataki paniki, depresję czy też obniżenie poczucia własnej wartości i wiary we własne siły. Dochodzą do tego wstyd i poczucie winy, że to ofiara doprowadziła do tej sytuacji, odizolowanie i trudności w wypełnianiu codziennych obowiązków, problemy w relacjach personalnych. Ponadto widoczne są negatywne skutki w zdrowiu fizycznym objawiające się bólami i zawrotami głowy, zaburzeniami snu, odżywiania i czynności układu krwionośnego.

Sieć internetowa dla wielu osób, niezależnie od wieku, stanowi tak poważny obiekt zainteresowania, że potrafią się one w niej zapomnieć. Sytuacja ta jest szczególnie niebezpieczna dla młodych osób, które de facto nie są jeszcze obciążone obowiązkami tak jak osoby dorosłe. U części użytkowników utrata kontroli nad czasem spędzanym przed komputerem i poszukiwanie coraz intensywniejszych bodźców mogą prowadzić do nadużywania Internetu, co finalnie jest określane mianem uzależnienia od sieci bądź terminem „siecioholizm". Jakie działania najczęściej prowadzą do uzależnienia? Najczęstszymi formami aktywności online wpływającymi na nadużywanie Internetu jest korzystanie z serwisów społecznościowych, gier, serwisów pornograficznych oraz wszelkich form hazardu. Zjawiskiem potęgującym skalę zagrożenia uzależnieniem od Internetu jest nieustannie rosnąca popularność urządzeń mobilnych pozwalających na niemal nieograniczony dostęp do sieci i aplikacji internetowych. Co gorsza, dzięki specyfice tych urządzeń znacznie ograniczona i utrudniona jest kontrola rodzicielska. Obecnie zdecydowana większość młodych ludzi spędza każdego dnia wiele godzin, korzystając z Internetu. Niewątpliwie jest to wyraźny znak ostrzegawczy dla rodziców, jednak nie stanowi on jeszcze „diagnozy" uzależnienia od sieci. Aby podejrzewać, iż taki nałóg faktycznie może dotyczyć danej osoby, należy stwierdzić bezpośrednio, iż czas spędzany w Internecie oraz intensywność poszukiwanych przez nią doznań wyraźnie wymykają się spod kontroli, a ponadto – co ważniejsze – korzystanie z sieci prowadzi do zaniedbywania innych aspektów życia, w tym nawet potrzeb fizjologicznych. Objaw może także stanowić cierpienie osoby uzależnionej w przypadku braku możliwości dostępu do sieci. Obserwując liczbę i jakość godzin spędzanych przez dziecko przed komputerem czy z urządzeniem mobilnym w dłoni, należy zwracać szczególną uwagę na takie aspekty, jak przerost zainteresowania komputerem ponad inne zainteresowania, zaniedbywanie obowiązków szkolnych i rodzinnych, powstawanie konfliktów rodzinnych, złość dziecka na zwrócenie mu uwagi dotyczącej używania urządzeń elektronicznych czy Internetu, reakcja charakteryzująca się rozdrażnieniem bądź agresją na momenty, w których dostęp do sieci jest utrudniony bądź niemożliwy.

Wszechstronność Internetu sprawia, że dzieci i młodzież w najmniej oczekiwanym momencie mogą trafić na materiały dla nich niepożądane, niestety także te zachęcające do zachowań autodestrukcyjnych. Odczytywanie tego typu treści wiąże się z dużym prawdopodobieństwem, iż świat stanie się dla dziecka niezrozumiały, wręcz okaże się dla niego samego zagrożeniem. Dziecko przestanie czuć się bezpiecznie. Niektóre figurujące w sieci witryny internetowe mogą stanowić dla dziecka wskazówki, jak zdobyć narkotyki, jak je zażywać czy też jak je zastąpić substancjami legalnego pochodzenia wywołującymi zbliżone działanie. Inne zachęcają np. do zmiany sposobu odżywiania, samodzielnego leczenia, samookaleczenia czy w końcu – samobójstwa. Korzystając z takich stron internetowych, dzieci mogą się z powodzeniem dowiedzieć, w jaki sposób skrzywdzić samego siebie, jak to zrobić, aby mniej bolało, czy wreszcie mogą się utwierdzić w przekonaniu, że tego typu zachowania są jedynym właściwym wyjściem z problematycznej sytuacji. Często zawierają też wskazówki, w jaki sposób ukryć te zachowania przed rodziną i przyjaciółmi. Młodzi ludzie, którzy mają problem z samoakceptacją i percepcją własnego ciała, są dość wrażliwi na tym punkcie, a co za tym idzie – szczególnie narażeni na wszelkie sugestie dotyczące sposobu żywienia oraz diet wspomagających utrzymanie szczupłej sylwetki. Diety cud, bo o takich się najczęściej słyszy i czyta, częstokroć zawierają błędne informacje odnośnie do zdrowego odżywiania się, a stosowanie się do zawartych tam wskazówek i rad może się skończyć poważnym uszczerbkiem na zdrowiu lub wręcz zagrażać życiu osób z nich korzystających. Strony promujące zaburzenia odżywiania noszą nazwę ProAna (Pro Anorexia) i ProMia (Pro Bulimia). Na ich popularność wpływa czynnik wspólnoty – dzieci mające np. problem z nadwagą mogą porozmawiać, wymienić poglądy i spostrzeżenia z innymi dziećmi borykającymi się z podobnym problemem. Czują się tam zazwyczaj bardzo swobodnie, gdyż w odróżnieniu od sytuacji, które często mają miejsce w ich życiu „niewirtualnym", są tam w zupełności akceptowane. Pikanterii dodaje nagonka medialna promująca i podkreślająca wzorce piękna prezentowane przez bardzo szczupłe modelki i modelów. Tendencja ta sprzyja propagowaniu idei odchudzania wśród nastolatków i dzieci.

Innym niebezpiecznym zjawiskiem, także dotyczącym dużej grupy użytkowników − zwłaszcza tych w młodym wieku − jest wyszukiwanie odpowiedzi w sieci na dotykające ich problemy medyczne, zamiast zasięgnięcia porady lekarza. „Dr Google" zastępujący prawdziwego specjalistę to wcale nie żart, lecz niezbyt trafny pomysł wielu użytkowników sieci internetowej. U dzieci problem związany z poszukiwaniem skutecznego lekarstwa lub metody na zażegnanie problemu zdrowotnego potęgowany jest przede wszystkim przez ich ufność do odnalezionych w sieci informacji, a także wstyd, który paraliżuje je przed rozmową z rodzicami, lekarzem czy innymi osobami. Specjaliści w zakresie medycyny przyznają zgodnie, że korzystanie z pomocy medycznej w Internecie ma jakikolwiek sens tylko wtedy, gdy naprawdę doskonale wiemy, co nam dolega, kiedy mamy konkretne wyniki badań i niepodważalne dane. Drugą kwestią jest warunek, że osoba zgłosi się w Internecie z konkretną prośbą o poradę do określonego serwisu bądź specjalisty, a nie będzie polegała na opinii anonimowych internautów na otwartym forum lub czacie. Pokusa szybkiej, bezpłatnej, anonimowej i niewzmagającej poczucia wstydu porady lekarskiej może korcić każdego – tym bardziej dziecko czy nastolatka – ale skutki takiego leczenia mogą być naprawdę złe, bo zamiast wyzdrowieć, można tylko skomplikować sobie sytuację.

Powszechny dostęp do Internetu, wykorzystanie go przez młodych ludzi w życiu codziennym, społecznym, w edukacji czy rozrywce przyniosły wiele różnorodnych wyzwań. Sytuacje, w których dzieci zawierają znajomości za pośrednictwem sieci internetowej, po czym zostają zwerbowane do grup przestępczych, sekt, zachęcone do podjęcia czynności mających na celu wyrządzenie im krzywdy czy też wykorzystania seksualnego, stanowią nie lada wyzwanie dla organów ścigania i wymiaru sprawiedliwości. Zjawisko uwodzenia dzieci za pośrednictwem Internetu (z języka angielskiego zjawisko to określone jest jako *grooming*) stanowi szczególną kategorię relacji stworzoną między osobami dorosłymi a dziećmi w celu ich uwiedzenia i wykorzystania seksualnego, które może przybierać różnorodne formy, poczynając od prezentowania dziecku materiałów o treści pornograficznej, przez wyłudzanie intymnych zdjęć i filmów, zmuszanie do wykonywania i dokumentowania w postaci elektronicznej czynności seksualnych, na fizycznym krzywdzeniu seksualnym dziecka podczas spotkania w świecie realnym poprzestając. Pomimo trwającego przez jakiś czas w Internecie procesu uwodzenia dziecka, nie musi dojść do fizycznego kontaktu uwodziciela, tj. sprawcy z jego ofiarą, czyli z dzieckiem. Proces ten jednak zawsze wyrządza głęboką krzywdę dziecku i pozostawia bliznę na psychice do końca jego życia. Gdzie w Internecie dziecko się może spotkać ze zjawiskiem groomingu? Przede wszystkim

tam, gdzie bardzo często się loguje, gdzie czuje się bezpiecznie, swobodnie, gdzie nie spodziewa się żadnego zagrożenia. Takimi miejscami są przede wszystkim portale społecznościowe oraz aplikacje, które umożliwiają komunikację pomiędzy użytkownikami sieci. To wymarzona przestrzeń, idealne pole do popisu dla osób chcących nawiązać relacje z nieznajomymi, często w ogóle bez wyobrażenia konsekwencji takiej znajomości, bez podstawowej weryfikacji, czy rozmówca jest faktycznie tą osobą, za którą się podaje. Działanie sprawców takich przestępstw niemal zawsze opiera się na działaniu „pod przykrywką", z wykorzystaniem cudzych bądź zmyślonych lub fałszywych danych. Zanim sprawcy rozpoczną proces nawiązywania i dalszego rozwijania nowej znajomości, najpierw starają się uzyskać jak najwięcej informacji na temat swojej ofiary. Rozmowa staje się łatwiejsza, jeśli sprawca przedstawi zainteresowania podobne do zainteresowań swojej ofiary. Młode osoby często publikują na portalach społecznościowych wiele swoich zdjęć i osobistych informacji, wyrażają tam swoje uczucia, powody, dla których są zadowolone bądź nie, często będąc nieświadomym, zapominając lub po prostu nie myśląc o tym, iż jeśli już chcą cokolwiek opublikować, to trzeba ten materiał lub dane odpowiednio zabezpieczyć, ograniczyć dostęp do nich osobom nieznajomym i niepowołanym. Wskutek takiego działania sprawcy w łatwy sposób uzyskują interesujące ich informacje na temat swojej potencjalnej przyszłej ofiary. Badania wskazują, iż przeciętny wiek osób, które pierwszy raz logują się do sieci, w Polsce wynosi 8 lat[3]. Poddając analizie zjawisko uwodzenia za pośrednictwem Internetu, zauważono, że procederu kontaktowania się w sieci internetowej dzieci z nieznajomymi, których wcześniej dzieci nie poznały osobiście, doświadczyło 25% spośród nich. Mimo tej stosunkowo dużej liczby, 8% z nich spotkało się w życiu rzeczywistym z osobą poznaną online[4]. Uwodzenie dziecka w Internecie stanowi zazwyczaj proces rozciągnięty w czasie. W większości przypadków nie można przypisać go do żadnego sztampowego modelu działania sprawcy groomingu, gdyż z reguły jest on dostosowany do preferowanej formy kontaktu z ofiarą i przede wszystkim jej reakcji. Ze względu na uwarunkowania rozwojowe, dzieci z reguły są ufne i nie zawsze potrafią krytycznie ocenić sytuację, w jakiej się znajdują. Zjawisko to wzmagane jest przez takie czynniki, jak problemy dzieci w relacjach z innymi, problemy emocjonalne, niskie poczucie własnej wartości, brak nadzoru ze strony dorosłych czy chociażby naturalna cecha, jaką jest czysta dziecięca ciekawość. Wiele dzieci czy osób małoletnich zostaje całkowicie zmanipulowanych przez zachowania ze strony sprawców i zupełnie nieświadomie wpada w zastawioną przez nich pułapkę. Zdarzają się jednak sytuacje, ze to właśnie młode osoby same szukają w sieci kontaktów seksualnych. Wówczas ofiary najczęściej w ogóle nie stawiają oporu wobec wykorzystania seksualnego. Ostatecznie jakakolwiek z opisanych relacji by nie nastąpiła, to kontakt między ofiarą a sprawcą sprowadza się do takiego zmanipulowania dziecka, że nie jest ono w stanie kontrolować tego, w jakie działania się angażuje. Mogą się zdarzyć także sytuacje skrajne, kiedy to osoby małoletnie dopuszczają się prostytucji online, sprzedając swoje nagie zdjęcia lub udostępniając innym osobom film stanowiący „seks pokaz". Większość dzieci to jednak ofiary wcześniejszego wykorzystania seksualnego lub innego rodzaju przemocy, co sprawia, że jeszcze bardziej są one narażone na tego typu zagrożenia. Polskie prawo określa uwodzenie dzieci przez dorosłych sprawców jako przestępstwo ścigane na mocy art. 200a Kodeksu karnego[5].

Coraz częstszym zjawiskiem wśród młodych ludzi na całym świecie jest wzajemne przesyłanie erotycznych zdjęć i filmów. Niestety, cechą tych zachowań jest to, że potrafią doprowadzić do bardzo poważnych konsekwencji. Sexting, bo o nim mowa, z każdym rokiem zwiększa skalę, a jak wynika z badań, w Polsce już co ósmy nastolatek w wieku 14–18 lat przesyła tego typu materiały, w tym jedna trzecia z badanych nastolatków zdeklarowała się, że takowe otrzymuje[6]. Większość badanych uczniów przyznała, iż nie doświadczyła niczego złego w związku z wysyłaniem lub otrzymaniem nagich zdjęć, co nie daje jednak gwarancji, że tak się nie stanie. A co jeśli takie zdjęcia trafią do większej liczby odbiorców niż ta jedna jedyna, często ukochana czy podobająca się osoba? Kiedy i w jaki sposób takie zdjęcia dostają się w niepowołane ręce? Otóż najczęściej zdarza się tak, iż trafiają one na wszelkiego typu portale społecznościowe, grupowe e-maile, fora internetowe, hostingi zdjęć czy inne miejsca w sieci po jakiejś kłótni czy zerwaniu związku osób przesyłających je sobie wzajemnie. Często stanowi to akt zemsty. Osoby, których nagie ciało jest przedmiotem rozesłanych zdjęć, stają się w ten sposób obiektem żartów, pośmiewiskiem, celem nieprzyjemnych epitetów, przez co bardzo często popadają w depresję, przechodzą załamanie nerwowe, tracą chęć do kontaktu z rówieśnikami, uczęszczania do szkoły czy chociażby samego wychodzenia z domu. Zdarza się, iż zachowania rówieśników wobec tych osób są tak intensywne, że konieczna jest zmiana szkoły, jednak to też nie zawsze przynosi oczekiwany efekt, ponieważ nowi koledzy również mogą znaleźć wcześniej zamieszczone nagie zdjęcia w sieci. Bywa, że osoby, które wysłały komuś swoje nagie zdjęcia, stają się ofiarą szantażu w postaci złożenia groźby, iż jeśli sobie nie zrobi i nie wyśle kolejnego nagiego zdjęcia czy filmu, wówczas jej wcześniej wykonane i wysłane zdjęcia lub film trafią do sieci w miejsce, do którego każdy ma swobodny dostęp. Skutkiem tego typu sytuacji są niestety zdarzające się próby samobójcze osób, których nagie zdjęcia znalazły się w rękach osób niepowołanych. Sprzyja temu fakt, iż osoby te wstydzą się komukolwiek opowiedzieć o swoim problemie, krępują się rozmowy z kimkolwiek z rodziny czy ze znajomych, nawet z najbliższą przyjaciółką lub kolegą. Atak społeczeństwa i rówieśników jest dla niej tak silny, że pomimo iż o zaistniałej sytuacji dowiadują się rodzice, nauczyciele czy pedagodzy i ich pełnego wsparcia, a także podjętej terapii, równowaga psychiczna takich osób jest już czasem nie do odbudowania. Takie sytuacje na szczęście zdarzają się rzadko, jednak przyglądając się badaniom i statystykom, które w zakresie sextingu rosną niezmiernie szybko, należy się spodziewać, iż konsekwencje tych zdarzeń także się nasilą. Ofiarami sextingu padają najczęściej młode dziewczyny, które są proszone przez ich chłopaków o przesłanie nagiego zdjęcia lub filmu w tzw. dowód miłości. Niestety, często myślą, że dlaczego nie wysłać chłopakowi takiego zdjęcia, skoro przecież wszyscy tak robią i nic się nie dzieje? Czy to, że inni tak postępują bądź uleganie presji „drugiej połówki" stanowią sensowne argumenty? Czy są warte utraty prywatności i poszanowania własnego ciała? Kwestia ta, podobnie jak też inne zjawiska opisane w niniejszym artykule, są warte głębokiego przemyślenia.

[1] https://akademia.nask.pl/ [dostęp: 15.11.2017 r.].
[2] B. Harwas-Napierała, J. Trempała, *Psychologia rozwoju człowieka. Rozwój funkcji psychicznych*, PWN, Warszawa 2004, t. 2, s. 85.
[3] https://akademia.nask.pl/ [dostęp: 15.11.2017 r.].
[4] M. Wojtas, *Uwodzenie dzieci w internecie i inne niebezpieczne kontakty,* w: *Bezpieczeństwo dzieci online*, Polskie Centrum Programu Safer Internet, Warszawa 2014.
[5] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2017 r. poz. 2204, z późn. zm.).
[6] https://akademia.nask.pl/ [dostęp: 15.11.2017 r.].

Zagrożenia cyberprzestrzeni jako element WOJNY HYBRYDOWEJ

gen. broni prof. dr hab. Tadeusz Jemioło

Uczelnia Techniczno-Handlowa im. Heleny Chodkowskiej w Warszawie

Współczesne wojny wyróżniają się stosowaniem wielu form i środków ich prowadzenia, które mają charakter podprogowy. Najczęściej są to wojny hybrydowe. Za przykład może posłużyć aneksja Krymu oraz ciągle toczące się wojna na wschodzie Ukrainy. W ostatnim okresie nastąpiło zainteresowanie się bezpieczeństwem cyberprzestrzeni, którego zagrożenie znalazło wyraz również w trakcie ostatnich ćwiczeń wojskowych ZAPAD prowadzonych przez Federację Rosyjską. Zaistniała więc ważna okoliczność, aby przybliżyć teorię tej sfery bezpieczeństwa.

Upadek bipolarnego podziału świata oraz zakończenie zimnej wojny zrodziły pytanie o możliwości występowania wojen i o ich charakter. Wśród wielu analityków zajmujących się sprawami bezpieczeństwa zapanował pogląd o zwróceniu uwagi na problematykę ekonomiczną, natomiast zagadnienia wojen potraktowano jako zjawiska mało prawdopodobne. Wielu z nich zauważyło jednak, iż trwająca ponad 50 lat równowaga strachu pomiędzy Wschodem a Zachodem stwarzała warunki do utrzymującej się stabilności w układzie międzynarodowym. Zadawano często pytanie, czy jednobiegunowość świata manifestująca się hegemonizmem Stanów Zjednoczonych będzie mogła zapewnić tę stabilność w nadchodzących dziesięcioleciach. Odpowiedź na tak postawione pytanie wydaje się przecząca. Zmieniło się globalne środowisko bezpieczeństwa charakteryzujące się występowaniem konfliktów wewnętrznych oraz pojawieniem się nowych wyzwań i zagrożeń. Najczęściej pojawiają się nowe zagrożenia o charakterze asymetrycznym, spośród których w ostatnich latach na znaczeniu przybrał terroryzm wraz z jego różnorodnością. Obserwujemy także pojawienie się nowych aktorów, których rola w kształtowaniu się bezpieczeństwa międzynarodowego ciągle wzrasta[1].

Zmiana globalnego środowiska bezpieczeństwa pociągnęła za sobą pojawienie się nowych wojen. To wojny hybrydowe stały się słowem kluczowym w opisie stanu bezpieczeństwa oraz rozszerzeniem podmiotowego i przedmiotowego charakteru tych wojen. Od dawna było wiadomo, że wojny hybrydowe charakteryzują się różnorodnością form i sposobów prowadzenia. Niemniej jednak rozgłos wojny te zyskały po aneksji Krymu przez Federację Rosyjską oraz po walkach z tzw. Państwem Islamskim. W obliczu wielu ocen dotyczących wojny hybrydowej zachodzi potrzeba przybliżenia teorii tych wojen. Wbrew krążącym opiniom to nie Rosjanie są twórcami koncepcji wojny hybrydowej, ale amerykańscy analitycy wojskowi. Koncepcja ta miała być odpowiedzią na doświadczenia zdobyte przez armię Stanów Zjednoczonych w konfliktach w Afganistanie i Iraku oraz w tzw. wojnie z terroryzmem, a także próbą nowego podejścia teoretycznego, które będzie skuteczniej wyjaśniać otaczającą rzeczywistość[2]. Analitykami zajmującymi się tą problematyką byli William J. Nemeth oraz Frank G. Hoffman. Pierwszy z nich, dokonując oceny konfliktu rosyjsko-czeczeńskiego, często stosował pojęcie hybrydowości – nie tylko w odniesieniu do działań czeczeńskich bojowników, ale także do sposobu funkcjonowania tamtejszego społeczeństwa. Stwierdził również, że cechą społeczeństwa hybrydowego jest połączenie nowoczesnych teorii politycznych z tradycyjną organizacją społeczną i obyczajowością. Hybrydowość społeczeństwa ma bezpośrednie przełożenie na sposób przygotowania i prowadzenia wojny.

Zgodnie z teorią Nemetha wojna hybrydowa posiada następujące cechy:

- organizacja armii odzwierciedla poziom rozwoju społeczno-ekonomicznego oraz obowiązujące w niej normy;
- odmienne od zachodniego rozumienie siły militarnej; w wojnie hybrydowej ważną rolę odgrywają elementy walki partyzanckiej, których skuteczność ocenia się jako wysoką, pomimo bardzo dobrego wyposażenia (uzbrojenia) strony przeciwnej; w walce partyzanckiej zacierają się różnice między żołnierzami a cywilami;
- umiejętność zastosowania zaawansowanych technologii cywilnych i wojskowych.

Nie pomniejszając zasług Williama J. Nemetha, warto przytoczyć teorie Franka G. Hoffmana oraz rosyjskiego generała Walerija Gierasimowa będącego szefem Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej.

Teoria wojny hybrydowej według Franka G. Hoffmana

Frank G. Hoffman – były oficer armii amerykańskiej wraz ze swoim zespołem przeprowadził wiele badań związanych z teorią współczesnych wojen. Wyniki swoich naukowych poszukiwań opublikował w artykule „Conflict in the 21st century Rise of the Hybrid Wars". Zamieścił w nim także definicję wojny hybrydowej, zgodnie z którą wojny hybrydowe zawierają w sobie zestaw różnych metod działań wojennych, np. działania konwencjonalne, nieregularne taktyki, ugrupowania zbrojne, akty terrorystyczne, w tym masową przemoc, oraz akty przestępcze[3]. Zgodnie z twierdzeniem Hoffmana wojny hybrydowe mogą być prowadzone zarówno przez podmioty państwowe, jak i pozapaństwowe. Mogą w nich uczestniczyć małe oddziały lub większe zgrupowania. Dowodzenie działaniami w wojnach hybrydowych odbywa się na ogół w sposób scentralizowany, z myślą o uzyskaniu większych efektów tych wojen.
Analitycy skupieni wokół Hoffmana za klasyczną wojnę hybrydową uznali II wojnę libańską z 2006 r. pomiędzy armią izraelską a Hezbollahem. Wśród wielu cech opisujących tę wojnę do najważniejszych zaliczono:

- wysoki poziom wyszkolenia wojskowego oddziałów Hezbollahu;
- umiejętność wtapiania się żołnierzy Hezbollahu w ludność cywilną;
- wykorzystanie infrastruktury miejskiej do organizowania zasadzek;
- zdolność stosowania zaawansowanych technologii wojskowych;
- umiejętność obsługi sprzętu wojskowego, w tym rakietowego;
- umiejętność i skuteczność prowadzenia rozpoznania, w tym radioelektronicznego;
- zdolność prowadzenia walki radioelektronicznej.

Wojna hybrydowa w ujęciu gen. Walerija Gierasimowa

Analitycy wojskowi Federacji Rosyjskiej prowadzą na dużą skalę badania związane z nowoczesnymi wojnami. Fakt, że w tych badaniach czynną rolę odgrywa gen. Gierasimow będący aktualnym szefem Sztabu Generalnego Sił Zbrojnych, dowodzi ich znaczenia. Gen. Gierasimow nie mówi wprost o wojnach hybrydowych, lecz przedmiot zainteresowań badawczych potwierdza, iż te badania w dużej mierze są poświęcone teorii wojen hybrydowych. Przebieg konfliktu na Ukrainie stanowi najlepszy przykład, jak doktryna gen. Gierasimowa została zastosowana w praktyce.
Gen. Gierasimow zwraca uwagę na to, że w XXI w. będzie można zaobserwować tendencję do zanikania granic między stanem pokoju i wojny. Stwierdził on także, że współczesne wojny nie będą poprzedzone ich wypowiadaniem. Sugeruje również, że nie będą one przebiegały według schematów zawartych w zasadach sztuki wojennej. Według gen. Gierasimowa na sile będą przybierać niemilitarne środki działań wojennych. Wojny będą przebiegać według nieznanych wcześniej schematów. Wojny hybrydowe cechują się także wykorzystaniem aspektów propagandowych, ekonomicznych oraz humanitarnych. Wykorzystanie w umiejętny sposób tych elementów może prowadzić do określonej polaryzacji nastrojów społecznych.
W doktrynie gen. Gierasimowa duży nacisk kładzie się na działania asymetryczne. Stąd szerokie wykorzystanie służb specjalnych oraz opozycji politycznej w danym kraju. Chodzi o to, aby wojną objąć największe obszary państwa będącego potencjalnym przeciwnikiem. Najlepiej, gdyby wojna hybrydowa przybrała postać wojny partyzanckiej i wojny domowej. Według gen. Gierasimowa obecnie zacieśniają się różnice między strategicznym, operacyjnym i taktycznym poziomem działania.

WNIOSKI

Ocena doktryn wojen hybrydowych wskazuje, że zarówno Hoffman, jak i Gierasimow dostrzegają wiele elementów wspólnych w teorii wojen hybrydowych, a także elementy je różniące. Obydwaj analitycy podkreślają, że wojny hybrydowe charakteryzują się różnorodnością form i metod ich prowadzenia. Mają one nieregularny przebieg, a dowodzenie nimi odbywa się w zdecentralizowany sposób. Zaciera się stan wojny i pokoju oraz ciężko rozróżnić żołnierzy i cywilów. Coraz częściej spotykamy działania tzw. samotnych wilków, których rozpoznanie i wykrywanie nie jest łatwe. Stratedzy zajmujący się nowymi wojnami prognozują, że wojny te będą służyć do osiągania celów politycznych i propagandowych. Powyższą teorię może potwierdzić przebieg konfliktów na Ukrainie oraz wojna z tak zwanym Państwem Islamskim. W obydwu przypadkach bojownicy uczestniczący w wojnach hybrydowych posługiwali się najnowszymi technologiami o zastosowaniu wojskowym. Problematyka wojny hybrydowej zostanie omówiona poniżej, na podstawie genezy i przebiegu konfliktu na Ukrainie oraz wojny z Państwem Islamskim.

Przebieg konfliktu z Ukrainą oraz wojny z Państwem Islamskim

Analizowanie wojny hybrydowej w oparciu o teorię wojny Karla von Clausewitza nie zdaje egzaminu. Teoretyk ten opisywał konflikt z punktu widzenia strategii wojskowej dotyczącej logistyki, komunikacji, struktury itp. Do wojny hybrydowej bardziej przystaje stanowisko chińskiego myśliciela Sun Tzu, który patrzył na konflikt całościowo, a za podstawowe narzędzie walki uznawał informację. Zmylenie przeciwnika

mogło pozwolić na zwycięstwo bez wypowiedzenia wojny. Można to odnieść na przykład do polskiego gazoportu[4].
Poszukiwania wspólnych elementów obu wojen i na tej podstawie badanie ich struktury nie oddaje w pełni ich analogii. Wydaje się, że bardziej wiarygodne jest porównanie tych elementów i na tej podstawie budowanie odpowiedniego modelu wojny hybrydowej. Opiera się on głównie na celach, które mają bardzo zróżnicowany charakter oraz pobudki. To one właśnie pchają określoną stronę do tej wojny. Z łatwością można dostrzec, iż każdemu z tych konfliktów towarzyszą różne cele. W odniesieniu do Rosji chodzi o to, aby destabilizować sytuację na Ukrainie i nie dopuścić w przyszłości do integracji tego państwa z NATO i UE, natomiast Państwo Islamskie przyjęło cel tworzenia warunków do budowy globalnego kalifatu. Dlatego też dąży do zniszczenia Syrii oraz Iraku.
Jeżeli uznać, że Państwo Islamskie uciekło się do wojny hybrydowej z powodu braku sił klasycznych, to możemy stwierdzić, że w przypadku konfliktu na Ukrainie Rosja kieruje się takimi działaniami, które nie stanowią (jak na razie) podstaw do jej oskarżania o agresję zbrojną prowadzoną przeciwko Ukrainie. Rosja czyni wiele na rzecz odwrócenia uwagi społeczności międzynarodowej od konfliktu zbrojnego, który na obecnym etapie posiada charakter wojny hybrydowej. Wojna ta jest sposobem na obniżenie poziomu wojny klasycznej do sytuacji, w której możemy mówić o agresji poniżej progu wojny, oraz tworzy warunki do zacierania się pokoju i wojny. Analiza wojen hybrydowych wskazuje, że zawierają one zarówno wojskowe, jak i cywilne aspekty.

Militarne aspekty wojny hybrydowej

Ocena dotychczasowego przebiegu konfliktu na Ukrainie oraz działań Państwa Islamskiego wskazuje, że w obu przypadkach mamy do czynienia z tymi samymi lub podobnymi działaniami wojskowymi. Można do nich zaliczyć:
- działania regularne,
- działania nieregularne,
- akty terrorystyczne.

Sposób stosowania odpowiedniej formy działań ma charakter zmienny. Są one wykorzystywane na różnych etapach tych działań oraz z określoną intensywnością.
W przypadku Ukrainy możemy mówić o dwóch różnych fazach konfliktu. Pierwsza z nich dotyczy aneksji Półwyspu Krymskiego przez Rosję, druga zaś działań prowadzonych w rejonie Donbasu. W pierwszej sytuacji mieliśmy do czynienia z działaniami nieregularnymi realizowanymi przez służby specjalne Rosji pod przykryciem lokalnych oddziałów samoobrony. Zadaniem tych oddziałów było prowadzenie intensywnych działań psychologicznych, zaś w dalszej kolejności przejmowanie budynków administracji rządowej, infrastruktury krytycznej oraz jednostek wojskowych.
W drugiej fazie, która trwa cały czas, główny wysiłek agresorów został skupiony na destabilizacji południowo-wschodniej Ukrainy. Rosyjscy separatyści, rosyjscy ochotnicy oraz najemnicy z innych państw prowadzą regularne działania wojskowe z wykorzystaniem nowoczesnego sprzętu wojskowego, takiego jak czołgi, bojowe wozy piechoty, a także systemy obrony powietrznej. Dochodziło do wielu aktów terrorystycznych oraz porwań ukraińskich działaczy politycznych i społecznych wiernych władzy centralnej.
W przeciwieństwie do konfliktu ukraińskiego działania prowadzone przez Państwo Islamskie na obszarze Syrii oraz Iraku można podzielić na trzy fazy. Pierwsza z nich obejmowała lata 2009–2011 i charakteryzowała się asymetrią i nieregularnością oraz wykorzystaniem zamachów bombowych. Działania te były prowadzone przeciw wojskom amerykańskim oraz irackim. W latach 2012–2013 ISIS realizowało drugą fazę działań ukierunkowanych na stosowanie terroru wobec ludności cywilnej, kierując się zwłaszcza przesłankami religijnymi. Trzecia faza, która rozpoczęła się w 2014 r. i trwa do dziś, cechuje się prowadzeniem działań konwencjonalnych z wykorzystaniem sprzętu i uzbrojenia zdobytego w irackich i syryjskich bazach wojskowych.
Do działań wojskowych prowadzonych w ramach wojny hybrydowej można zaliczyć demonstracje siły i działania propagandowe stosowane cały czas wobec Ukrainy ze strony Federacji Rosyjskiej. Tworzenie nowych jednostek wojskowych i ich dyslokacja przy granicy ukraińskiej służą zastraszaniu ludności i wywoływaniu wśród niej niepokoju. Do działań wojskowych należy także zaliczyć wiele naruszeń przestrzeni powietrznej Ukrainy i wzmożone działania na morzu. Prowadzone ćwiczenia wojskowe o dużym rozmachu i w sposób nieplanowany mają dowodzić wysokich zdolności operacyjnych wojsk rosyjskich. W ostatnim okresie zostało zarządzone w sposób alarmowy sprawdzenie gotowości bojowej sił zbrojnych dyslokowanych przy granicy z Ukrainą.

Niemilitarne aspekty wojny hybrydowej

Skuteczność prowadzenia wojny hybrydowej w dużej mierze zależy od niemilitarnych aspektów jej przebiegu. Można do nich zaliczyć różne formy i metody, które kształtują negatywne nastroje i sieją zwątpienie wśród ludności cywilnej. Obniżają również wolę walki, co w przypadku działań wojennych odgrywa istotną rolę. Wszystkie niemilitarne działania agresora mają na celu doprowadzić do zakończenia konfliktu zgodnie z interesami agresora. O wpływie działań niemilitarnych na skuteczność wojny hybrydowej zaświadcza wyraźnie prowadzona przez Federację Rosyjską wojna z Ukrainą. Analiza jej przebiegu wskazuje, iż wśród niemilitarnych metod prowadzenia wojny hybrydowej można wyróżnić:
- wielokierunkowe działania dyplomatyczne;
- presję ekonomiczną;
- działania ofensywne w cyberprzestrzeni;
- dużą aktywność służb specjalnych.

Skuteczność stosowania wojny hybrydowej

Wśród analityków zajmujących się badaniem przesłanek prowadzenia wojny hybrydowej często jest zadawane pytanie o okoliczności podjęcia decyzji o jej rozpoczęciu. Okazuje się bowiem, iż musi zaistnieć wiele warunków, aby agresor osiągnął założone przez siebie cele. Odpowiedź na tak sformułowane pytanie można uzyskać, dokonując oceny ostatnich wydarzeń na Ukrainie, w Syrii oraz w Iraku.
Pierwszą okolicznością pozwalającą podejmować decyzje o rozpoczęciu i prowadzeniu wojny hybrydowej jest poważny kryzys w państwie będącym celem ataku. Takie państwo

okazuje symptomy państwa upadłego i nie jest w stanie podejmować skutecznych działań zwróconych przeciw agresorowi. Drugim warunkiem umożliwiającym agresorowi podjęcie decyzji o wojnie hybrydowej jest istnienie mniejszości narodowych lub religijnych, które solidaryzują się z potencjalnym agresorem. Współczesne technologie informatyczne pozwalają w bezpośredni sposób dotrzeć do pojedynczego odbiorcy informacji wśród ludności kraju będącego ofiarą agresji. Strona napadająca posiada wpływ na ilość i jakość różnych oddziaływań propagandowych wpływających na wolę walki strony napadniętej. To zjawisko można nazwać natarciem propagandowym, a jego wpływ na stronę napadniętą jest bardzo duży.
Działania agresora mają zintegrowany charakter nakierowany na osiąganie założonych celów, które oprócz dużej liczby zabitych charakteryzują się dużym wydźwiękiem propagandowym i psychologicznym. Coraz częstsze wojny hybrydowe rodzą pytanie o przeciwdziałanie im.

Jak odpowiedzieć na wojnę hybrydową?

Problem wojen hybrydowych manifestujących się konfliktem na Ukrainie wywołał głębokie poruszenie w Sojuszu Północnoatlantyckim oraz w Unii Europejskiej. W reakcji na ten konflikt NATO postanowiło podjąć się ambitnego zadania polegającego na opracowaniu zbioru narzędzi służących do powstrzymywania wojny hybrydowej i obrony przed przeciwnikami wykorzystującymi tę strategię[5].
Przedstawiciele Sojuszu NATO dostrzegli, że wojna hybrydowa może mieć charakter wielopoziomowy i być wymierzona w społeczeństwo państwa będącego ofiarą agresji. Agresor często sięga po ukryte środki, aby uniemożliwić przypisanie winy i działania odwetowe.
Aktualna polityka NATO w zakresie powstrzymywania wojny hybrydowej polega na szybkiej reakcji zbrojnej[6]. Polityka ta jakkolwiek wydaje się racjonalna, to może przysparzać kłopoty realizacyjne w związku z procesem podejmowania decyzji w ramach Sojuszu Północnoatlantyckiego. Konflikt w postaci wojny hybrydowej może się rozwijać niepostrzeżenie, co wymaga natychmiastowej reakcji. Zapobieganie jest chyba najlepszym sposobem przeciwdziałania wojnie hybrydowej. Nieregularne zagrożenia są znacznie trudniejsze do opanowania, gdy przerodzą się w otwarte próby destabilizacji[7]. Sojusz Północnoatlantycki i UE zdecydowały o zacieśnieniu współpracy na rzecz przeciwdziałania wojnom hybrydowym. Przyjęto, że dotychczasowe działania w ramach reagowania kryzysowego są właściwą płaszczyzną do podjęcia przez obie organizacje konkretnych działań.
Stratedzy Sojuszu Północnoatlantyckiego dostrzegli, że aby skutecznie bronić się przed wojną hybrydową, Sojusz będzie musiał rozbudować swoje zdolności oraz wzmocnić współpracę z UE. Sekretarz Generalny Sojuszu Jens Stoltenberg uznał, że najważniejszym elementem wojny hybrydowej jest dezinformacja, zatem bronią przeciwko niej powinna być informacja.
Wojna hybrydowa na Ukrainie jest niczym innym niż znaną od wieków walką partyzancką, nakierowaną między innymi na walkę o dostęp do najnowszych technologii, często nowszych od tych, z których korzysta zwalczana strona rządowa. Nie jest to wojna, która opiera się na zasadach doktryny Clausewitza, chociażby ze względu na cechy charakteryzujące jej przebieg. Trudno w niej dopatrywać się frontu, gdyż pole walki jest rozproszone. Na początku wojny nie było wiadomo, kim są napastnicy. Pojawiały się mylące informacje, iż są to komandosi przebrani w cywilne ubrania, żołnierze misji pokojowej czy może ekipy konwojów humanitarnych.
Rosyjskie władze pytane o broń, którą posługiwali się napastnicy, stwierdziły, iż istnieje duże prawdopodobieństwo, że kupili ją w sklepie. Wypowiedź ta wskazywała na to, że Rosja ucieka się do nowej formy wojny, która stanowi realizację zadań wynikających z zapisów nowej doktryny wojskowej Federacji Rosyjskiej przyjętej w 2010 r. Przypuszczenia te potwierdził w lutym 2013 r. szef Sztabu Generalnego Federacji Rosyjskiej Walerij Gierasimow, który powiedział, że: „granice między wojną i pokojem stają się coraz bardziej zamazane”[8]. Stwierdził także, że wszystkie te działania mogą być uzupełniane przez sterowane wybuchy gniewu lokalnej ludności, działalność V kolumny oraz zamaskowanych sił zbrojnych”[9]. Wystąpienia „zielonych ludków” są zatem zaplanowanym i przemyślanym wystąpieniem zaakceptowanym przez rosyjskich dowódców wojskowych.
Według Amerykańskiego Departamentu Obrony wojny hybrydowe to nieregularne działania wojenne, „preferowanie niebezpośrednich i asymetrycznych metod, które mogą łączyć w sobie cały zestaw możliwości, zarówno wojskowych, jak i innego typu, a mających na celu doprowadzenie do erozji siły przeciwnika, jego wpływów i woli”[10].

„Wojna hybrydowa może być konfliktem, w którym wojska będą ukrywać się za anonimowymi ludźmi; prowadzącymi działania terrorystyczne, operacje, które trudno zakwalifikować. Wojny te określa także słowo dwuznaczność, w której śmiało możemy zadać pytanie, czy zielone ludziki to uzbrojeni cywile, czy też żołnierze. Armia ta nazywana jest »armią duchów« i stanowi wielką siłę wsparcia działań separatystów na zmieniającym się froncie[11].
Wojna hybrydowa w drugiej dekadzie XXI w. przedstawia się jako idealna alternatywa dla zaatakowania lub zdestabilizowania innego kraju przez państwa, które z różnych względów nie chce angażować się w otwarty konflikt zbrojny. Wojna hybrydowa jest we współczesnych warunkach jednym z największych zagrożeń bezpieczeństwa międzynarodowego.
Zagrożenia hybrydowe oraz ich wzrastająca różnorodność i natężenie skłoniły Sojusz NATO do poważnego traktowania pojawiających się zagrożeń dla bezpieczeństwa państw NATO. Dlatego też w grudniu 2015 r. NATO przyjęło strategię reagowania na wojnę hybrydową. Sekretarz Generalny Sojuszu Jens Stoltenberg powiedział, iż: »dzisiaj przyjęliśmy strategię walki z zagrożeniami hybrydowymi. Jako pierwsze na te zagrożenia powinny odpowiedzieć państwa NATO, które zetkną się z nimi bezpośrednio. Ta sfera wydaje się także perspektywiczna dla współpracy między Unią Europejską i NATO, przed którymi stają jednakowe wyzwania dla bezpieczeństwa«”[12].

Na słowa Sekretarza Generalnego zareagowała Federica Mogherini, przedstawicielka UE ds. zagranicznych i polityki bezpieczeństwa, która złożyła deklarację, że Unia opracuje strategię radzenia sobie z pełzającą wojną hybrydową. Zapewniła także, że „służba zagraniczna UE we współdziałaniu z Komisją Europejską rychło przedstawią koncepcję reagowania na zagrożenia hybrydowe. Będzie się ona zasadzać na monitoringu i analizie. Tę koncepcję powinniśmy opracować, ściśle współpracując z NATO”[13].

Wyrazem poważnego podejścia do wcielenia postanowień strategii NATO w części dotyczącej zagrożeń hybrydowych było ćwiczenie Anakonda-16, podczas którego przećwiczono scenariusz wspólnej obrony w sytuacji wojny hybrydowej.

Analiza warunków pozwalających na efektywne prowadzenie wojny hybrydowej pokazała, że są na nią narażone przede wszystkim państwa pogrążone w głębokim kryzysie, których społeczeństwo jest podzielone i skonfliktowane na tle politycznym, etnicznym lub religijnym. W tym kontekście obawy państw UE dotyczące objęcia ich wojną hybrydową przez Rosję są przesadzone. Oczywiście nie można wykluczyć zastosowania przez Rosję któregoś z elementów wojny hybrydowej wobec nich. Należy jednak pamiętać, że wtedy ma się do czynienia nie z wojną hybrydową, ale – w zależności od użytych środków – z wojną informacyjną, działalnością dywersyjno-sabotażową czy wojną handlową. Aby mówić o wojnie hybrydowej, musi zostać spełniony jeden ważny warunek, na który zwracali uwagę zarówno Hoffman, jak i Gierasimow. Chodzi tu o jednoczesne użycie środków militarnych, niemilitarnych oraz propagandowych na poziomie strategicznym, operacyjnym i taktycznym prowadzenia konfliktu[14].

Przykładem państwa, które jako strona silniejsza prowadzi wojnę hybrydową ze słabszym przeciwnikiem, jest Rosja i jej działania na Ukrainie.

W tej wojnie można wyróżnić cztery fazy:

- dywersję polityczną,
- budowanie pozycji społecznej i politycznej separatystów,
- interwencję zbrojną,
- odstraszanie.

Cechę charakterystyczną wojny hybrydowej stanowi zachodzenie tych faz na siebie. Ich intensywność jest różna. Pomimo wyraźnych oznak udziału regularnych sił zbrojnych władze Rosji oficjalnie zaprzeczają udziałowi w wojnie[15].

Przeprowadzona analiza wojen hybrydowych pozwala stwierdzić, że mają one charakter wielowymiarowy, sprowadzający się do jednoczesnego oddziaływania w sferze militarnej, informacyjnej, cybernetycznej i ekonomicznej. Głównym polem bitwy będzie umysł pojedynczego człowieka, wybranych grup społecznych i elit władz, dlatego wojna nowej generacji będzie nierozerwalnie związana z działaniami dezinformacyjnymi i psychologicznymi.

Ewolucja wojen hybrydowych wskazuje, że nie ograniczają się one tylko do aktorów pozapaństwowych i do stereotypu myślowego, że to słabszy przeciwnik wykorzystuje tę formę działań przeciwko silniejszemu. Doświadczenia wyniesione z działań w Iraku i Afganistanie, a przede wszystkim na Ukrainie, wskazują, że to państwa mogą „przekształcić regularne pododdziały sił zbrojnych w formacje nieregularne, które będą dysponować klasycznymi zdolnościami i adaptować nową taktykę działania, a następnie wspierać pododdziały regularne[16].

Zdaniem byłego szefa Biura Bezpieczeństwa Narodowego Stanisława Kozieja system bezpieczeństwa narodowego w Polsce trzeba dostosować do nowego rodzaju zagrożeń, które pojawiły się podczas wojny na Ukrainie[17].

Przygotowanie systemu obronnego państwa w zakresie przeciwstawienia się wojnie hybrydowej jest zadaniem priorytetowym ze względu na pojawianie się nowych zagrożeń asymetrycznych. Wszystko wskazuje na to, że w przypadku wojny hybrydowej musielibyśmy jej stawić czoła samodzielnie. Jest bowiem mało prawdopodobne, aby w gronie państw NATO uzyskać konsensus co do wspólnego działania w razie wojny hybrydowej.

Były Szef Biura Bezpieczeństwa Narodowego zaznaczył, że należy wyspecjalizować armię, ale także wykorzystać inne służby w systemie bezpieczeństwa, takie jak np. Policję czy straże, ponadto zadbać o wzmożone zainteresowanie całego społeczeństwa, organizacji społecznych i proobronnych. Dobrą zapowiedzią tego typu działań jest decyzja rządu o utworzeniu wojsk obrony terytorialnej.

Dotychczasowa polityka Rosji nie wskazuje na to, aby wojna hybrydowa objęła Polskę, gdyż wiązałoby się to z rozpoczęciem operacji przez NATO, co byłoby nieracjonalne. Nie można natomiast wykluczyć, iż mogą zaistnieć jakieś próby działania przeciwko krajom bałtyckim zamieszkiwanym przez dużą mniejszość rosyjską. Działania te mogłyby przybrać postać aktywności tzw. zielonych ludzików – na wzór Krymu.

Rodzi się również pytanie o przygotowanie sojuszu NATO do przeciwstawienia się wojnie hybrydowej. Sekretarz generalny Sojuszu Jens Stoltenberg przyznał niedawno w rozmowie z „Newsweekiem”, iż NATO jest przygotowane na całe spektrum możliwych zagrożeń, które miałyby wpływ na bezpieczeństwo terytorium Sojuszu, w tym na wojnę hybrydową. Na szczycie w Walii uzgodniono, że zostaną opracowane ćwiczenia, które dotyczą zagrożeń związanych z wojną hybrydową.

> Współczesne działania wojenne o charakterze hybrydowym w coraz większym stopniu obejmują wojnę w cyberprzestrzeni. Wskazuje się na potrzebę ich technologicznego i operacyjnego dowartościowania. Niektórzy stratedzy wojskowi ogłosili nawet potrzebę utworzenia wojsk informacyjnych. W planach tworzenia tych wojsk uciekają się do rozwiązań stosowanych zwłaszcza w armii amerykańskiej, w NATO oraz w Federacji Rosyjskiej. Obecne rozwiązania dotyczące „armii informacyjnej” są punktowe, bez żadnych oznak rozwiązań systemowych. Największy postęp w tworzeniu armii informacyjnych można zaobserwować w Marynarce Wojennej Stanów Zjednoczonych, w której pododdziały działają bez ich wzajemnych sprzężeń systemowych.

Niemniej jednak Amerykanie zakładają, że muszą wypromować swoją przewagę w cyberprzestrzeni na wzór przewagi w walkach na lądzie, w powietrzu, na morzu oraz z Hamasem. Aktualny sposób kształtowania wojsk informacyjnych ma – w ocenie strategów amerykańskich – charakter początkowy. Nie zaprzeczają jednak, że bezpieczeństwo cyberprzestrzeni odgrywa coraz to większą rolę w systemie bezpieczeństwa Stanów Zjednoczonych. Odnosi się to zarówno do sfery cy-

wilnej, jak i wojskowej. Odnotowane w ostatnim okresie włamania do systemów teleinformatycznych wskazują na coraz większe oddziaływanie w przestrzeni cybernetycznej nie tylko w wymiarze taktycznym, ale także strategicznym. Radioelektryczne obezwładnianie systemów teleinformatycznych może prowadzić do ich unieszkodliwienia, a tym samym do uczynienia ich niesprawnymi do prowadzenia i dowodzenia.

Ostatnio przeprowadzone przez Federację Rosyjską ćwiczenia „Zapad" jednoznacznie wskazują na znaczny postęp tego państwa w rozwoju broni niekinetycznej, w tym systemów pozwalających na zapewnienie bezpieczeństwa w cyberprzestrzeni. Okazuje się, że komputer może być ważnym elementem wspierającym prowadzenie operacji połączonych w warunkach wyraźnej asymetrii zagrożeń.

Pojęcie bezpieczeństwa cyberprzestrzeni, jako stały element debaty dotyczącej bezpieczeństwa narodowego i międzynarodowego, pojawiło się w połowie lat 90. ubiegłego wieku w Stanach Zjednoczonych. Tematyka bezpieczeństwa w odniesieniu do cyberprzestrzeni stanowiła wówczas przedmiot rozważań dotyczących głównie zagrożeń systemów teleinformatycznych należących do infrastruktury krytycznej państwa. Zainteresowanie problemem zagrożeń cyberprzestrzeni (określanych mianem cyberzagrożeń) było z jednej strony wynikiem zmiany paradygmatu bezpieczeństwa po zakończeniu zimnej wojny i wzrostu ryzyka zagrożeń pozamilitarnych i asymetrycznych, z drugiej zaś – skutkiem szybkiego rozwoju i upowszechniania technologii informacyjnej i komunikacyjnej (ang. *Information and Communications Technology*, ICT). Rozważania i działania prowadzone wówczas w USA były naśladowane przez inne wysoko rozwinięte państwa.

Poszczególne zagadnienia z obszaru bezpieczeństwa cyberprzestrzeni, takie jak: cyberprzestępczość, hacking, cyberterroryzm, bezpieczeństwo teleinformatycznej infrastruktury krytycznej, zaczęły się pojawiać w dokumentach politycznych i doktrynalnych[18].

Do zamachu terrorystycznego w Stanach Zjednoczonych w 2001 r. problematyce bezpieczeństwa cyberprzestrzeni nie poświęcono należytej uwagi. Swoistego rozgłosu ta kwestia nabrała po ukazaniu się pracy Dana Vertona zatytułowanej *Black Ice. Niewidzialna groźba cyberterroryzmu*. Wydano ją również w Polsce. Przyczyniła się w znacznej mierze do popularyzacji zagadnień cyberterroryzmu i utrwaliła na długi czas postrzeganie bezpieczeństwa cyberprzestrzeni przez pryzmat ataków na infrastrukturę krytyczną. Do tej pory takie ataki odbywały się rzadko, a ich skutki nie miały charakteru kaskadowego. W międzyczasie na podstawie ustawy specjalnej „USA PATRIOT Act" i w imię wojny USA z terroryzmem zaczęły się rozwijać programy globalnej, masowej inwigilacji, o czym opinia publiczna dowiedziała się dopiero dziesięć lat później.

Schyłek pierwszej dekady XXI w. zaowocował pojawieniem się przypuszczeń dotyczących tworzenia przez kolejne państwo oddziałów sił zbrojnych przeznaczonych do walki w cyberprzestrzeni. Znalazło to także wyraz w Koncepcji Strategicznej NATO, ogłoszonej w 2010 r. Uznano wówczas, że ataki z wykorzystaniem cyberprzestrzeni stanowią zagrożenie dla administracji rządowej, biznesu, gospodarki, a potencjalnie także transportu, sieci dostaw i innej infrastruktury krytycznej, mogące negatywnie wpływać na dobrobyt oraz bezpieczny rozwój strefy euroatlantyckiej[19].

W ostatnim okresie daje się zauważyć zmianę optyki zagrożeń cyberprzestrzeni państwa. D.S. Reveron już w 2012 r. ocenił, iż najpoważniejszym zagrożeniem cyberprzestrzeni państwa są cyberataki przeprowadzone przez inne państwo[20]. Potwierdzeniem tej tezy było opublikowanie przez Juliana Assange oraz Edwarda Snowdena w 2013 r. niejawnych dokumentów (w tym ściśle tajnych materiałów instytucji rządowych z USA) ukazujących skalę i charakter niejawnych aktywności państw w cyberprzestrzeni, w tym szkodliwego oddziaływania. Mimo ujawnienia w 2013 r. przez Edwarda Snowdena faktu prowadzenia tego rodzaju działań i szoku opinii światowej nie zostały one wstrzymane. W miarę zachodzących przekształceń środowiska bezpieczeństwa cyberprzestrzeni, państwa zaczęły również rozwijać struktury ofensywne, a charakter działań na rzecz bezpieczeństwa cyberprzestrzeni zaczął się zmieniać z reaktywnego na proaktywny. Bezpieczeństwo cyberprzestrzeni państwa wiązano wówczas głównie z ochroną infrastruktury krytycznej. Dostrzeżono również, że stanowi ono jeden z elementów bezpieczeństwa narodowego.

Pod koniec pierwszej dekady XXI w. wiele państw ogłosiło swoje strategie bezpieczeństwa cyberprzestrzeni. Dostrzeżono wówczas rosnącą skalę zjawiska cyberprzestępczości i jego wpływ na gospodarkę państwa. Następna zmiana w postrzeganiu bezpieczeństwa cyberprzestrzeni nastąpiła w 2013 r., kiedy ujawniono zjawisko inwigilacji przez Stany Zjednoczone.

Wojna hybrydowa na Ukrainie ukazała nowe oblicze wojny, prowadzonej również na płaszczyźnie cyberprzestrzeni, która jest płaszczyzną intensywnych działań propagandowo-dezinformacyjnych.

W tej sytuacji rodzi się pytanie na temat zapewnienia bezpieczeństwa cyberprzestrzeni RP. Do 2016 r. administracja rządowa RP nie miała w istocie wizji sposobu zapewniania bezpieczeństwa cyberprzestrzeni państwa, czego wyrazem jest bezskuteczność prowadzonych od 2008 r. działań na rzecz opracowania strategii bezpieczeństwa cyberprzestrzeni RP. Pewną zapowiedzią poprawy tego stanu jest wypowiedź Ministra Obrony Narodowej RP o utworzeniu wojsk cybernetycznych, które będą liczyć ponad tysiąc żołnierzy. Ich powstanie pochłonie – zgodnie z zapowiedzią – 2 mld zł. Informacja o utworzeniu tego rodzaju wojsk została przekazana przez Ministra Obrony Narodowej w Krakowie podczas III Europejskiego Forum Cyberbezpieczeństwa CYBERSEC 9 października 2017 r.[21]

W swoim wystąpieniu Minister Obrony Narodowej podkreślił, że we współczesnym świecie cyberprzestrzeń jest obszarem działań wojennych „w nie mniejszym stopniu niż ma to miejsce w przypadku lądu, morza, powietrza i przestrzeni kosmicznej". Poinformował także o powołaniu biura ds. organizacji wojsk cybernetycznych oraz pełnomocnika MON ds. bezpieczeństwa cyberprzestrzeni. Zauważył, że w dziedzinie technologii „trwa ciągły wyścig zbrojeń, który przynosi coraz więcej kompleksowych zagrożeń". Nie istnieją instytucje albo organizacje, które nie byłyby narażone na ataki w sferze cybernetycznej. Podkreślił, że zagrożone może być

nawet funkcjonowanie całego państwa – jeżeli chcemy budować potencjał w cyberprzestrzeni, musimy zidentyfikować naturę zagrożeń[22].

Podał także kilka przykładów ataków w cyberprzestrzeni. Zaliczył do nich: paraliż stron internetowych parlamentu, ministerstw i banków w Estonii 2007 r., ataki hakerskie przed Szczytem NATO w Warszawie i podczas niego, działania rosyjskich hakerów przeciw elektrowniom w amerykańskim stanie Vermont oraz aktywność północnokoreańskiej grupy Lazarus, która próbowała zdestabilizować globalny system finansowy. Wspomniał także o wirusie „Pietia", który wyrządził szkody na Ukrainie, oraz o działaniach rosyjskich hakerów podczas referendum w Katalonii[23].

Według Ministra Obrony Narodowej przytoczone powyżej przypadki nie są indywidualnymi działaniami hakerów komputerowych. Działania te wymagają złożonego procesu organizacji, aktywnego wsparcia państw stojących za tymi atakami. To sprawia, że rządy muszą coraz częściej dbać o swoje bezpieczeństwo w cyberprzestrzeni. Według Ministra zagrożenie dla cyberprzestrzeni RP przybiera większego znaczenia w warunkach wzmacniania przez Federację Rosyjską wysiłku na rzecz wzrostu skuteczności działań w cyberprzestrzeni. Prezydent Federacji Rosyjskiej Władimir Putin podpisał nową doktrynę bezpieczeństwa, tworząc wojska informacyjne. Informacja tym samym stała się bronią, jak stwierdził Minister Antoni Macierewicz.

Do zwiększenia działań na rzecz bezpieczeństwa cyberprzestrzeni RP przyczyniły się w znacznej mierze czynniki zewnętrzne – obowiązki wynikające z członkostwa Polski w UE i NATO. Byłoby nieprawdą stwierdzenie, że dotychczasowe wysiłki na rzecz opracowania strategii bezpieczeństwa w cyberprzestrzeni RP nie dały efektu. Wyrazem tego jest chociażby *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015*, która została opatrzona słowem wstępnym Prezydenta: „Doktryna cyberbezpieczeństwa RP wskazuje strategiczne kierunki działania dla zapewnienia bezpieczeństwa Rzeczpospolitej Polskiej w cyberprzestrzeni. Jednocześnie powinna być traktowana jako jednolita podstawa koncepcyjna, zapewniająca spójne i kompleksowe podejście do zagadnień cyberochrony i cyberobrony jako wspólny mianownik dla działań realizowanych przez podmioty administracji publicznej, służby bezpieczeństwa i porządku publicznego, siły zbrojne, sektor prywatny oraz obywateli"[24].

[1] H. Welzer, *Wojny klimatyczne*, Wydawnictwo Krytyki Politycznej, Warszawa 2000, s. 72–174.

[2] A. Gruszczak, *Hybrydowość współczesnych wojen – analiza krytyczna*, w: *Asymetria i hybrydowość – stare armie wobec nowych konfliktów*, red. B. Zapała, W. Sokała, Biuro Bezpieczeństwa Narodowego, Warszawa 2011, s. 11.

[3] Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości?*, „Przegląd Bezpieczeństwa Wewnętrznego – Wydanie Specjalne" 2015, s. 42.

[4] W. Jakubik, *Jak odpowiedzieć na wojnę hybrydową*, w: *Wiadomości Onet*, wiadomosci.onet.pl/jak-odpowiedziec-na-wojne-hybrydowa/c4thcpp [dostęp: 4.08.2016 r.].

[5] P. Pindják, *Powstrzymywanie wojny hybrydowej szansą na współpracę NATO i Unii Europejskiej?* https://www.nato.int/docu/review/2014/Also-in-2014/Detterring-hybrid-warfare/PL/index/htm [dostęp: 4.12.2017 r.].

[6] Tamże.

[7] Tamże.

[8] P. Górka, *Wszystko może stać się bronią, czyli co się dzieje na Ukrainie*, www.pch24.pl [dostęp: 4.12.2017 r.].

[9] Tamże.

[10] *Wojna hybrydowa – co to takiego?* http://orwellsky.blog.onet.pl/2012/02/27/wojna-hybrydowa-co-to-takiego/ [dostęp: 8.12.2017 r.]

[11] Cezary Szczepaniuk, *Dziwna wojna na Ukrainie przykładem wojny hybrydowej*, http://blog.centruminicjatyw.org/2015/03/wojna_hybrydowa/ [dostęp: 8.12.2017 r.].

[12] *NATO przyjmuje strategię reagowania na wojnę hybrydową*, https://kresy.pl/wydarzenia/nato-przyjmuje-strategie-reagowania-na-wojne-hybrydowa [dostęp: 4.12.2017r.].

[13] Spotkanie NATO i UE 7.12.2015. r. poświęcone przyjęciu strategii reagowania na wojny hybrydowe, zob. *NATO przyjmuje strategię reagowania na wojnę hybrydową*, https://kresy.pl/wydarzenia/nato-przyjmuje-strategie-reagowania-na-wojne-hybrydowa/ [dostęp: 8.12.2017 r.].

[14] Ł. Skoneczny, *Wojna hybrydowa – wyzwanie przyszłości? Wybrane zagadnienia,* w: „Przegląd Bezpieczeństwa Wewnętrznego – Wydanie Specjalne" 2015, s. 12.

[15] A. Kuk, *Kanwa wywiadu agenturalnego*, Warszawa 1994, s. 19.

[16] M. Banasik, R. Parafianowicz, *Teoria i praktyka działań hybrydowych*, „Zeszyty naukowe AON" 2015, 2/99, s. 10–11.

[17] S. Koziej, *Musimy się przygotować na wojnę hybrydową*, http://www.newsweek.pl/polska/koziej-musimy-sie-przygotowac-na-wojne-hybrydowa,artykuly,358198,1.html [dostęp: 8.12.2017 r.].

[18] M. Dunn, Comparative Analysis of Cybersecurity Initiatives Worlwide Thematic Meeting of Geneva 28 June – 1 July 2005, https://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf [dostęp: 11.12.2017 r.].

[19] *Koncepcja strategiczna NATO*, BBW, Warszawa 2012.

[20] D.S. Reveron, *Cyberspace and National Security. Threats, Opportunities, and Power in Virtual World,* Georgetown University Press, Washington 2012.

[21] M. Wosion-Czoba, *Macierewicz: wojska cybernetyczne mają liczyć przynajmniej 1 tys. żołnierzy,* http://www.pap.pl/aktualnosci/news,1117038,macierewicz-informacja-jedna-z-najwazniejszych-broni-naszego-przeciwnika.html [dostęp: 8.12.2017 r.].

[22] Tamże.

[23] Tamże.

[24] *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej 2015*, en.bbn.gov.pl/ftp/dok.01/DCB.pdf [dostęp: 5.12.2017 r.].

Summary

Threats of cyberspace as an element of a hybrid war

A modern warfare is characterrized by mixing a range of methods which are know as a sublimal war. The most frequent form of the sublimal war are hybrid wars. The annexation of Crimea and a continuous warfare in the Eastern Ukraine are the examples of a continuous warfare. Lately, there has been a growing interest in a safety of cyberspace. The cyberspace safety was part of the most recent military training known as ZAPAD carried out by the Russian Federation. In view of the modern development sit is necessary to increase the knowledge about the cyberspace sphere of safety.

ANALIZA KRYMINALNA

w dobie społeczeństwa informacyjnego

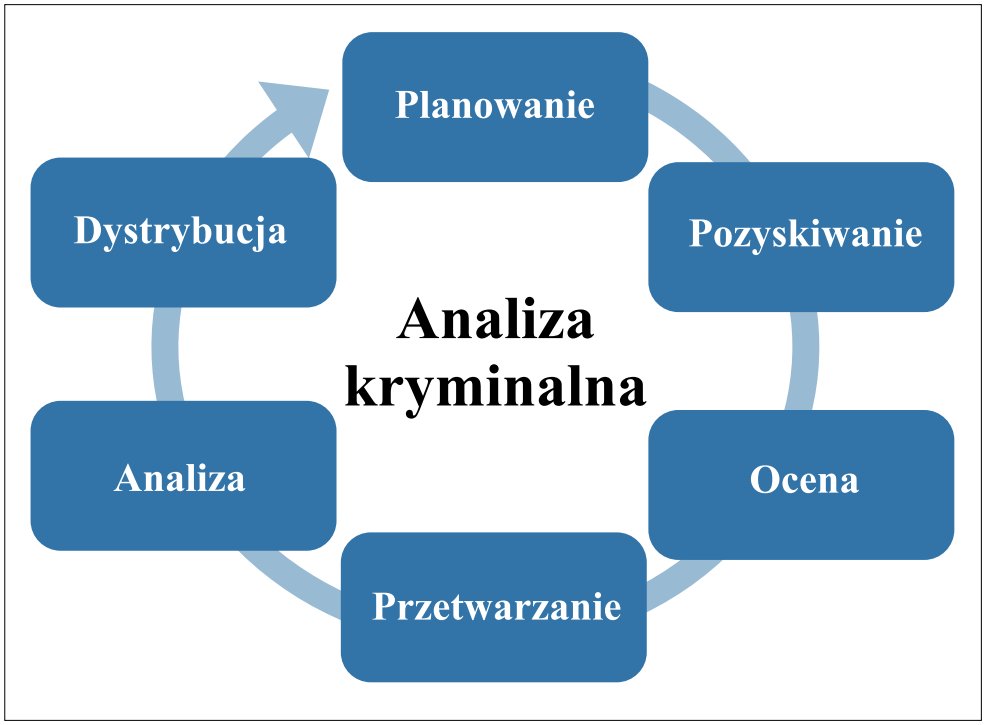
kom. Rafał Świeżak

Ekspert Wydziału Analizy Kryminalnej
Biura Wywiadu i Informacji Kryminalnej
Komendy Głównej Policji

Rozwój przestępczości komputerowej i przenoszenie do cyberprzestrzeni przestępczości tradycyjnej (np. narkotykowej) stawia organy powołane do zwalczania przestępczości przed zupełnie nowego rodzaju wyzwaniami. Narzędziem pomocnym w walce z tymi zjawiskami może być analiza kryminalna rozumiana jako poszukiwanie różnego rodzaju powiązań pomiędzy pozornie niepowiązanymi faktami w celu wykrycia sprawcy bądź wskazania nowego kierunku działań wspomagających proces wykrywczy. Sprawy, które warto poddawać analizie, to w szczególności sprawy wielowątkowe, o dużym stopniu skomplikowania, ciężarze gatunkowym oraz o dużym zasięgu terytorialnym. Współcześnie analiza kryminalna opiera się na przetwarzaniu dużych ilości danych (w tym metadanych) w celu identyfikacji powiązań pomiędzy różnymi obiektami i konstruowania na tej podstawie hipotez i wniosków.

Szybki rozwój i globalna dostępność technologii teleinformatycznych (ICT – Information and Communication Technologies), m.in. Internetu, pamięci przenośnych, dysków twardych, a także komputerów osobistych, serwerów, sieci komputerowych, aplikacji informatycznych i złożonych systemów związanych z przetwarzaniem i przesyłaniem danych (IT – Information Technology), a co za tym idzie – rozwój nowego rodzaju przestępczości – przestępczości komputerowej (cyberprzestępczości), stanowią obecnie ogromne wyzwanie dla analityków kryminalnych na całym świecie. Cyberprzestępczość jest kojarzona głównie z osobami przełamującymi zabezpieczenia oprogramowania komputerowego (hacker). Tymczasem do cyberprzestrzeni coraz częściej migruje tradycyjna przestępczość, na przykład pornografia dziecięca czy handel narkotykami. Niestety świadomość zagrożeń związanych z przestępczością komputerową jest, ogólnie rzecz biorąc, wciąż nikła, a wykrycie sprawcy niejednokrotnie bardzo trudne. Niezwykle pomocne w zwalczaniu cyberprzestępczości może być wykorzystanie jednego z najskuteczniejszych i najnowocześniejszych narzędzi w pracy wykrywczej Policji – analizy kryminalnej.

Początki współczesnej analizy kryminalnej sięgają lat sześćdziesiątych i początku lat siedemdziesiątych XX w., kiedy to po raz pierwszy w Stanach Zjednoczonych opracowano metodologię stosowania prostego języka symboli służącego do wizualizacji zawiłych danych w formie diagramów w walce z przestępczością zorganizowaną (Anacapa Science Program). W 1992 r. w Zutphen w Holandii, w ramach powołanej w 1986 r. przez Radę Europejską wewnętrznej grupy do spraw bezpieczeństwa TREVI III (fr. *Terrorisme, Radicalisme, Extremisme, Violence Internationale*) do walki z przestępczością zorganizowaną, powstał zespół ekspertów, który właściwie zajmował się tymi samymi problemami, co program naukowy ANACAPA. W 1994 r. Europejski Komitet Interpolu utworzył grupę roboczą do spraw analizy kryminalnej, która w 1997 r. wydała pierwszą w Europie broszurę o analizie kryminalnej *Crime Analysis Booklet*. W Interpolu także zdefiniowano analizę kryminalną: iden-



tyfikacja i udostępnianie wglądu w relacje między danymi o przestępstwach a innymi potencjalnie istotnymi danymi, w celu ich wykorzystania przez organy ścigania i sądownictwo.

W 1999 r. na spotkaniu w Tampere liderzy krajów członkowskich Unii Europejskiej podjęli decyzję, zgodnie z którą państwa członkowskie i kandydujące do wstąpienia do Unii Europejskiej, w tym Polska, w celu zwiększenia skuteczności zwalczania poważnej i zorganizowanej przestępczości powinny współpracować i stopniowo budować oraz rozwijać już istniejące struktury analityczne w służbach policyjnych. Na tej podstawie została opracowana „Strategia wdrożenia i funkcjonowania struktur wywiadu i analizy kryminalnej w polskiej Policji". Pierwsze komórki analizy kryminalnej w Polsce zostały utworzone w 2001 r. Opracowany w 2004 r. Krajowy Model Wywiadu Kryminalnego, zgodnie z przyjętymi założeniami i kierunkami, został dostosowany do standardów Unii Europejskiej. Dotyczyło to zarówno realizacji analiz operacyjnych, strategicznych, jak i procedury naboru oraz kształcenia analityków kryminalnych, których pierwowzorem stał się model opracowany na podstawie doświadczeń szkoleniowych realizowanych w ramach umów twinningowych w 2000 i 2001 r. przez ekspertów z Holandii i Wielkiej Brytanii. W przyjętym modelu wywiadu kryminalnego pierwszorzędne znaczenie ma planowanie, pozyskiwanie informacji, ocena, gromadzenie i przetwarzanie informacji, analiza informacji oraz właściwe jej prezentowanie i przekazywanie, wspomaganie ważniejszych postępowań oraz wskazywanie potencjalnych kierunków zagrożenia przestępczością i wytyczanie kierunków przeciwdziałania i zwalczania przestępczości.

Analiza kryminalna to analizowanie informacji, poszukiwanie różnego rodzaju powiązań pomiędzy pozornie niepowiązanymi faktami w celu wykrycia sprawcy bądź wskazania nowego kierunku działań wspomagających proces wykrywczy. W praktyce najczęściej sprowadza się to do przetwarzania dużej ilości danych w oparciu o ustaloną metodologię i konstruowania hipotez i wniosków. Podstawą metod i technik analizy kryminalnej są graficzne wizualizacje w formie wykresów, diagramów, map, statystyk i raportów przedstawionych w prostej i czytelnej formie.

Wyspecjalizowane komórki analizy kryminalnej w Polsce funkcjonują na poziomie Komendy Głównej Policji, Centralnego Biura Śledczego Policji oraz komend wojewódzkich. Opisując ich zadania, można ogólnie powiedzieć, że praca ta ma charakter typowo „usługowy". Jednostki organizacyjne Policji, prokuratury czy sądy zgłaszają swoje potrzeby w zakresie analiz dotyczące prowadzonych postępowań.

Z wnioskiem o wykonanie analizy kryminalnej może wystąpić kierownik komórki organizacyjnej służby kryminalnej lub śledczej albo osoba przez niego upoważniona – w Komendzie Głównej Policji, Centralnym Biurze Śledczym Policji, komendach wojewódzkich i Komendzie Stołecznej Policji. Natomiast w komendach powiatowych, miejskich i rejonowych Policji – komendant lub osoba przez niego upoważniona. Ponadto analizy kryminalne mogą być wykonywane również na zlecenie innych organów administracji państwowej uprawnionych do ścigania sprawców przestępstw (np. prokuratury). Wniosek o analizę powinien zawierać nazwę jednostki organizacyjnej zlecającej wykonanie analizy, numer sprawy, której zlecenie dotyczy, imię i nazwisko osoby prowadzącej sprawę oraz cel i zakres analizy. Zleceniodawca powinien wraz z wnioskiem dostarczyć wszystkie materiały niezbędne do wykonania analizy kryminalnej[1].

Sprawy, które warto poddawać analizie, to w szczególności sprawy wielowątkowe, o dużym stopniu skomplikowania, ciężarze gatunkowym oraz o dużym zasięgu terytorialnym, gdzie zazwyczaj występuje bardzo dużo różnych informacji. Analizę kryminalną stosuje się głównie przy wykrywaniu najpoważniejszych przestępstw kryminalnych oraz do zwalczania przestępczości zorganizowanej, zagrożeń terrorystycznych i ekstremistycznych.

Nie zawsze analizy kryminalne dotyczą całości materiałów prowadzonego postępowania. Analizie może zostać poddany fragment sprawy, na przykład połączenia telefoniczne, przelewy finansowe czy zawartość danego dysku twardego lub innego nośnika danych. Najlepiej jednak, gdy do zagadnienia podchodzi się kompleksowo i analizie poddawane są całe duże sprawy wraz z pełnym zgromadzonym materiałem dowodowym czy operacyjnym. Kiedy zestawi się ze sobą wiadomości na różnych płaszczyznach, na przykład czasu, miejsca i sposobu działania sprawcy, daje to zaskakujący efekt w postaci uporządkowania posiadanych informacji, wskazania konkretnego

kierunku lub kierunków prowadzenia dalszych czynności oraz niejednokrotnie doprowadzenia do zidentyfikowania sprawcy przestępstwa. I sprawy, które wcześniej wydawały się nie do wykrycia, kończyły się sukcesem.
Bardzo ważne jest, aby analizę kryminalną stosować na jak najwcześniejszym etapie sprawy, od pierwszych czynności. Niestety, praktyka bardzo często wygląda w ten sposób, że analiza kryminalna traktowana jest jako „ostatnia deska ratunku" w momencie, gdy – zdaniem prowadzących sprawę – wyczerpane zostały wszystkie środki dowodowe czy wykrywcze. Niejednokrotnie, rzeczywiście, analiza kryminalna pozwala w takich sytuacjach, poprzez wskazanie nowych środków dowodowych czy kierunków czynności wykrywczych, pchnąć sprawę na nowe tory. Często jednak okazuje się, że w tym momencie jest już za późno, by ustalenia poczynione w toku analizy mogły mieć istotny wpływ na prowadzone postępowanie (np. przeprowadzenie czynności, których potrzeba wynikła z analizy, ze względu na upływ czasu jest już niemożliwe lub bezcelowe).

Zdarza się, że w wyjątkowych sytuacjach tworzy się zespoły analityczne czy centra analityczne. Dzieje się tak w okolicznościach, kiedy m.in. ogromne znaczenie dla rozwiązania sprawy ma czas lub ogrom materiału przekracza zdolności analityczne jednego umysłu. Centra analityczne powstają w przypadku wydarzeń o charakterze międzynarodowym lub niezwykle ważnych z innego powodu. Ostatnie takie centrum działało w Biurze Wywiadu i Informacji Kryminalnych Komendy Głównej Policji w związku z ubiegłorocznym szczytem NATO w Warszawie. Jego zadaniem było zbieranie, przetwarzanie i analizowanie informacji dotyczących wszelkich zagrożeń bezpieczeństwa i porządku publicznego.

W jednej ze spraw, dotyczącej wielomilionowych wyłudzeń, analizie poddano wiele danych zabezpieczonych w formie elektronicznej na dyskach twardych, które wydawały się istotne z punktu widzenia prowadzonego postępowania przygotowawczego. Do analizy zostały przekazane obrazy dysków twardych – kopie binarne. We wstępnej fazie analizy zidentyfikowano łącznie kilkaset tysięcy plików do dalszej selekcji, pliki uszkodzone w sposób uniemożliwiający ich odczytanie oraz określoną liczbę plików zaszyfrowanych do dalszych badań. Inwentaryzacji poddano również pliki w formacie pdf oraz w formatach graficznych. W toku analizy kryminalnej wyodrębniono powiązania pomiędzy wskazanymi osobami i podmiotami występującymi w wymienionych plikach – co było celem analizy. Wyszukiwanie powiązań uwzględniało zarówno treść dokumentów, jak i inne elementy, nagłówki plików pocztowych, znaczniki plików, dane numeryczne itp. Wyniki analizy zapisano w katalogach, nazwanych jak obiekty, których dane dotyczyły, ze ścieżkami dostępu do plików źródłowych, o łącznej pojemności ponad 110 GB.
Powyższy przykład ukazuje, że współcześnie analiza kryminalna łączy w sobie funkcje informatyczno-analityczne do pozyskiwania dużej ilości danych (metadanych), ich segregacji, przetwarzania, analizowania i raportowania w różnych formach. W celu identyfikacji i korelacji informacji o kluczowych obiektach, takich jak: nazwy firm, sumy pieniędzy, adresy e-mail, adresy IP, numery telefonów, numery kart kredytowych i inne; analizie poddawane są dane o złożonych formatach plików pochodzących z różnych źródeł (systemów operacyjnych, baz danych, serwerów, systemów plików urządzeń mobilnych, usług e-mail w chmurze i innych), ale także wszystkie informacje obrazujące to, co się działo z plikiem, np. jak i kiedy był używany i do kogo został przesłany.
Naturalnie bez nowoczesnych narzędzi, a takimi są odpowiednie programy komputerowe, nie jest możliwe przeprowadzenie skomplikowanej analizy, jednak w całym jej procesie najważniejszy jest człowiek, analityczne myślenie, interdyscyplinarność i elastyczność. Analitycy kryminalni korzystają z zestawu różnego rodzaju specjalistycznego oprogramowania komputerowego, w zasadzie ze wszystkiego, co może być pomocne i jest dostępne na rynku.
Żyjemy w dobie nowych technologii, społeczeństwa informacyjnego i w konsekwencji – w dobie nowych wyzwań i zagrożeń. Analiza kryminalna wpisuje się w ten trend i jest odpowiedzią na zachodzące zmiany i niebezpieczeństwa. To jedno z najskuteczniejszych i najnowocześniejszych narzędzi, którymi dysponuje Policja. To dziedzina, która nieustannie się rozwija i właściwie z każdym rokiem powiększa możliwości. Generalną zasadą jest, że z różnych względów analityk kryminalny pozostaje w cieniu sukcesów rozwiązanych spraw, a było ich naprawdę wiele, o czym świadczy fakt, że analitycy kryminalni nie narzekają na brak zleceń.
Wydział Analizy Kryminalnej Biura Wywiadu i Informacji Kryminalnych Komendy Głównej Policji obecnie pod kierownictwem podinsp. Artura Jarosza opiera się na pracy zespołu analityków kryminalnych, w którego skład wchodzą jedni z najlepszych w kraju ekspertów w tej dziedzinie. Od wielu lat wykonują oni analizy kryminalne na potrzeby najcięższych gatunkowo, najbardziej złożonych i wielowątkowych spraw i mogą się pochwalić licznymi sukcesami polegającymi na dokonaniu istotnych ustaleń, przyczyniających się do rozwiązania wielu bardzo trudnych kwestii.

[1] Zarządzenie nr 1012 Komendanta Głównego Policji z dnia 23 września 2004 r. w sprawie stosowania przez Policję analizy kryminalnej (Dz. Urz. KGP Nr 20, poz. 124, z późn. zm.).

Summary

Crime analysis in the age of information society

Development of computer crimes and the transfer of traditional crimes (e.g. drug crimes) to cyberspace pose new challenges for bodies established to combat crimes. Crime analysis perceived as searching various connections among seemingly unrelated facts, the aim of which is to find a perpetrator or to indicate a new direction of actions, can be a very helpful tool. One should analyse in particular multithreaded, complicated, serious cases of significant territorial scale. Currently crime analysis is based on processing large amount of data (including metadata) in order to find connections between different objects and to draw conclusions and hypotheses.

Tłumaczenie: Joanna Łaszyn

LOKALIZOWANIE

punktów dostępowych oraz urządzeń w sieci bezprzewodowej Wi-Fi

podkom. Tomasz Boroń

Naczelnik Wydziału do Walki z Cyberprzestępczością
Komendy Wojewódzkiej Policji w Bydgoszczy

Niniejszy artykuł stanowi opis sieci bezprzewodowych. Autor przedstawia ich rozwój, typy oraz specyfikę działania. Ponadto omawia metody lokalizowania punktów dostępowych oraz urządzeń w sieci bezprzewodowej.

Zapewnienie bezpieczeństwa teleinformatycznego w obecnych czasach stawia przed Policją nowe wyzwania. Generalnie głównym zadaniem jest monitorowanie, przeciwdziałanie, ujawnianie i gromadzenie dowodów przestępstw dla organów procesowych, pomoc merytoryczna i techniczna podległym jednostkom. Cyberprzestępczość to nie tylko typowe przestępstwa komputerowe wskazane w kodeksie karnym, ale też inne przestępstwa, do których popełnienia zostały użyte urządzenia telekomunikacyjne oraz informatyczne.

Ogrom analizowanych danych, uzyskanych w trakcie ujawniania przestępstw komputerowych, wymusza na prowadzących sprawę poświęcenie większej ilości czasu potrzebnego do ustalenia sprawcy. Dodatkowym utrudnieniem jest brak ujednoliconego systemu, który by standaryzował otrzymane dane od operatorów.

Obecnie, żeby sprostać nowym wyzwaniom, trzeba nieustannie śledzić rozwój nowych technologii oraz nowe metody popełniania przestępstw.

Typowe obszary zagrożeń:

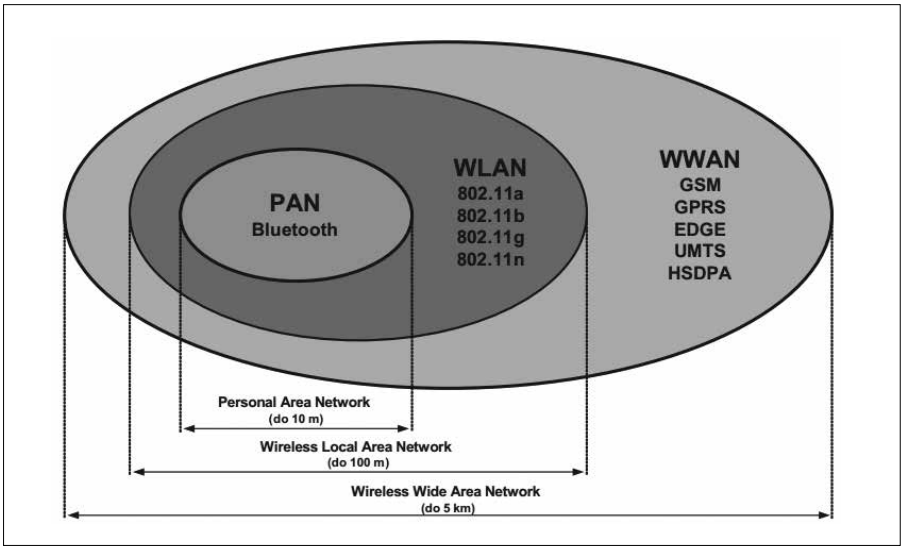
- pornografia dziecięca;
- propagowanie przemocy, nienawiści, zakazanych ideologii;
- przejmowanie tożsamości;
- przełamywanie zabezpieczeń kont pocztowych, kont bankowości elektronicznej, kont na portalach społecznościowych;
- szantaż;
- podrabianie dokumentów i pieniędzy;
- kradzież własności intelektualnych;
- e-handel zakazanymi produktami;
- oszustwa na portalach aukcyjnych;
- podsłuch elektroniczny;
- niszczenie, wykradanie danych;
- zakłócanie pracy serwerów/komputerów w sieci;
- wykorzystywanie komunikatorów do komunikowania się sprawców.

W dzisiejszych czasach urządzenia Wi-Fi opanowały większość gałęzi życia człowieka. W niektórych dziedzinach ich obecność jest niezbędna. Urządzenia te gromadzą i udostępniają duże ilości danych. Jednak, aby udostępniać nam swoje zasoby, muszą się między sobą porozumieć. Dlatego są one połączone w sieci komputerowe. Jedną z takich sieci jest bezprzewodowa sieć lokalna.

Rozwój sieci bezprzewodowych na świecie kształtował się w trzech etapach. Pierwszy etap to teoretyczna koncepcja badań i poszukiwań możliwych zastosowań. Drugi etap to projektowanie sprzętu i jego rozwój. Trzeci etap związany jest z promowaniem i upowszechnieniem komunikacji bezprzewodowej. Badania nad rozwojem sieci bezprzewodowych odbywały się w dwóch kierunkach, tj. w związku ze świadczeniem usług związanych z komunikacją głosową oraz wymianą danych.

Obecnie mamy dwa typy sieci bezprzewodowej, które ze względu na zasięg możemy podzielić na dwa rodzaje. Są to sieci lokalne o niewielkim zasięgu oraz sieci rozległe WAN, których zasięg wielokrotnie przekracza górną granicę możliwości sieci lokalnych.

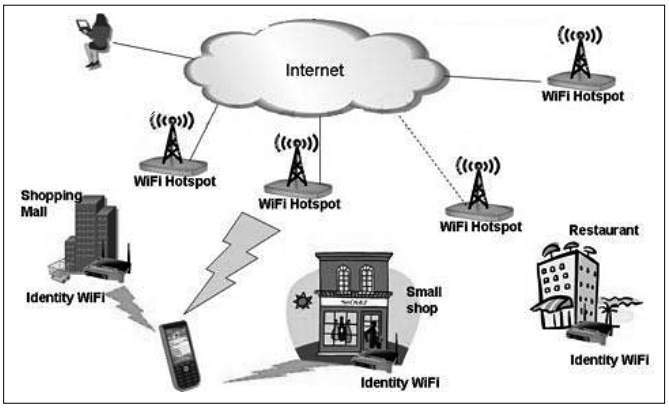
Teraz wystarczy połączenie z Internetem, aby móc dokonać zakupów w polskich i zagranicznych sklepach, wykonać szybkie i bezpośrednie płatności poprzez bankowe konta elektroniczne, wymieniać się danymi czy komunikować z ludźmi na całym świecie. Niskie ceny sprzętu komputerowego spowodowały, że komputer jest praktycznie w każdym gospodarstwie domowym, a łatwość jego konfiguracji sprawiła, że każdy po uruchomieniu systemu operacyjnego może połączyć się z globalną siecią.
Wprowadzanie nowych technologii dostępu do sieci oraz miniaturyzacja sprzętu komputerowego umożliwiają użytkownikom korzystanie z sieci bezprzewodowych, dzięki którym nie są ograniczeni długością „kabla" czy miejscem, w którym jest komputer.



Rys. 2. Typowy zasięg sieci bezprzewodowych.
Źródło: Sieci komputerowe, dr inż. Andrzej Opaliński, AGH Kraków, http://docplayer.pl/2951424-Sieci-komputerowe-sieci-bezprzewodowe-wydzial-inzynierii-metali-i-informatyki-przemyslowej-dr-inz-andrzej-opalinski-www-agh-edu.html.

Bezprzewodowe sieci lokalne

Historia sieci radiowych rozpoczęła się w okresie II wojny światowej. Pierwsze transmisje były przeprowadzane przez armię Stanów Zjednoczonych. Następnie na Uniwersytecie Hawajskim zbudowano pierwszą sieć bezprzewodową o nazwie „ALOHNET". Była to sieć o zasięgu lokalnym w topologii gwiazdy. Dziś większość dostępu do Internetu realizowana jest z udziałem komputerów przenośnych wyposażonych w kartę sieciową przeznaczoną do pracy w standardzie „802.11", który określa zasady pracy urządzeń. Technologia lokalnych sieci bezprzewodowych umożliwia transmisję danych w zależności od miejsca, od 30 do 300 m w terenie otwartym (rys. 1). Z wykorzystaniem anten kierunkowych odległość tę można zwiększyć do kilkunastu kilometrów. Aby osiągnąć tak duże odległości, muszą być zachowane pewne warunki, czyli pomiędzy antenami nie mogą występować żadne przeszkody w postaci np. murów, drzew. Jednakże wraz ze wzrostem odległości pogarsza się jakość sygnału, a szybkość transmisji danych maleje.



Rys. 1. Przykład zastosowania sieci bezprzewodowej.
Źródło: http://lejinternetplaza.com/what-is-wifi-and-how-to-use-it/.

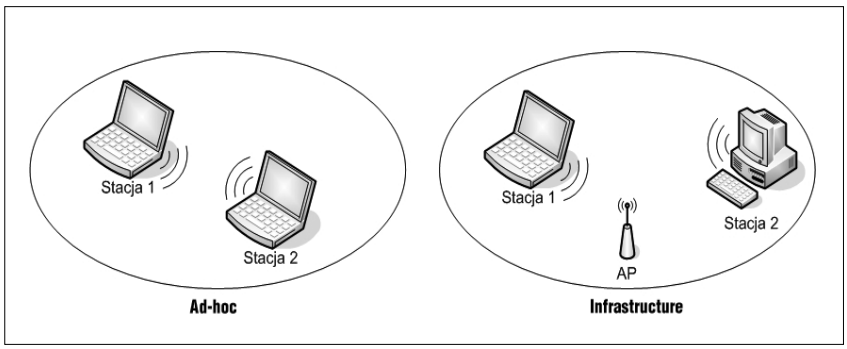
Standard 802.11

Obecnie istnieje wiele metod uzyskania połączenia bezprzewodowego – od łączy „IrDA" (podczerwień), poprzez „Bluetooth", sieci w standardzie „802.11", aż po bardzo drogie, wymagające profesjonalnego montażu, radiolinie. Jednakże ze względu na praktyczne zastosowanie, popularność i niedrogie urządzenia w tego typu połączeniach, standard „802.11" jest najczęściej wykorzystywany. Zasięg typowych sieci bezprzewodowych waha się w granicach: do 10 metrów – „Bluetooth", do 200 m – sieci w standardzie „802.11", aż po sieci „WWAN", które osiągają zasięg do 5 kilometrów (rys. 2).
Do chwili obecnej wykorzystywane były i są m.in. następujące wersje standardu „802.11" (tab. 1): „802.11", „802.11a", „802.11b", „802.11g", „802.11n".

Tabela 1. Porównanie standardów sieci bezprzewodowej 802.11.
Źródło: opracowanie własne.

	IEEE 802.11	IEEE 802.11a	IEEE 802.11b	IEEE 802.11g	IEEE 802.11n
Zasięg	60 m	75 m	100 m	100 m	200 m
Maksymalna szybkość transmisji	2 Mb/s	54 Mb/s	11 Mb/s	54 Mb/s	200/540 Mb/s
Wrażliwość na zakłócenia	średnia	średnia	mała	duża	mała
Długość fali / częstotliwość	2,4 GHz	5 GHz	2,4 GHz	2,4 GHz	2,4/5 GHz

Komunikacja w sieci bezprzewodowej WLAN odbywa się za pomocą modulowanej fali radiowej o częstotliwości 2,4 GHz (802.11b/g) oraz 5 GHz (802.11a, 802.11n).
Zastosowany rodzaj techniki umożliwiający podział zasobów komunikacyjnych pozwala na sprawną wymianę danych. Podstawowa technika zgodna ze standardem 802.11g wykorzystuje podział czasu (TDMA). Użytkownicy korzystają z jednej częstotliwości, ale każdy nasłuchuje w innym czasie. Innym rozwiązaniem jest współdzielenie częstotliwości, czyli komunikowanie się w tym samym czasie na różnych częstotliwościach. Następne rozwiązanie to używanie sieci w tym samym czasie i na tej samej częstotliwości z wykorzystaniem kodowania ortogonalnego[1] pozwalającego wyodręb-



Rys. 3. Dwa różne tryby pracy: Ad-Hoc i Infrastructure. Źródło: https://pl.wikipedia.org/wiki/Punkt_dostępu.

nić transmisję wygenerowaną przez konkretnego użytkownika (CDMA). W nowszych rozwiązaniach zastosowano technikę unikalnego podziału czasu i częstotliwości dla danego użytkownika (OFDMA).
Sygnał radiowy dociera do odbiornika wieloma ścieżkami. Związane jest to z odbijaniem się fal od przeszkód znajdujących się w zasięgu sieci radiowej, dlatego do odbiornika dociera wiele wersji tego samego sygnału w różnych odstępach czasu. Opóźnienie sygnału może spowodować zakłócenia, w wyniku czego sygnał stanie się niezrozumiały dla odbiornika.

Architektura i topologia sieci w standardzie 802.11

Architektura sieci w standardzie „802.11" umożliwia połączenie sieci bezprzewodowych w dwóch trybach pracy (rys. 3):
- „Ad-hoc" – sieć tymczasowa,
- „Infrastructure" – sieć stacjonarna.

Sieci tymczasowe „Ad-hoc" wykorzystują komunikację „P2P" do przesyłania danych. W tym trybie pracy nie jest wymagany „Access Point"w celu zapewnienia fizycznego połączenia z siecią przewodową. Takie sieci tworzone są m.in. na potrzeby konferencji, zjazdów, spotkań. Wadą takiego rozwiązania jest niewielki zasięg.
Sieci stacjonarne „Infrastructure" zawierają element stały, tzw. „Access Point", który pośredniczy w transmisji danych pomiędzy siecią bezprzewodową a siecią przewodową. Cały ruch odbywa się za pośrednictwem „Access Point". Punkty dostępowe „Access Point" połączone są przewodem z siecią przewodową.
Najczęściej sieć bezprzewodowa jest uzupełnieniem tradycyjnej sieci przewodowej.
Obecnie wśród sieci bezprzewodowych można wyróżnić dwa typy topologii:
- **topologia gwiazdy** – najbardziej popularna; w celu komunikacji wykorzystuje jeden punkt dostępu („Access Point"); pakiet danych wysłany z węzła sieciowego jest odbierany w stacji centralnej i kierowany przez nią do odpowiedniego węzła; sieci budowane w tej topologii mają duże możliwości i są wydajne;
- **topologia kraty** – w sieciach kratowych poszczególne węzły (punkty „Access Point") nie komunikują się z innymi węzłami za pośrednictwem centralnych punktów przełączania, ale wymieniają z nimi dane bezpośrednio lub przez inne węzły wchodzące w skład kraty.

Działanie protokołu 802.11

Komputer z włączoną kartą bezprzewodową może się znajdować w trzech stanach pracy:
- stan początkowy – sieć nie jest uwierzytelniona i skojarzana z punktem dostępowym,
- uwierzytelniony,
- uwierzytelniony i skojarzony – sieć jest uwierzytelniona i skojarzona z danym punktem dostępowym.

Aby komputer mógł się połączyć z daną siecią, musi dokonać najpierw skanowania. Najprostszą metodą wykrywania sieci jest skanowanie pasywne. Każdy punkt dostępowy wysyła co jakiś określony czas ramkę informacyjną. Ramka ta dostarcza informacje, dzięki którym nasłuchujący komputer może podjąć próbę podłączenia się do punktu dostępowego. W przypadku wielu punktów dostępowych komputer wybiera sobie punkt dostępowy o największej sile nadawania.
Dalej następuje proces przyłączania realizowany w całości przez komputer do punktu dostępowego wybranego w procesie skanowania.
Następnie realizowane jest uwierzytelnianie tylko przez komputer. Punkt dostępowy w tym momencie traktowany jest jako wiarygodny.
Po uwierzytelnieniu komputer kojarzony jest z punktem dostępowym. Proces ten polega na przydzieleniu numeru AID (Association ID), który służy do identyfikowania komputera w procesie buforowania ramek przez punkt dostępowy.

Warstwa fizyczna IEEE 802.11

Sieć IEEE 802.11 wykorzystuje obszar ISM w paśmie 2,4 GHz (od 2400 do 2485 MHz).

Tabela 2. Standardy sieci WLAN.
Źródło: opracowanie własne.

Standard	Pasmo	Zasięg w pomieszczeniu	Zasięg w przestrzeni otwartej
802.11a	5 GHz	30–35 m	75 m
802.11b	2,4 GHz	50 m	120 m
802.11g	2,4 GHz	35 m	~ 100 m
802.11n	2,4 / 5 GHz	70 m	~ 100 m

Tabela 3. Kanały i częstotliwości.
Źródło: https://pl.wikipedia.org/wiki/IEEE_802.11.

Kanał	Dolna częstotliwość [GHz]	Środkowa częstotliwość [GHz]	Górna częstotliwość [GHz]
1	2	3	4
1	2,401	2,412	2,423
2	2,406	2,417	2,428
3	2,411	2,422	2,433

1	2	3	4
4	2,416	2,427	2,438
5	2,421	2,432	2,443
6	2,426	2,437	2,448
7	2,431	2,442	2,453
8	2,436	2,447	2,458
9	2,441	2,452	2,463
10	2,446	2,457	2,468
11	2,451	2,462	2,473
12	2,456	2,467	2,478
13	2,461	2,472	2,483
14	2,473	2,484	2,495

Propagacja[2] fali radiowej w pomieszczeniu

Propagacja fali radiowej w budynku jest specyficzna, ponieważ napotyka na różne przeszkody, które tłumią sygnał. Do obliczenia tłumienia sygnału w pomieszczeniu wykorzystywany jest np. model „Multi-Wall".
Polega na badaniu poziomu sygnału po jego przejściu przez różnego rodzaju przeszkody. Model ten bazuje na obliczeniu różnicy mocy sygnału przebiegającego w linii prostej od nadajnika do odbiornika, natrafiającego na różnego typu przeszkody (sygnał jest osłabiany o daną wartość charakterystyczną dla tej przeszkody).

Tabela 4. Charakterystyka tłumienia wg modelu „Multi Wall". Źródło: Ł. Jasiński, *Pomiar tłumienia ścian i innych elementów charakterystycznych dla środowiska wewnątrzbudynkowego w paśmie 2,4 GHz,* Wrocław 2011.

Nazwa elementu	Materiał	Grubość [cm]	Tłumienie [dB]
Ściana wewnętrzna	Cegła	10	7
Ściana zewnętrzna	Cegła	3	9
Ściana działowa	Rigips i wełna szklana	7	2
Strop	Beton	30	11
Okno	Szkło	szyba x 2 + przerwa 1 cm	4,5
Drzwi	Drewno	4	2,5

Wady sieci radiowych

Korzystanie z sieci radiowych wiąże się z występowaniem następujących zakłóceń:
- ściany budynku obniżają szybkość przesyłu danych,
- urządzenia elektryczne zakłócają fale radiowe,
- rozproszenie energii,
- zakłócenia zewnętrzne,
- wzajemne zakłócanie się urządzeń bezprzewodowych.

Sprzęt do transmisji bezprzewodowej

Sieć bezprzewodowa do wysyłania i odbierania danych używa fal elektromagnetycznych (radiowych lub podczerwonych). Transmitowane dane nakładane są na nośnik radiowy (fale radiowe), które to później odbierane są przez punkt odbiorczy.
W dziedzinie sprzętu stosowanego do transmisji danych w sieciach bezprzewodowych panuje ogromna różnorodność. Istnieje wiele rozwiązań, różniących się przeznaczeniem, parametrami technicznymi i ceną.
Do budowy lokalnych sieci bezprzewodowych wykorzystywane są najczęściej następujące urządzenia:
- bezprzewodowe karty sieciowe,
- punkt dostępowy i router,
- anteny.

Bezprzewodowe karty sieciowe

Każdy komputer, aby mógł pracować w sieci, musi być wyposażony w bezprzewodową kartę sieciową. Jest ona podstawowym elementem każdej sieci. Karty te mają identyczne przeznaczenie jak karty sieci przewodowych. Wyróżniamy karty PCI, karty wbudowane w komputerze przenośnym, karty na USB i inne. Takie karty zawierają nadajnik radiowy.
Wybór bezprzewodowej karty sieciowej jest bardzo istotny, bowiem występują znaczne różnice pomiędzy dostępnymi kartami sieciowymi. W celu wyboru jak najlepszej karty sieciowej należy zwrócić uwagę na:
- rodzaj chipsetu znajdującego się na karcie,
- moc wyjściową i możliwości jej dowolnej zmiany,
- czułość odbiornika,
- obecność anten zewnętrznych,
- obsługa standardu „802.11".

Punkt dostępowy i router

Bezprzewodowy punkt dostępowy („Access Point") jest to urządzenie, które zapewnia komputerom dostęp do zasobów sieci. Punkty dostępowe mogą komunikować się ze sobą, co umożliwia budowę bardzo rozległych sieci bezprzewodowych.
Bezprzewodowy router pełni rolę węzła komunikacyjnego, służącego do rozdzielania sygnału i rozgałęzienia połączeń sieciowych.

Anteny wykorzystywane w sieciach bezprzewodowych

Urządzenia wykorzystujące łączność bezprzewodową nie mogą obejść się bez anten. Dzięki nim możemy zwiększyć zasięg poprzez skupienie sygnału radiowego oraz szerokość

wiązki promieniowania. Anteny charakteryzuje się za pomocą dwóch głównych parametrów: zysku i szerokości wiązki. Czasami pod uwagę bierze się strefę pokrycia i polaryzację. Anteny charakteryzują się następującymi parametrami:

- promieniowanie,
- kąt promieniowania,
- zysk,
- polaryzacja.

Ateny dzielimy na trzy podstawowe kategorie:

- antena dookólna,
- antena sektorowa,
- antena kierunkowa.

Antena dookólna

Może być instalowana na maszcie, na podstawie, na płaszczyźnie masy lub do sufitu. Emituje sygnał równomiernie we wszystkich kierunkach, w płaszczyźnie poziomej, okrywając kąt 360 stopni. Wykorzystywana jest w celu zwiększenia zasięgu sieci. Typowym zastosowaniem anten dookólnych jest połączenie punkt – wielopunkt z centralnym punktem dostępowym obsługującym wielu klientów, a czasami inne punkty dostępowe korzystające z anten kierunkowych.

Antena sektorowa

Emituje sygnał w sektorze określonym za pomocą kąta od 90 do 200 stopni. Anteny tego typu najczęściej wykorzystywane są w połączeniach poprzez ulicę albo w celu pokrycia długiego holu lub korytarza. Anteny sektorowe rozmieszczone dookoła, co pewien kąt, mogą zastąpić anteny dookólne.

Antena kierunkowa

Emituje najwęższy sygnał (sygnał jest skupiony) i dzięki temu antena tego typu ma największy zysk energetyczny. Stosowana jest w przypadku połączeń na duże odległości.

Metody lokalizacji

Urządzenia bezprzewodowe można lokalizować za pomocą metod tradycyjnych, takich jak pomiar kąta nadejścia sygnału (AoA), pomiar czasu, w jakim sygnał pokonuje drogę od nadajnika do odbiornika (ToA), a także za pomocą siły odbieranego sygnału (RSS).

Najbardziej rozpowszechnione metody lokalizowania to:

- trilateracja,
- triangulacja,
- Radio Frequency Fingerprinting.

Trilateracja

Metoda polegająca na obliczeniu odległości z co najmniej trzech punktów. Bieżące położenie urządzenia to miejsce, gdzie nakładają się trzy okręgi ze środkami w punktach orientacyjnych, a promienie okręgów wyznaczane są przez odległości od poszczególnych punktów orientacyjnych.

Triangulacja

Metoda polegająca na wyznaczaniu w terenie współrzędnych punktu. Punkt dostępu, który odbiera sygnał, wyznacza okręg. Bieżące położenie urządzenia to miejsce, gdzie nakładają się trzy okręgi ze środkami w punktach orientacyjnych, a promienie okręgów wyznaczane są przez odległości od poszczególnych punktów orientacyjnych.

Radio Frequency Fingerprinting

System do pomiaru częstotliwości radiowej jest skalibrowany poprzez pomiar siły odbieranego sygnału w określonych miejscach.

Dane te są wysyłane do bazy danych. W momencie próby znalezienia urządzenia bezprzewodowego, każdy punkt dostępu odpowiada. Następnie system śledzenia lokalizacji bierze informacje uzyskane z punktów dostępu i tworzy model środowiska radiowego.

Podsumowanie

W obecnych czasach nastąpił gwałtowny rozwój cyberprzestępczości. Sprawcy tego typu przestępstw mają coraz większą wiedzę z dziedziny informatyki, a co za tym idzie – potrafią również zacierać ślady swojej działalności przestępczej.

Dowodem działalności przestępczej może być ruch w sieci, zachowane dane w urządzeniach sieciowych, w urządzeniach pamięci masowej, urządzeniach przenośnych, zapisy w historii przeglądarek internetowych, wpisy w rejestrze po stronie klienta, jak i po stronie serwera.

Namierzanie użytkownika w otwartym terenie z rozproszoną zabudową nie sprawia większych problemów. Duży problem stanowi wskazanie dokładnego miejsca przy zabudowie zwartej.

Idea powstania urządzenia umożliwiającego lokalizowanie urządzeń pracujących w standardzie „802.11" pozwoli identyfikować użytkowników korzystających z sieci Wi-Fi, którzy za jej pomocą popełniają przestępstwa. Będzie również stanowić pomoc w ratownictwie, poszukiwaniu osób zaginionych oraz skradzionego sprzętu teleinformatycznego.

[1] Ortogonalność (z gr. *ortho* – prosto, prosty, *gonia* – kąt) – uogólnienie pojęcia prostopadłości znanego z geometrii euklidesowej na abstrakcyjne przestrzenie z określonym iloczynem skalarnym, jak np. przestrzenie unitarne (w tym przestrzenie Hilberta) czy przestrzenie ortogonalne. Pojęcie ortogonalności bywa uogólnianie również na przestrzenie unormowane, w których nie ma naturalnej struktury iloczynu skalarnego (ortogonalność w sensie Pitagorasa, ortogonalność w sensie Jamesa, ortogonalność w sensie Birkhoffa, T-ortogonalność). Źródło: https://pl.wikipedia.org/wiki/Ortogonalno%C5%9B%C4%87 [dostęp: 13.12.2017 r.].

[2] https://pl.wikipedia.org/wiki/Propagacja_fal_radiowych acji [dostęp: 13.12.2017 r.].

Summary

Locating access points and devices in the Wi-Fi wireless network

The present article constitutes the description of wireless networks. The author presents their development, types and specificity of action. Moreover he discusses methods of locating access points and devices in the wireless network.

Tłumaczenie: Joanna Łaszyn

USTALANIE POŁOŻENIA TELEFONU KOMÓRKOWEGO

z wykorzystaniem aplikacji Android

kom. Rafał Lewandowski

młodszy wykładowca
Zakład Służby Kryminalnej CSP

W dzisiejszych czasach telefon komórkowy służy nam już nie tylko do rozmowy i pisania wiadomości SMS. Rozwój technologii spowodował, że telefony komórkowe zastępują nam wiele urządzeń, m.in. aparat fotograficzny, nawigację, odtwarzacz muzyczny i wideo oraz komputer z dostępem do Internetu. Powstaje wiele aplikacji, które wykorzystujemy w codziennym życiu, np. podczas uprawiania sportu, zwiedzania czy podróżowania autem. Telefony komórkowe (smartfony) stały się oknem na świat, urządzeniami, za pomocą których możemy wykonać wiele czynności, nie wychodząc z domu.

Możliwości wykorzystania telefonów komórkowych w pracy policjantów są omawiane w Centrum Szkolenia Policji w Legionowie na „Kursie specjalistycznym w zakresie czynności zmierzających do zabezpieczenia majątkowego" oraz na „Kursie specjalistycznym w zakresie uzyskiwania informacji z Internetu dla policjantów zwalczających przestępczość komputerową". Przedmiotem niniejszego artykułu jest jedna z aplikacji telefonu komórkowego z systemem Android, która może być użyta w celu odnalezienia osoby, zlokalizowania zaginionego telefonu, usunięcia jego danych oraz zablokowania telefonu tak, aby prywatne dane właściciela nie dostały się w niepowołane ręce.

Smartfon to „przenośne urządzenie telefoniczne łączące w sobie funkcje telefonu komórkowego i komputera kieszonkowego. Pierwsze smartfony powstały pod koniec lat 90., a obecnie łączą funkcje telefonu komórkowego, poczty elektronicznej, przeglądarki sieciowej, pagera, GPS, jak również cyfrowego aparatu fotograficznego i kamery wideo"[1]. W nowszych modelach dostępne są też funkcje typowe dla komputera kieszonkowego, takie jak zarządzanie informacjami osobistymi. Większość nowych modeli potrafi odczytywać dokumenty biurowe w formatach ogólnodostępnych i stosowanych w komputerach przenośnych czy laptopach.

Android to „system operacyjny z jądrem Linux dla urządzeń mobilnych, takich jak telefony komórkowe, smartfony, tablety i netbooki. W 2013 r. był najpopularniejszym systemem mobilnym na świecie. Wspomniane jądro oraz niektóre inne komponenty, które zaadaptowano do Androida, opublikowane są na licencji GNU GPL"[2].

GNU General Public License to „licencja wolnego i otwartego oprogramowania stworzona w 1989 r. przez Richarda Stallmana i Ebena Moglena na potrzeby Projektu GNU, zatwierdzona przez Open Source Initiative"[3].

GPS to „globalny system wyznaczania pozycji (lokalizacji) obiektów wykorzystujący sztuczne satelity Ziemi, przeznaczony do ciągłego, szybkiego i dokładnego wyznaczania trzech współrzędnych, określających pozycję anteny odbiornika osobistego albo zainstalowanego na obiekcie stałym lub ruchomym, znajdującym się na lądzie, wodzie lub w powietrzu"[4].

Przedstawię jedną z możliwości smartfonów z systemem operacyjnym Android na przykładzie menadżera urządzeń Android, z wykorzystaniem telefonu HTC oraz konta znajdującego się w telefonie Samsung. W komputerze stacjonarnym, na laptopie, a także na telefonie – wykorzystując przeglądarkę internetową – możemy ustalić położenie innego telefonu komórkowego, i co za tym idzie, osoby, która z niego korzysta. Na przykład często udajemy się z dziećmi na różne festyny, koncerty i inne imprezy. Jeśli zdarzy się, że dziecko zniknie nam z pola widzenia, oddali się gdzieś, możemy – wykorzystując menadżera urządzeń Android – dość dokładnie ustalić jego położenie. Jesienią zwykle dzieje się tak, że wielu grzybiarzy, wciągniętych w poszukiwanie grzybów, traci orientację w terenie i gubi się w lesie. Tutaj również może nam pomóc wykorzystanie tej funkcji telefonu. Warunkiem jest podzielenie się z kimś bliskim adresem e-mail i hasłem założonym na telefonie.

Telefony komórkowe, wykorzystujące system operacyjny Android, wymagają założenia konta Google i zalogowania

się na nie, co umożliwia korzystanie ze sklepu z aplikacjami Google Play oraz z innych funkcji telefonu. Telefon komórkowy, który ma konto Google, można zlokalizować przez menadżera urządzeń Android dostępnego w Internecie pod adresem https://www.google.com/android/find?hl=pl. Usługa *Znajdź moje urządzenie* (menadżer urządzeń Android) jest domyślnie włączona na urządzeniach z Androidem, powiązanych z kontem Google.

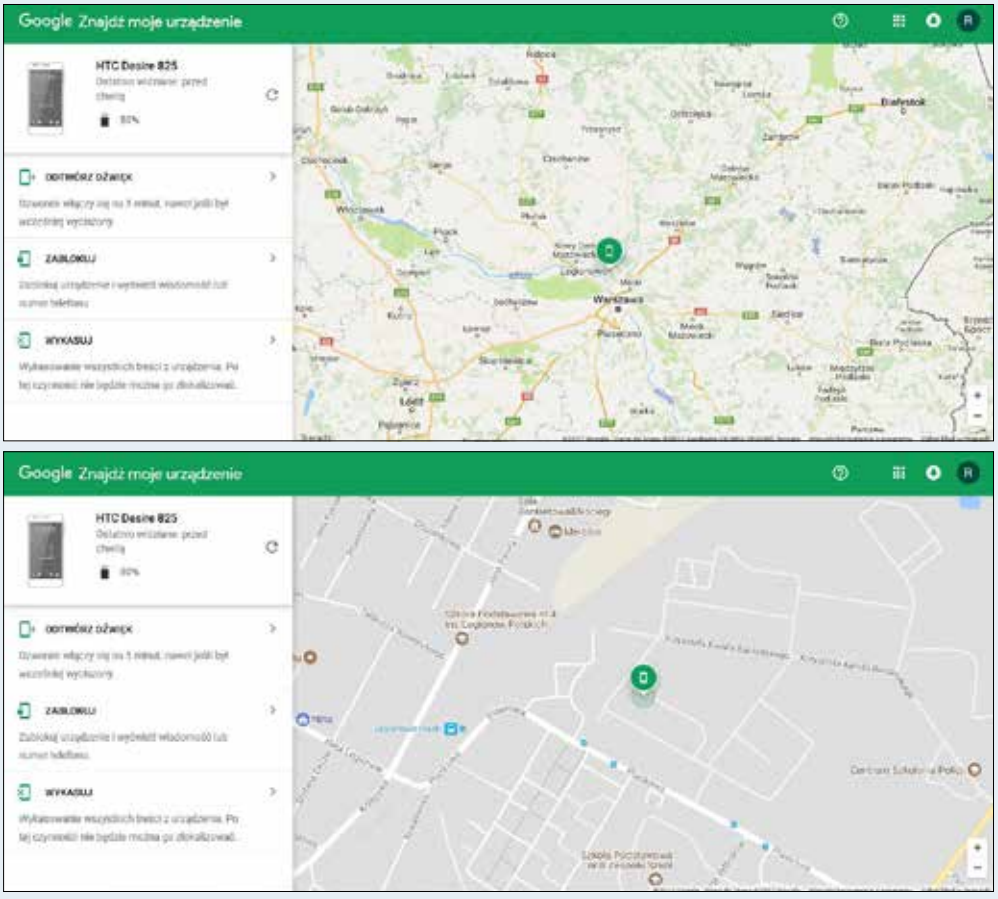
Niestety, aby wykorzystać możliwości systemu operacyjnego Android, musi być spełnionych kilka warunków. Urządzenie, którego położenie chcemy ustalić, musi być włączone i musi mieć użytkownika zalogowanego na konto Google. Ponadto musi mieć włączoną mobilną transmisję danych lub Wi-Fi oraz musi być widoczne w Google Play. W ustawieniach telefonu musi być włączona *Lokalizacja* oraz usługa *Znajdź moje urządzenie*. Na jakość ustalenia położenia i jego obszar wpływa kilka cech funkcjonalności telefonu. Jedną z nich jest włączony GPS w telefonie komórkowym, który umożliwia dokładniejsze ustalenie położenia telefonu. GPS w telefonie wykorzystuje również dodatek zwany geotagging. Jest to funkcja umożliwiająca połączenie danych współrzędnych geograficznych z wykonaną fotografią. Temat ten został omówiony w jednym z wcześniejszych numerów „Kwartalnika Policyjnego”[5]. Na prawidłowe działanie odbiornika GPS w telefonie wpływ ma każda przeszkoda znajdująca się pomiędzy odbiornikiem a satelitą. Mogą to być zarówno wysokie budynki, drzewa, jak i bardzo gęste chmury. Kolejną ważną cechą, umożliwiającą dokładne namierzenie telefonu komórkowego, jest uruchomienie sieci WiFi w telefonie, która pozwoli na dokładniejszą lokalizację.

Po wyświetleniu adresu https://www.google.com/android/find?hl=pl pojawia się następujący widok:

Rys. 1.

Należy się zalogować, wykorzystując adres e-mail i hasło założone na telefonie komórkowym, którego położenie chcemy ustalić. Po zalogowaniu się na konto uruchamia się strona z widokiem przedstawionym na rys. 2.

Na stronie zobaczymy nazwę telefonu, w tym przypadku HTC Desire 825, i mapę z lokalizacją telefonu. Strona umożliwia



Rys. 2.

Źródło: R. Lewandowski, 16.10.2017 r.

Rys. 3.

Rys. 4.

również zdalne odtworzenie dźwięku – dzwonek włączy się na 5 minut, nawet jeśli był wcześniej wyciszony lub włączone były tylko wibracje. Funkcję tę można wykorzystać chociażby do znalezienia telefonu w domu, jeśli ktoś jest osobą roztargnioną i nie wie, gdzie odłożył telefon. Opcja *Zablokuj – zablokuj urządzenie i wyświetl wiadomość lub numer telefonu* powoduje zablokowanie urządzenia za pomocą kodu PIN, wzoru lub hasła. Ekran blokowania został przedstawiony na rys. 3.

Możemy dodać wiadomość składającą się z treści i numeru telefonu, która wyświetli się na telefonie, aby znalazca telefonu mógł zadzwonić do osoby, która utraciła telefon.

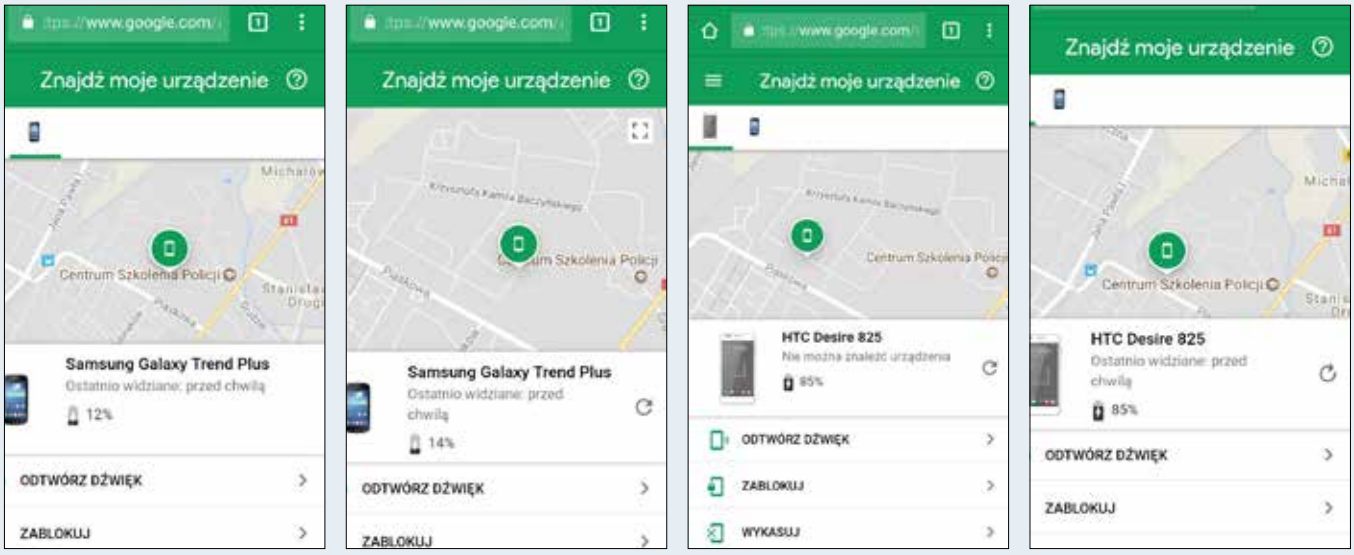
Kolejną funkcją na stronie jest opcja *Wykasuj*. Jej włączenie powoduje trwałe wykasowanie wszystkich danych z urządzenia. Po wykasowaniu danych usługa *Znajdź moje urządzenie* nie będzie działać na urządzeniu. Jeśli urządzenie jest offline, kasowanie rozpocznie się zaraz po połączeniu z Internetem. Aby znów móc używać urządzenia, należy zalogować się na swoje konto Google (rys. 4).

W sytuacji, gdy jesteśmy gdzieś poza mieszkaniem, nie mamy możliwości skorzystania z komputera stacjonarnego albo laptopa, możemy ustalić położenie innego telefonu, wykorzystując swój telefon z dostępem do Internetu. Procedura postępowania jest taka sama jak na komputerze, wykorzystujemy dowolną przeglądarkę internetową, wchodzimy na stronę wyżej wymienioną w przeglądarce na telefonie. Wyświetli nam się takie okno jak na komputerze stacjonarnym (rys. 5).

Niezależnie od marki telefonu, rodzaju Androida, możemy wyszukiwać położenie telefonu w menadżerze urządzeń Android. Podobną funkcję zastosował producent telefonów Samsung, który stworzył swoją własną aplikację w celu ustalenia położenia telefonu komórkowego. Działa ona niezależnie od funkcji menadżera urządzeń Android i można ją zastosować zamiennie lub wspólnie, porównując położenie telefonu. Na telefonie należy dodatkowo założyć konto Samsung, oddzielnie działające obok konta Google. Taki telefon będzie posiadał więc dwa konta umożliwiające odnalezienie telefonu. Następnie należy przejść na stronę internetową: https://findmymobile.samsung.com/ (rys. 6).

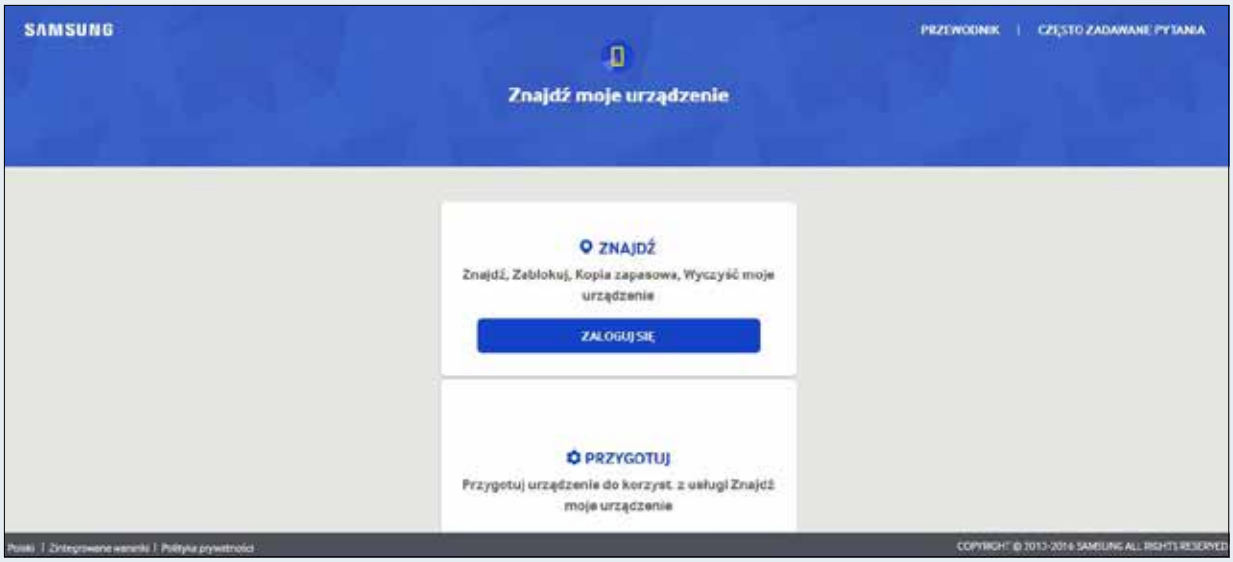
Należy się zalogować na stronie e-mailem i hasłem, które zostało założone na telefonie – może to być to samo konto, które zostało wykorzystane do założenia konta Google lub zupełnie nowe. Po zalogowaniu się urządzenie zostaje namierzone automatycznie. Dokładność ustalenia obszaru położenia telefonu jest mniejsza niż funkcjonalność menadżera urządzeń Android, ale pozwala na określenie obszaru, w którym znajduje się telefon (rys. 7).

Dodatkowo, oprócz lokalizacji telefonu, mamy do wyboru funkcje: *Zadzwoń na moje urządzenie, Zablokuj moje urządzenie, Wyczyść moje urządzenie przenośne, Pobierz dzienniki* i *Odblokuj moje urządzenie*. Powyższe funkcje mają takie samo działanie jak w opcji menadżera urządzeń Android – możemy zdalnie zablokować urządzenie hasłem lub pinem przed niepowołanymi osobami. Możemy również zdalnie usunąć dane z telefonu, aby osoba, która weszła w jego posiadanie, nie mogła przejrzeć jego zawartości. Ponadto po zablokowaniu telefonu i z chwilą jego odnalezienia możemy odblokować swoje urządzenie. Funkcja *Pobierz dzienniki* umożliwia pobranie do 50 ostatnich pozycji z dziennika, tzn. z książki połączeń rozmów przychodzących i wychodzących, jak również i SMS-ów. Lista odpowiedzi dziennika pokaże nam: dzień, miesiąc i rok oraz dokładną godzinę połączenia i – jeśli numer jest zapisany w książce kontaktowej – wskaże, pod jakimi danymi wprowadziliśmy numer oraz czas połączenia (rys. 8).

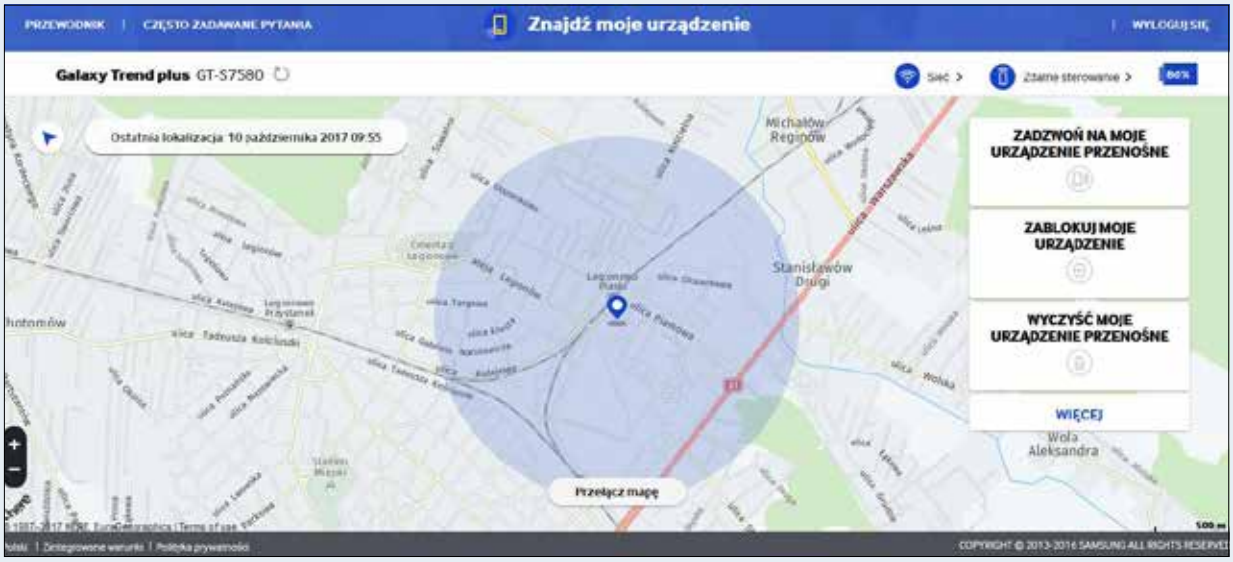


Rys. 5.

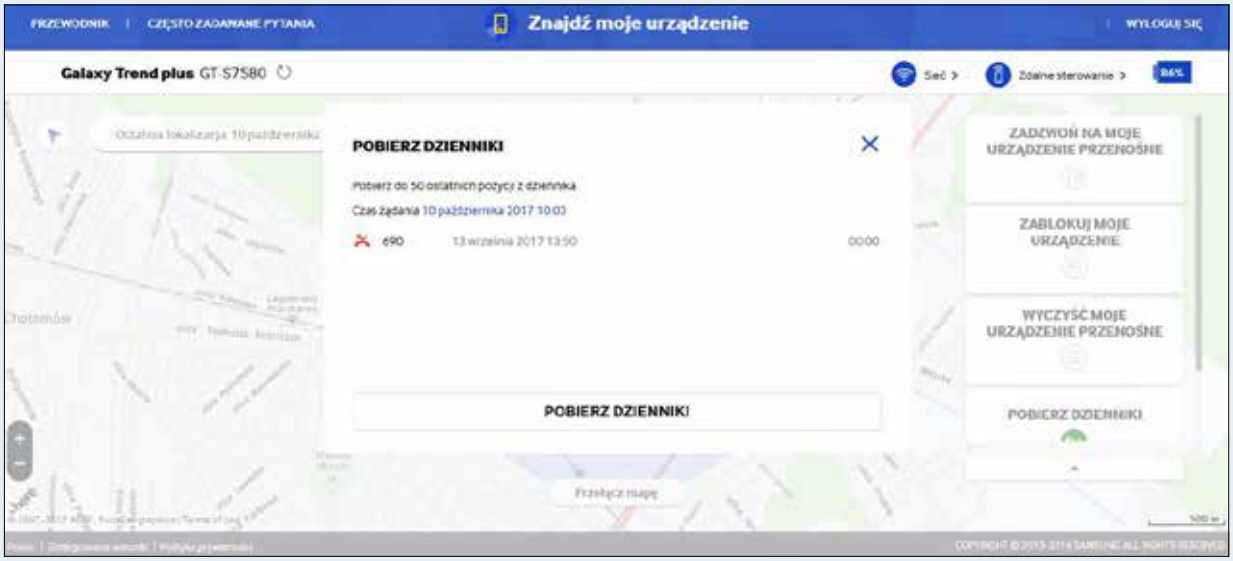
Źródło: R. Lewandowski, 16.10.2017 r.



Rys. 6.



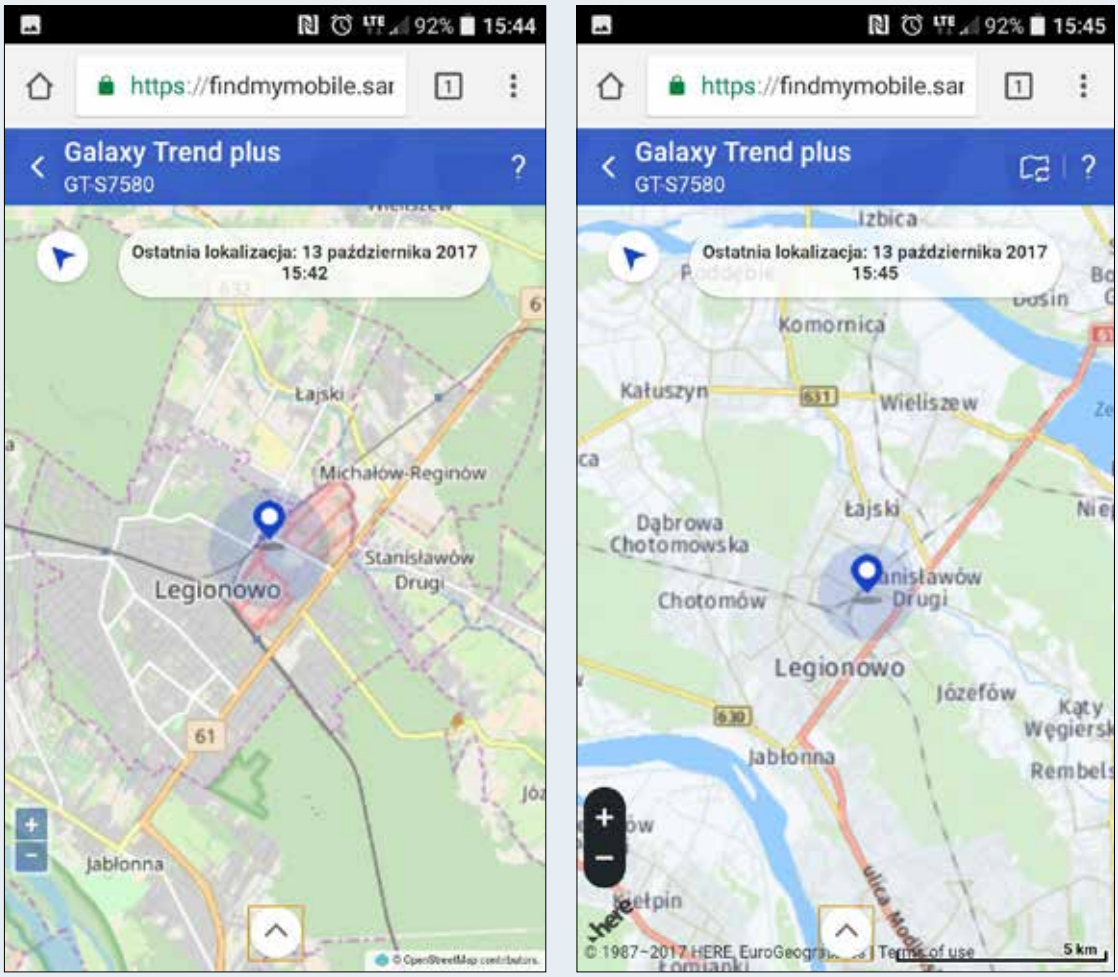
Rys. 7.



Rys. 8.

Źródło: R. Lewandowski, 16.10.2017 r.

Rys. 7.



Źródło: R. Lewandowski, 16.10.2017 r.

Analogicznie, wykorzystując własny telefon komórkowy z dostępem do Internetu, możemy zalogować się na konto Samsung (rys. 9).

Podsumowując, powyżej zostały przedstawione dwie możliwości ustalenia położenia naszego telefonu, które mogą być wielokrotnie używane w pracy policjantów i innych służb, a także w codziennym życiu. Może się zdarzyć, że zgubimy telefon albo zostawimy go u znajomych lub w innym miejscu. W takiej sytuacji nie należy wpadać w panikę, wystarczy wykorzystać możliwości naszego telefonu, aby ustalić jego położenie. Również w przypadku zgłoszeń kradzieży telefonu komórkowego warto wykorzystać funkcje, które zostały opisane powyżej. Możliwości ich wykorzystania jest wiele, powstały one, aby chronić nas, nasze dobra materialne, a także naszych bliskich. Wielokrotnie słyszymy o zaginięciach osób czy dzieci. Umiejętność wykorzystania opisanych wyżej funkcji telefonu może przyczynić się do odnalezienia nie tylko telefonu, ale również bliskich nam osób. Warto znać funkcje, które posiadają nasze telefony – nigdy nie wiemy, kiedy będziemy zmuszeni z nich skorzystać.

[1] *Smartfon,* w: *Wikipedia,* https://pl.wikipedia.org/wiki/Smartfon [dostęp: 16.11.2017 r.].
[2] *Android,* w: *Wikipedia,* https://pl.wikipedia.org/wiki/Android_(system_operacyjny) [dostęp: 16.11.2017 r.].
[3] *GNU,* w: *Wikipedia,* https://pl.wikipedia.org/wiki/GNU_General_Public_License [dostęp: 16.11.2017 r.].
[4] *GPS,* w: *Encyklopedia PWN,* https://encyklopedia.pwn.pl/haslo/GPS;3907249.html [dostęp: 16.11.2017 r.].
[5] R. Lewandowski, T. Siemianowski, *Geolokalizacja zdjęć*, „Kwartalnik Policyjny" 2015, nr 3, s. 111–118.

Bibliografia

Lewandowski R., Siemianowski T., *Geolokalizacja zdjęć*, „Kwartalnik Policyjny" 2015, nr 3.
www.wikipedia.org
www.support.google.com
www.encyklopedia.pwn.pl

Summary

Specifying the location of the mobile phone with the use of the Android application

In preset times we use the mobile phone not only to have phone calls or write text messages. The development of technology caused, that mobile phones replace a lot of devices, among others a camera, navigation, a musical player and a video as well as a computer with the access to the Internet. A lot of applications are created, which we use in our everyday life, e.g. while practicing sport, doing sightseeing or travelling by car. Mobile phones (smart phones) have become a window onto the world, devices with the aid of which we can carry out a lot activities, without leaving home.

Tłumaczenie: Renata Cedro

Procesowy aspekt zwalczania CYBERPRZESTĘPCZOŚCI

insp. w st. spocz. Roman Wojtuszek

Główny specjalista Wydziału Dochodzeniowo-Śledczego
Biura Kryminalnego KGP

W artykule poruszono zagadnienie procesowego ujawniania i utrwalania dowodów elektronicznych, tj. czynności procesowych mających postać zatrzymania danych informatycznych oraz przeszukania urządzenia zawierającego takie dane lub systemu informatycznego. Autor przedstawia istotę tych czynności. Zaprezentowane zostały regulacje przyjęte w Polsce w kontekście uregulowań międzynarodowych. Ponadto omówiono uzyskiwanie przez Policję danych telekomunikacyjnych i internetowych w postępowaniu przygotowawczym, w tym w trybie art. 20c ustawy o Policji.

Uwagi wstępne

W 2015 r. w Polsce komputery były wykorzystywane w 94,0% ogółu przedsiębiorstw, a 92,7% podmiotów gospodarczych i 75,8% gospodarstw domowych (77,7% miejskich i 72,0% wiejskich) posiadało dostęp do Internetu. Własną stronę internetową posiadało 65,4% ogółu przedsiębiorców, a 22,2% korzystało z mediów społecznościowych. Internet w kontaktach z administracją publiczną wykorzystywało 93,6% ogółu przedsiębiorstw. Z Internetu korzystało 68,0% osób w wieku 18–74 lata (72,9% w miastach i 60,0% na wsi)[1]. Liczba abonentów telefonii ruchomej w 2016 r. wynosiła ponad 55 milionów (55 879 000)[2]. Powyższe dane wskazują, że obecnie praktycznie wszystkie przejawy życia społecznego i gospodarczego są powiązane z wykorzystaniem komputerów, dokumentów elektronicznych oraz systemów informatycznych. Oznacza to nasilenie istniejących oraz pojawianie się nowych zagrożeń – przestępstw umiejscowionych w przestrzeni wirtualnej, popełnianych z wykorzystaniem systemów informatycznych, w tym sieci o globalnym zasięgu lub narzędzi informatycznych.

Postęp techniczny, w szczególności w obszarze technologii informatycznych, doprowadził do modyfikacji istniejących oraz powstawania nowych zagrożeń o charakterze przestępczym – określanych jako cyberprzestępczość. Cyberprzestępstwa polegają na posługiwaniu się systemami lub sieciami informatycznymi w celu naruszania jakiegokolwiek dobra prawnego chronionego przez prawo karne. Obejmują również zamachy skierowane na systemy komputerowe i sieci teleinformatyczne, dane i programy komputerowe, a więc grupę czynów określanych powszechnie jako przestępstwa *stricte* komputerowe lub przestępstwa przeciwko bezpieczeństwu przetwarzanej informacji. Warto jednak zauważyć, że pojęcia „cyberprzestępstwa" nie należy utożsamiać i stosować zamiennie z określeniem „przestępstwo internetowe", obejmującym jedynie grupę czynów, które mogą być popełnione tylko w Internecie lub z jego pomocą[3]. Cyberprzestępstwa stanowią więc czyny wymierzone w dane i systemy informatyczne (gdzie przetwarzanie danych jest przedmiotem czynności wykonawczych) oraz przestępstwa, w których technologie informatyczne są wykorzystywane przy popełnianiu już stypizowanych w prawie karnym czynów zabronionych (np. oszustwo komputerowe i piractwo komputerowe). Cyberprzestępczość obejmuje:

1) przestępstwa przeciwko bezpieczeństwu przetwarzanej informacji (np. art. 267 § 1 i § 2, 267 § 3, 267 § 4, 268, 268a, 269 § 1 i § 2 i 269b k.k.),
2) przestępstwa związane z użyciem środków masowego przekazu do rozpowszechniania lub prezentowania informacji zakazanych przez prawo, czyli tzw. przestępstwa związane z treścią informacji (np. art. 202 § 4, 202 § 4a, 212, 216, 255, 255a, 256 k.k.),

3) pozostałe przestępstwa instrumentalnego wykorzystania (użycia) elektronicznych sieci informatycznych i systemów informatycznych do naruszania dóbr prawnych, chronionych przez prawo karne (np. art. 165 § 1 pkt 4, 270 § 1 i inne przestępstwa przeciwko wiarygodności dokumentów określone w rozdz. XXXIV k.k., 286, 287, k.k.).

Omawiając grupę czynów zabronionych związanych z treścią informacji, należy zauważyć, że ich wspólną cechą jest odwołanie się do określonego sposobu działania sprawcy, polegającego na szeroko rozumianym rozpowszechnianiu lub prezentowaniu w sieciach informatycznych treści zakazanych przez prawo. Podstawą ich wyodrębnienia nie jest przedmiot zamachu, lecz ustawowo określony sposób działania sprawcy. W skład tak rozumianych przestępstw, związanych z treścią informacji, wchodzą m.in. przestępstwa związane z różnego rodzaju intelektualnym oddziaływaniem na psychikę oraz emocje innych osób w celu np. wywołania podniecenia seksualnego, wrogości wobec określonej grupy osób, poniżenia lub też mające na celu przekonanie ich do określonych poglądów lub postaw.

Zatrzymanie danych informatycznych oraz przeszukanie urządzenia zawierającego takie dane lub systemu informatycznego

Regulacja prawna odnosząca się do procesowego uzyskiwania dowodów ze systemów informatycznych i urządzeń zawierających dane informatyczne znajduje się w Konwencji Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r.[4] Nałożyła ona na jej strony obowiązek przyjęcia odpowiednich rozwiązań proceduralnych, niezbędnych dla celów prowadzonych postępowań karnych w sprawach o przestępstwa w niej określone. Polska, realizując jej postanowienia, dostosowała obowiązujące przepisy do prawa międzynarodowego.

Zatrzymanie danych informatycznych oraz przeszukanie urządzenia zawierającego takie dane lub systemu informatycznego, jako czynności procesowe, do polskiej procedury karnej wprowadzono w 2003 r. Stało się tak poprzez dodanie do ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2017 r. poz. 1904, z późn. zm.), zwanej dalej „k.p.k.", art. 236a stanowiącego o odpowiednim stosowaniu przepisów traktujących o zatrzymaniu rzeczy i przeszukaniu danych znajdujących się w systemie informatycznym lub na nośniku, w tym korespondencji przesyłanej pocztą elektroniczną[5].

W 2004 r. przepis zmodyfikowano – zadecydowano o odpowiednim stosowaniu przepisów rozdziału 25 k.p.k. także w odniesieniu do urządzenia zawierającego dane informatyczne w zakresie danych przechowywanych w tym urządzeniu[6]. Powody zmian wyjaśnia uzasadnienie projektu ustawy, cyt.: „Konwencja o cyberprzestępczości nakłada na strony obowiązek zapewnienia możliwości prowadzenia działań m.in. procesowych w odniesieniu do systemów komputerowych i przechowywanych w nich informacji. Konwencja opiera się w tej mierze na słusznym założeniu, że «tradycyjne» sposoby pozyskiwania dowodów nie przystają do urządzeń komputerowych i do danych zapisanych przy ich użyciu. Stosowanie dotychczasowych przepisów o przeszukaniu czy zatrzymaniu rzeczy nie jest wystarczające do pozyskiwania na użytek procesu karnego i wykorzystywania jako dowodów informacji przechowywanych w systemach komputerowych lub na nośnikach informacji zapisywanych przy użyciu tych systemów. Istniejące w prawie polskim rozwiązania, podobnie jak w wielu innych systemach prawnych, koncentrują się na systemie komputerowym i zapisanym w nim nośniku jako rzeczach ruchomych, podczas gdy dla postępowania karnego najistotniejsze są zapisane w nich informacje. Informacje istotne dla postępowania mogą również znajdować się w ruchu, to jest być przesyłane między dwoma systemami komputerowymi przy użyciu sieci telekomunikacyjnych. Usługi takie często są świadczone przez inne podmioty niż operatorzy publicznych sieci. Wprowadzenie stosownych rozwiązań procesowych jest również warunkiem niezbędnym do prowadzenia współpracy międzynarodowej, która choć systemowo lokuje się w ramach wzajemnej pomocy prawnej w sprawach karnych, to wymaga wewnętrznych regulacji procesowych"[7].

W rezultacie nowelizacji art. 236a k.p.k. otrzymał, obowiązujące do dziś w niezmienionym kształcie, brzmienie[8]. Użyte w nim pojęcia „**dane informatyczne**" i „**system informatyczny**" nie są zdefiniowane w polskim prawie karnym. Dlatego należy posłużyć się ich definicjami zawartymi w Konwencji Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r. (Dz. U. z 2015 r. poz. 728), według której:

- „**system informatyczny**" oznacza każde urządzenie lub grupę wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych (art. 1 lit. a.),
- „**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 (art. 1 lit. b.).

Natomiast pod pojęciem „**urządzenie**" należy rozumieć przedmiot umożliwiający wykonanie określonego procesu, często stanowiący zespół połączonych ze sobą części tworzących funkcjonalną całość, służący do określonych celów, mający określoną formę budowy w zależności od spełniających parametrów pracy i celu przeznaczenia. W tak rozumianym pojęciu narzędzia mieści się również telefon komórkowy.

Kluczowe w tym przepisie pojęcia to „**dysponent**" oraz „**użytkownik**". Nie budzi wątpliwości, że „**dysponent**" to osoba upoważniona do rozporządzania urządzeniem lub systemem, mająca go do dyspozycji, rozporządzająca nim według swego uznania, np. właściciel urządzenia, administrator systemu. Natomiast „**użytkownik**" to osoba używająca urządzenia lub systemu, korzystająca z niego, eksploatująca go, czerpiąca jakieś korzyści z cudzego urządzenia lub systemu, np. posiadacz konta poczty elektronicznej[9]. Należy pamiętać, że „Zakres przedmiotowy odpowiedniego stosowania przepisów rozdziału 25 k.p.k. ograniczony został do danych przechowywanych w systemie lub na nośniku i znajdujących się w dyspozycji lub użytkowaniu wskazanych wyżej osób. Oznacza to, że w razie żądania wydania danych, powinny one być w zasięgu określonej osoby, natomiast nie muszą znajdować się w miejscu jej przebywania (np. domu, miejscu pracy), byleby tylko osoba ta w sposób legalny mogła spowodować ich przesłanie, skopiowanie, edycję itp. Dane te nie muszą także znajdować się na terytorium Polski, mogą to być np. dane przechowywane w skrzynce pocztowej znajdującej się na serwerze zagranicznym"[10]. Mogą to być więc także dane przechowywane w chmurze obliczeniowej[11].

Przepis art. 236a k.p.k. zawiera ponadto sformułowanie „**korespondencja przesyłana drogą elektroniczną**". Podzielam pogląd, że należy je interpretować jako „odnoszące się do korespondencji elektronicznej, która może być w ogóle przesyłana, lecz nie znajduje się w tym stadium w danej chwili (np. została zapisana przed wysłaniem lub już przesłana)". Z punktu widzenia art. 236a k.p.k. możliwość uzyskania wglądu do zasobów poczty email będzie dotyczyła wszystkich informacji, jakie zostały nadesłane, wysłane lub które są przechowywane w zasobach należących do użytkownika bądź dysponenta systemu informatycznego albo urządzenia zawierającego dane informatyczne, np. telefonu komórkowego.

Wybrane aspekty przeszukania urządzenia (systemu)

Przeszukanie to określona przez k.p.k. czynność procesowa, której celem jest wykrycie (znalezienie) osób lub rzeczy, jak również uzyskanie określonych danych. Tej czynności można poddać pomieszczenie, rzecz, osobę, miejsce oraz **urządzenie zawierające dane informatyczne**, **a także system informatyczny**.

Odpowiednie stosowanie przepisów rozdziału 25 k.p.k. oznacza, że część przepisów dotyczących zatrzymania rzeczy lub przeszukania stosuje się wprost, część z niezbędnymi modyfikacjami, a pozostałych nie stosuje się w ogóle[12]. Przeszukania urządzenia lub systemu informatycznego może dokonać prokurator albo na polecenie sądu lub prokuratora – Policja, a także inny organ. Celem takiego przeszukania jest znalezienie określonych danych informatycznych, przy czym muszą to być dane tego rodzaju, że mogą stanowić dowód w sprawie lub podlegać zajęciu w postępowaniu karnym. Inaczej mówiąc, ma ono **celu znalezienie określonych danych informatycznych w urządzeniu, z którego wykorzystaniem dopuszczono się przestępstwa, a także wszelkich informacji mogących uwiarygodnić zaistnienie okoliczności mających wpływ na przebieg postępowania karnego**. Przeważnie w sprawach o przestępstwa popełniane z użyciem komputera takim obiektem zainteresowania będzie sam komputer, choć niejednokrotnie okoliczności, jakie towarzyszą popełnieniu czynów, do których udowodnienia się zmierza, mogą determinować zainteresowanie elementami wyposażenia komputera, drukarką, skanerem, nagrywarką płyt CD lub innymi urządzeniami, a także telefonem komórkowym.

Przeszukanie w środowisku komputerowym może przybierać dwie zasadnicze postaci: przeszukanie systemu informatycznego lub nośnika oraz przeszukanie danych. Typowymi czynnościami przeszukania danych są zarówno szukanie danych z użyciem hasła lub słów kluczowych, jak i ich czytanie, sprawdzanie, przeglądanie.

Przeszukanie urządzenia lub systemu może być dokonywane w tzw. wypadkach niecierpiących zwłoki. Należy się zgodzić z tezą, iż „W przypadku przeszukania środowisk komputerowych owe przypadki niecierpiące zwłoki będą miały miejsce w szczególności wtedy, kiedy istotne z punktu dowodowego dane będą w pamięci operacyjnej komputera (telefonu komórkowego – R.W.), a zajdzie obawa, że po wyłączeniu systemu ich odzyskanie stanie się niemożliwe lub znacznie utrudnione, bądź też zaistnieje przypuszczenie, że osoba podejrzana wie już o prowadzonych przez organ ścigania czynnościach i może podjąć próbę usunięcia danych albo fizycznego zniszczenia nośników"[13]. Po przeprowadzeniu przeszukania w wypadkach niecierpiących zwłoki organ go dokonujący (policjant) ma obowiązek niezwłocznego zwrócenia się do prokuratora lub sądu o zatwierdzenie przeszukania. Postanowienie to doręcza się osobie, u której dokonano przeszukania, w terminie 7 dni od daty przeprowadzenia czynności, ale tylko na jej żądanie zgłoszone do protokołu.

Mając na uwadze odpowiednie stosowanie przepisów, należy podkreślić, że przed rozpoczęciem przeszukania, osoba, u której ma ono nastąpić, powinna zostać poinformowana o jego celu i wezwana do dobrowolnego wydania danych. Chodzi tu głównie np. o dobrowolne wskazanie, gdzie w systemie informatycznym lub urządzeniu znajdują się dane, które są poszukiwane. W przypadku wydania żądanych danych, uwzględniając treść art. 227 k.p.k., według którego przeszukanie powinno być dokonywane zgodnie z celem tej czynności, skoro jego cel został osiągnięty, przeszukanie nie powinno być kontynuowane. Przepis k.p.k. stanowi, iż podczas przeszukania ma prawo być obecna osoba, u której ma ono nastąpić, a także osoba wskazana przez ten podmiot, jeżeli nie umożliwia to przeszukania lub nie utrudnia go w istotny sposób. Prowadzący czynność (prokurator, funkcjonariusz Policji, ewentualnie innego organu) może również przybrać dowolną osobę do uczestniczenia w czynności. Należy pamiętać, że wskazanie lub przybranie osób to tylko uprawnienie, a nie obowiązek, a więc, zgodnie z k.p.k., przeszukanie urządzenia lub systemu informatycznego może się odbyć także w obecności „jedynie" przeszukującego oraz osoby, u której dokonuje się tej czynności (ewentualnie dorosłego domownika lub sąsiada – art. 224 § 3 k.p.k.). Trzeba podkreślić, że podczas przeszukania jest niedopuszczalne umożliwienie dysponentowi lub użytkownikowi bezpośredniego dostępu do urządzeń lub systemów.

Z czynności przeszukania urządzenia lub systemu informatycznego sporządza się protokół[14]. W kontekście powyższych uwag pojawiają się pytania:

1) czy zawsze trzeba zabezpieczać przedmioty, tj. urządzenia, np. komputery i nośniki danych informatycznych, czy też może wystarczające będzie zabezpieczenie samych danych?
2) kiedy zasadne jest zabezpieczanie danych wraz z nośnikiem, a kiedy wystarczy samo skopiowanie tych danych?

Jak się wydaje, interesujących dla praktyki policyjnej odpowiedzi na te pytania udzielili dr Marek Chrabkowski i mgr inż. Krzysztof Gwizdała[15] w artykule pt. *Zabezpieczenie dowodów elektronicznych* opublikowanym w 2015 r. w grudniowym numerze „Prokuratury i Prawa"[16]. Należy akceptować stanowisko autorów, zgodnie z którym **zabezpieczanie danych informatycznych wraz z nośnikiem jest zasadne w sytuacji, gdy**:

- nośnik ten będzie zaliczony w poczet materiału dowodowego;
- sytuacja na miejscu przeszukania nie pozwala na poprawne, tj. zgodne z wypracowanymi zasadami kryminalistyki, skopiowanie danych;
- sposób zabezpieczenia danych przez ich dysponenta uniemożliwia ich skopiowanie;
- na nośniku zawarto dane objęte tajemnicą prawnie chronioną, a organ uprawniony do ujawnienia tajemnicy nie jest organem dokonującym przeszukania;
- czas trwania zabezpieczenia danych przekraczałby rozsądne granice.

Inaczej mówiąc, jednym z czynników mających wpływ na sposób zabezpieczania danych informatycznych są parametry techniczne nośników danych zastanych na miejscu prowadzenia czynności procesowych. Wzrost pojemności nośników postępuje zdecydowanie szybciej niż możliwych do osiągnięcia prędkości ich kopiowania za pomocą odpowiednich narzędzi. W konsekwencji może to powodować sytuacje, w których wykonanie procesowych kopii kilku nośników o dużej pojemności może trwać wiele godzin, a w przypadku ich uszkodzeń – nawet kilka dni. Za słuszny należy uznać pogląd, że czas trwania czynności nie uzasadnia odstępowania od prawidłowej metodyki zabezpieczania dowodów elektronicznych, ale może stanowić podstawę odstąpienia od kopiowania danych i zabezpieczenia ich po prostu wraz z nośnikiem.

Innym czynnikiem, właściwie wykluczającym możliwość wykonania kopii danych i pozostawienia sprzętu w dyspozycji osób zainteresowanych, jest sposób zabezpieczenia dostępu do danych zawartych na nośnikach[17]. W przypadku, gdy odszyfrowanie danych zawartych na dysku jest możliwe tylko za pomocą modułu, który je zaszyfrował, i jest on umieszczony na płycie głównej komputera (a więc poza nośnikiem danych), zachodzi konieczność zabezpieczenia całego komputera.

Natomiast w pozostałych przypadkach organy procesowe mogą poprzestać na skopiowaniu danych informatycznych. Należy się zgodzić z poglądem Rzecznika Praw Obywatelskich, iż „zatrzymywanie całego urządzenia zawierającego dane informatyczne do celów postępowania karnego w większości przypadków jest zbędne, gdyż sam nośnik nie jest przydatny ani do ustalenia istoty przestępstwa, ani do wykrycia jego sprawcy, ani też do udowodnienia mu przestępstwa. Wartość dowodową ma bowiem zapis w komputerze, a nie sam sprzęt. Ponadto, skoro organom procesowym wolno zatrzymać dane, które są związane z nośnikiem, to tym bardziej wolno je skopiować, co stanowi zdecydowanie mniejszą dolegliwość dla osoby dotkniętej przeszukaniem”[18].

Udostępnianie Policji danych telekomunikacyjnych i internetowych

Na podstawie art. 20c ust. 1 ustawy o Policji[19] Policja ma prawo do uzyskiwania danych niestanowiących treści – odpowiednio – przekazu telekomunikacyjnego albo przekazu w ramach usługi świadczonej drogą elektroniczną, a także do przetwarzania tych danych bez wiedzy i zgody osoby, której dotyczą. Prawo to przyznano w celu zapobiegania przestępstwom lub ich wykrywania albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych. **Dane, do których uzyskiwania i przetwarzania Policja uzyskała dostęp, są określone odpowiednio w**:

- art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. − Prawo telekomunikacyjne (Dz. U. z 2017 r. poz. 1907, z późn. zm.) − tzw. dane telekomunikacyjne[20],
- art. 18 ust. 1–5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2017 r. poz. 1219, z późn. zm.) – tzw. dane internetowe.

Ponadto, zgodnie z art. 20cb ust. l, Policja jest uprawniona do pozyskiwania – w celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych m.in. danych:

- z wykazu, o którym mowa w art. 179 ust. 9 ustawy – Prawo telekomunikacyjne (dane z elektronicznego wykazu abonentów, użytkowników lub zakończeń sieci, w tym dane uzyskiwane przy zawarciu umowy),
- o których mowa w art. 161 ustawy – Prawo telekomunikacyjne (dane dotyczące użytkownika, do których przetwarzania jest uprawniony dostawca publicznie dostępnych usług telekomunikacyjnych).

Znowelizowany przepis art. 20c ustawy o Policji wskazuje następujące cele gromadzenia i przetwarzania danych telekomunikacyjnych, pocztowych lub internetowych:

1) zapobieganie lub wykrywanie przestępstw (z wyłączeniem przestępstw skarbowych),
2) ratowanie życia lub zdrowia ludzkiego,
3) wsparcie działań poszukiwawczych lub ratowniczych.

Co istotne, niezależnie od celu przetwarzania, ich uzyskanie następuje w trybie określonym w art. 20c ust. 2–4 ustawy o Policji. **Oznacza to, że przedsiębiorca telekomunikacyjny lub usługodawca świadczący usługi drogą elektroniczną udostępnia nieodpłatnie te dane**:

1) policjantowi wskazanemu w pisemnym wniosku Komendanta Głównego Policji, Komendanta CBŚP, komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej;
2) na ustne żądanie policjanta posiadającego pisemne upoważnienie Komendanta Głównego Policji, Komendanta CBŚP, komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej;
3) za pośrednictwem sieci telekomunikacyjnej policjantowi posiadającemu pisemne upoważnienie Komendanta Głównego Policji, Komendanta CBŚP, komendanta wojewódzkiego Policji albo osoby przez nich upoważnionej.

W postępowaniu przygotowawczym Policja nie jest uprawniona do uzyskiwania danych telekomunikacyjnych i internetowych w drodze bezpośredniego zwracania się do przedsiębiorców. W dochodzeniu lub śledztwie takie dane Policja może uzyskać za pośrednictwem prokuratora. Ma tutaj bowiem zastosowanie przepis art. 236a k.p.k. Oznacza to, że zgodnie z przepisami procedury karnej, ujawnienie takich informacji, jak np. adres IP komputera (danych eksploatacyjnych) może nastąpić na żądanie sądu lub prokuratora poprzez wydanie odpowiedniego postanowienia na podstawie art. 218 w związku z art. 236a k.p.k.

Ustawa o Policji – jak wskazano wyżej – w art. 20c statuuje odrębną od k.p.k. podstawę prawną dla uzyskiwania przez policjantów danych telekomunikacyjnych lub internetowych (ust. 1). Przepis ten ustanawia procedurę ich uzyskiwania (ust. 2–4) oraz wskazuje sposób ich włączania do postępowania karnego (ust. 6)[21]. Policja może uzyskiwać dane telekomunikacyjne i internetowe, m.in. w celu zapobiegania przestępstwom lub ich wykrywania. Nie budzi wątpliwości, że postępowanie przygotowawcze to działalność Policji ukierunkowana na wykrywanie przestępstw. Tak więc policjant prowadzący postępowanie przygotowawcze, ale także postępowanie sprawdzające (art. 307 k.p.k.), może wystąpić – na podstawie art. 20c ustawy o Policji – o udostępnienie danych telekomunikacyjnych lub internetowych, a po ich uzyskaniu i stwierdzeniu, że mają one znaczenie dla postępowania karnego, powinien uruchomić procedurę ich przekazania określoną w ust. 6 art. 20c ustawy o Policji i doprecyzowaną w decyzji nr 98 KGP w sprawie uzyskiwania i przetwarzania przez Policję danych telekomunikacyjnych, pocztowych oraz internetowych.

Konkludując, policjant na dwa sposoby może uzyskać dane telekomunikacyjne lub internetowe dla potrzeb prowadzonego postępowania przygotowawczego lub sprawdzającego. We wszczętym postępowaniu, kiedy jego zakres przedmiotowy i podmiotowy jest już dookreślony, te dane Policja może uzyskać tylko za pośrednictwem prokuratora. W takim układzie procesowym – co do zasady – właściwym trybem uzyskiwania danych telekomunikacyjnych lub internetowych jest wydanie przez prokuratora (z urzędu lub na wniosek Policji) stosownego postanowienia na podstawie art. 218 k.p.k. w zw. z art. 236a k.p.k. Należy jednak pamiętać, że zgodnie z art. 20c ustawy o Policji, Policja może uzyskiwać przedmiotowe dane, m.in. w celu zapobiegania przestępstwom lub ich wykrywania. Wówczas przesłanki podjęcia czynności aktualizują się głównie w etapie realizowania przez Policję czynności operacyjno-rozpoznawczych. Zatem pełne wykorzystanie możliwości, jakie daje art. 20c ustawy o Policji, następuje w toku wykonywania czynności poprzedzających decyzję o wszczęciu postępowania przygotowawczego w sprawie, czyli także w postępowaniu sprawdzającym, o którym mowa w art. 307 k.p.k. Nie można jednak całkowicie wykluczać tej drogi uzyskiwania tych danych już we wszczętym postępowaniu, np. w odniesieniu do osób spoza kręgu podejrzanych objętych danym postępowaniem. Każdorazowo należy wówczas rozważać zasadność wykorzystania tej drogi oraz dokonywać oceny istnienia przesłanki warunkującej możliwość zastosowania czynności wskazanych w art. 20c ust. 1 ustawy o Policji. W takim przypadku przekazania danych mających znaczenie dla postępowania właściwemu miejscowo lub rzeczowo prokuratorowi dokonują odpowiednio Komendant Główny Policji, Komendant CBŚP albo komendant wojewódzki (Stołeczny) Policji.

Wyrażam nadzieję, że ten artykuł w jakimś stopniu będzie wsparciem w wypracowaniu prawidłowej interpretacji obowiązujących przepisów i w ślad za nią – poprawnej praktyki Policji w ramach prowadzonych pod nadzorem prokuratora postępowań przygotowawczych, w których znaczącą rolę dowodową odgrywają dane informatyczne.

[1] *Rocznik statystyczny Rzeczypospolitej Polskiej 2016*, Warszawa 2016, s. 439 i 441.

[2] *Poczta i telekomunikacja. Wyniki działalności w 2016 r.*, GUS, Warszawa 2017, s. 65.

[3] Zob. więcej M. Siwicki, *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7–8, s. 241–250.

[4] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie w dniu 23 listopada 2001 r. (Dz. U. z 2015 r. poz. 728).

[5] Ustawa z dnia 10 stycznia 2003 r. o zmianie ustawy – Kodeks postępowania karnego, ustawy – Przepisy wprowadzające Kodeks postępowania karnego, ustawy o świadku koronnym oraz ustawy o ochronie informacji niejawnych (Dz. U. Nr 17, poz. 155).

[6] Ustawa z dnia 18 marca 2004 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego oraz ustawy – Kodeks wykroczeń (Dz. U. Nr 69, poz. 629).

[7] Zob. prace Sejmu RP IV kadencji – Rządowy projekt ustawy o zmianie ustawy − Kodeks karny, ustawy − Kodeks postępowania karnego oraz ustawy − Kodeks wykroczeń druk sejmowy nr 2013, s. 34, http://orka.sejm.gov.pl/proc4.nsf/opisy/2031.htm.

[8] „236a. Przepisy rozdziału niniejszego 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 w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną".

[9] Patrz: *Kodeks postępowania karnego. Komentarz*, red. J. Skorupka, Wydawnictwo C.H. BECK, Warszawa 2015, s. 551.

[10] Patrz: A. Lach, *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, „Prokuratura i Prawo" 2003, nr 10, s. 21.

[11] Patrz: J. Kudła, A. Staszak, *Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. chmurze*, „Prokuratura i Prawo" 2017, nr 7–8, s. 21–57.

[12] Należy pamiętać, że czynności te reguluje k.p.k., ale także (w odniesieniu do Policji) cytowane w literaturze odnoszącej się do przeszukania systemu informatycznego wytyczne KGP w sprawie wykonywania niektórych czynności dochodzeniowo-śledczych przez policjantów. Patrz: rozdział 10 wytycznych nr 3 Komendanta Głównego Policji z dnia 30 sierpnia 2017 r. w sprawie wykonywania niektórych czynności dochodzeniowo-śledczych przez policjantów (Dz. Urz. KGP poz. 59).

[13] A. Lach, *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, „Prokuratura i Prawo" 2003, nr 10, s. 24.

[14] W Policji stosuje się opracowany w KGP wzór formularza protokołu przeszukania urządzenia zawierającego dane informatyczne, systemu informatycznego lub nośnika z danymi informatycznymi.

[15] Dr Marek Chrabkowski, Wyższa Szkoła Administracji i Biznesu im. Eugeniusza Kwiatkowskiego w Gdyni, mgr inż. Krzysztof Gwizdała, biegły z zakresu badań komputerowych przy Sądzie Okręgowym w Gdańsku.

[16] http://www.ies.krakow.pl/wydawnictwo/prokuratura/pdf/2015/12/9chrabkowski.pdf.

[17] Niektóre rozwiązania wykorzystują do szyfrowania zawartości dysków moduł sprzętowy, umiejscowiony na płycie głównej komputera (a więc poza nośnikiem danych). Odszyfrowanie danych zawartych na dysku jest możliwe tylko za pomocą modułu, który je zaszyfrował, stąd konieczność zabezpieczenia całego komputera.

[18] Wystąpienie RPO z dnia 2 czerwca 2016 r. do KGP, sygn. II.519.1253.2015.NBe.

[19] W brzmieniu nadanym ustawą z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 147).

[20] Patrz: rozporządzenie Ministra Infrastruktury z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania (Dz. U. Nr 226, poz. 1828).

[21] Przedmiotową problematykę uszczegóławia decyzja nr 98 Komendanta Głównego Policji z dnia 1 kwietnia 2016 r. w sprawie uzyskiwania i przetwarzania przez Policję danych telekomunikacyjnych, pocztowych oraz internetowych (Dz. Urz. KGP poz. 14, z późn. zm.).

Summary

The procedural aspect of the fight against cybercrime

In the article there was discussed an issue of procedural revealing and recording electronic evidence, i.e. procedural steps having a form of holding the IT data and searching the device containing such data or the IT system. The author presents the essence of these steps. Regulations accepted in Poland were presented in the context of international regulations. Moreover, obtaining telecommunications and Internet data in preparatory proceedings, including the procedures from Art. 20C of the Police Act, were discussed.

Tłumaczenie: Renata Cedro

PRAKTYCZNE ASPEKTY ZABEZPIECZANIA SPRZĘTU KOMPUTEROWEGO

podkom. Paweł Olber

Instruktor Zakładu Cyberbezpieczeństwa
Instytutu Służby Kryminalnej Wydziału Bezpieczeństwa Wewnętrznego
Wyższej Szkoły Policji w Szczytnie

W niniejszym artykule wyjaśniono istniejące wątpliwości dotyczące prawidłowego podejścia do pozyskiwania materiału dowodowego w formie cyfrowej. Autor odnosi się do metod i procedur opublikowanych w literaturze fachowej, które uważa za nieodpowiednie oraz anachroniczne. Twierdzi, iż należy sprostać wyzwaniom dotyczącym stałego i dynamicznego rozwoju technologicznego w kontekście wzrastającego znaczenia dowodów elektronicznych w sprawach karnych. Obecne podejście do przedmiotowego zagadnienia wymaga uaktualnienia w celu pozyskiwania materiału dowodowego w formie cyfrowej na miejscu zdarzenia poprzez zabezpieczenie nietrwałych danych. Autor artykułu porządkuje również podstawowe kwestie związane z elektronicznym materiałem dowodowym poprzez zdefiniowanie konkretnej koncepcji oraz przedstawienie jej charakterystycznych cech.

WSTĘP

Dowód cyfrowy posiada cechy, które odróżniają go od tradycyjnych dowodów rzeczowych, i w związku z tym powinien być traktowany w sposób szczególny. Dane w postaci cyfrowej mogą być łatwo zniszczone lub utracone. Pierwsze czynności na miejscu zdarzenia, w trakcie których zabezpieczane są cyfrowe środki dowodowe, mają istotny wpływ na przebieg całego postępowania karnego. Dlatego urządzenia i znajdujące się w nich dane muszą być prawidłowo zabezpieczone. Należy jednak zaznaczyć, że w krajowych przepisach prawnych brak jest wytycznych zawierających metodykę zabezpieczania śladów cyfrowych. Metodyka zabezpieczania cyfrowych środków dowodowych pozostawiona została praktyce, czyli pewnym zwyczajom i procedurom, które wyznacza wiedza oraz doświadczenie życiowe i praktyczne specjalistów informatyki śledczej.

Stały i dynamiczny rozwój nowych technologii wymusza konieczność ciągłej aktualizacji i nieustannego dostosowywania sposobu postępowania w zakresie zabezpieczania dowodów cyfrowych. Oczywiste jest, że zabezpieczenie tego rodzaju dowodów powinno być przeprowadzone w sposób pozwalający uniknąć ich modyfikacji.

Przegląd literatury z tego zakresu pozwala stwierdzić, że niektóre z zalecanych praktyk dotyczących zabezpieczenia budzą poważne wątpliwości, np. takie, które w przypadku uruchomionego sprzętu komputerowego nakazują m.in. natychmiastowe wyłączenie komputera poprzez wyciągnięcie wtyczki przewodu zasilającego. Zdaniem autora proponowane sposoby zabezpieczania dowodów cyfrowych stwarzają ryzyko trwałej utraty danych, pomimo że ich celem jest niedopuszczenie do takiej sytuacji. W związku z powyższym niezbędne wydaje się wyjaśnienie i usystematyzowanie problematyki związanej z zabezpieczaniem dowodów cyfrowych. Z uwagi jednak na ogromną liczbę i różnorodność urządzeń mogących zawierać dane cyfrowe, w niniejszym artykule kwestie te zostaną omówione na przykładzie sprzętu komputerowego.

Autor podejmie próbę oceny opisywanej w literaturze metodyki zabezpieczania dowodów elektronicznych w postaci sprzętu komputerowego. Ponieważ kluczową kwestią w zakresie zabezpieczania ich jest techniczna możliwość zabezpieczania danych ulotnych, zostaną zaproponowane ogólne założenia nowego podejścia do zabezpieczania dowodów elektronicznych, które zdaniem autora powinny być uwzględniane podczas zabezpieczania dowodów w postaci sprzętu komputerowego.

1. Dowód cyfrowy

W polskich przepisach prawnych nie ma żadnej definicji dowodu elektronicznego. Najczęściej przytaczana jest definicja opracowana przez Międzynarodową Organizację do spraw Dowodów Komputerowych (International Organization on

Computer Evidence), zgodnie z którą dowód elektroniczny to: „informacje przechowywane lub przekazywane w formie binarnej, które mogą być przedstawione w sądzie" (ang. *information stored or transmitted in binary form that may be relied upon in court*)[1]. Należy zaznaczyć, że dowód elektroniczny nie jest rzeczą i ma charakter niematerialny, mimo że jest przetwarzany z wykorzystaniem obiektów materialnych[2], na przykład za pośrednictwem sprzętu komputerowego. Właściwość ta sprawia, że dowód elektroniczny ma cechy szczególne, które odróżniają go od tradycyjnych dowodów rzeczowych[3]. Cechy te zostały wymienione poniżej.

Łatwość modyfikacji i usunięcia – niewłaściwe i niekontrolowane postępowanie z dowodami elektronicznymi może doprowadzić do ich nieuzasadnionej modyfikacji lub usunięcia. Uszkodzeniu ulec może także sam nośnik zawierający dane w postaci cyfrowej. Z tego powodu wymagane jest zastosowanie szczególnych środków ostrożności podczas zabezpieczania i analizy tego typu dowodów. Zdaniem autora, przed przystąpieniem do zabezpieczenia sprzętu komputerowego konieczne jest przeprowadzenie identyfikacji systemu operacyjnego oraz sprawdzenie jego zasobów. W ramach tej czynności osoba zabezpieczająca dane powinna dokonać m.in. sprawdzenia, czy zasoby systemu operacyjnego są zaszyfrowane, ponieważ ustalenia te będą determinowały sposób zabezpieczenia danych. Czynności te z pewnością spowodują modyfikację danych, przy czym są one niezbędne do prawidłowego zabezpieczenia materiału dowodowego. Bardzo ważne jest, aby zakres modyfikacji był minimalny, uzasadniony i bardzo szczegółowo opisany w sporządzonej dokumentacji procesowej.

Poszlakowy charakter – w większości przypadków dowód elektroniczny wskazuje na sprawcę przestępstwa dopiero w zestawieniu go z innymi dowodami. Pozyskanie danego dowodu elektronicznego nigdy nie prowadzi bezpośrednio do wskazania sprawcy przestępstwa. Zdaniem autora cecha ta charakteryzuje również inne ślady i dowody, w związku z czym brak jest uzasadnienia do stosowania jej jako kryterium odróżniające dowody elektroniczne od tradycyjnych dowodów rzeczowych.

Szczególne podejście – dowód elektroniczny musi być odpowiednio zabezpieczony, uwierzytelniony, a następnie poddany badaniom. Warto podkreślić, że sposób zabezpieczenia powinien być aktualny i dostosowany do rodzaju dowodu elektronicznego.

Równość kopii i oryginału – badania dowodów cyfrowych powinny być prowadzone na kopii utworzonej na zasadzie równości z oryginałem. Utworzoną kopię binarną należy uwierzytelnić za za pomocą funkcji skrótu.

2. Sprzęt komputerowy jako dowód cyfrowy

Wszelkie czynności związane z dowodami cyfrowymi powinny być wykonywane zgodnie z przyjętymi zasadami informatyki śledczej[4] – gałęzi nauk sądowych, której celem jest dostarczenie cyfrowych środków dowodowych popełnionych przestępstw lub nadużyć, a także odtworzenie stanu poprzedniego w celu ustalenia motywów działania sprawcy lub ofiary[5]. Zasady te sprowadzają się przede wszystkim do dbania autentyczność i wierność dowodu cyfrowego. Autentyczność odnosi się do bezsporności pochodzenia materiału, z kolei wierność rozumiana jest jako możliwość stwierdzenia, czy materiał nie został w żaden sposób zmieniony w trakcie zabezpieczenia lub podczas badań[6]. Zdaniem autora wierność dowodu cyfrowego należy rozumieć również jako możliwość udokumentowania świadomie wykonanych czynności w systemie operacyjnym zabezpieczanego komputera (co wiąże się także ze świadomą modyfikacją danych w minimalnym zakresie) oraz sposobność potwierdzenia tych zmian w późniejszym etapie podczas przeprowadzania badań informatycznych. Zasadność rozszerzenia znaczenia pojęciowego cechy, jaką jest wierność dowodu cyfrowego, wynika z aktualnego stanu wiedzy z zakresu nowych technologii. Dotyczy to również rozwiązań programowych, które obecnie umożliwiają zabezpieczanie danych ulotnych w szczególności w postaci pamięci RAM, co z kolei wiąże się z modyfikacją danych elektronicznych. Wydaje się jednak, że rozszerzenie dotychczasowego podejścia do dowodów cyfrowych o dodatkowy element, jakim są dane ulotne, jest racjonalne i uzasadnione. Potwierdzeniem tego stwierdzenia jest wyrok Sądu Najwyższego z dnia 20 czerwca 2013 r., sygn. III KK 12/13[7], z treści którego wynika, że informatyka śledcza jako dziedzina rozwija się w bardzo szybkim tempie. Wymiar sprawiedliwości musi więc dążyć do uzyskiwania wiedzy o jak najdoskonalszych metodach zabezpieczania dowodów w sprawie, a do takich niewątpliwie należą procedury przewidujące zabezpieczanie danych ulotnych. Sąd Najwyższy podkreślił również, że do tematu dowodów elektronicznych należy podejść bardzo ostrożnie, ponieważ statystycznie dane te bardzo często ulegają modyfikacjom, co wynika z samej istoty zapisu elektronicznego.

Sposób zabezpieczania sprzętu komputerowego zależy od stanu, w jakim znajduje się sprzęt w chwili podejmowania czynności. Możemy mieć do czynienia ze sprzętem, który jest wyłączony lub uruchomiony. Ocenienie stanu, w jakim znajduje się sprzęt w chwili zabezpieczenia, również może przysporzyć pewnych trudności osobie, która nie posiada stosownej wiedzy. Zdarzyć się może bowiem, że sprzęt znajduje się w stanie wstrzymania (w tzw. trybie uśpienia), w celu zmniejszenia poboru prądu. W tym stanie komputer wyłącza część urządzeń, np. monitor, dyski twarde oraz zmienia tryb pracy procesora[8]. Wszystkie informacje pozostają jednak zapisane w pamięci RAM, która jest pamięcią ulotną, przechowującą dane tak długo, jak długo włączone jest zasilanie. W przypadku odłączenia zasilania dane zapisane w pamięci RAM zostają utracone.

Zabezpieczenie wyłączonego sprzętu komputerowego jest bardzo proste i sprowadza się do opisu cech identyfikacyjnych sprzętu oraz odpowiedniego zabezpieczenia technicznego, w sposób chroniący sprzęt przed uszkodzeniami mechanicznymi.

Sposób zabezpieczenia uruchomionego komputera jest już trudniejszym zadaniem. Prawdą jest, że w takiej sytuacji należy zachować szczególną ostrożność, ponieważ każde użycie komputera (otwarcie lub zamknięcie programu, dokumentu itd.) prowadzi do modyfikacji danych. Nie sposób się jednak zgodzić ze stwierdzeniem, że przeglądanie zawartości uruchomionego sprzętu jest całkowicie niedopuszczalne[9]. Zdaniem autora istnieją uzasadnione przypadki, w których wymagane będzie sprawdzenie zawartości zasobów systemu operacyjnego. Zaliczyć do nich można chociażby konieczność sprawdzenia, czy uruchomiony system operacyjny korzysta z dodatkowych dysków sieciowych, które mogą znajdować się w tym samym pomieszczeniu, lub też konieczność sprawdzenia, czy dane znajdujące się na dysku komputera są zaszyfrowane. W zależności od stwierdzonych na miejscu faktów możliwe będzie podjęcie dalszych decyzji co do sposobu zabezpieczenia danych. Gdy okaże się, że system zawiera dane zaszyfrowane, konieczne będzie wykonanie obrazu zawartości pamięci RAM oraz obrazu

zawartości logicznej dysków zamontowanych w komputerze. Przedmiotowy sposób postępowania pozwoli na uzyskanie dostępu do danych cyfrowych, które w dalszej kolejności zostaną poddane badaniom kryminalistycznym, zgodnie z zakresem zleconym przez funkcjonariusza prowadzącego postępowanie.

3. Istniejące procedury zabezpieczania dowodów cyfrowych

Opisywane w literaturze przedmiotu procedury i metody zabezpieczania uruchomionego sprzętu komputerowego zawierają m.in. informacje o konieczności natychmiastowego odłączenia kabla sieciowego w celu uniemożliwienia zdalnej komunikacji z systemem. Ma to na celu jak najszybsze wyłączenie komputera w sposób, który nie wpłynie negatywnie na zawarte dane[10]. Przedmiotowy sposób postępowania należy uznać jednak za postępowanie nieaktualne, niewłaściwe, a wręcz destrukcyjne. Metoda ta przekreśla szansę uzyskania miarodajnej opinii biegłego. Z całą pewnością powyższe stwierdzenie podzielają sami biegli z zakresu badań informatycznych policyjnych laboratoriów kryminalistycznych, którzy od dawna nie stosują wyżej opisywanego podejścia. W przypadku, kiedy dane znajdujące się na dysku twardym będą zaszyfrowane, wyżej wymienione postępowanie dotyczące zabezpieczania komputera spowoduje ich bezpowrotną utratę, co z pewnością utrudni wyjaśnienie sprawy. W odniesieniu do istniejących metod można zadać pytanie, czy natychmiastowa izolacja sprzętu komputerowego poprzez odłączenie kabla sieciowego lub zasilającego na pewno nie spowoduje zmiany stanu systemu operacyjnego. Zdaniem autora każda decyzja podjęta przed zabezpieczeniem włączonego sprzętu komputerowego powoduje modyfikację danych, w tym również wyłączenie zasilania, odłączenie sprzętu od sieci czy też pozostanie biernym i niezrobieniem niczego.

4. Prawidłowe zabezpieczanie dowodów cyfrowych

Ze względu na specyfikę dowodów cyfrowych oraz (zdaniem autora) konieczność uwzględniania podczas zabezpieczania danych ulotnych, wskazane jest dobranie do tej czynności biegłego z zakresu badań informatycznych lub przeszkolonego specjalisty. Przy czym należy zaznaczyć, że zabezpieczenie danych ulotnych nie powinno być czynnością obligatoryjną, wykonywaną każdorazowo podczas zabezpieczania sprzętu komputerowego. Decyzja o zabezpieczeniu danych powinna być podjęta przez osobę uprawnioną, posiadającą odpowiednie kompetencje. Kilkanaście lat temu jako powód udziału biegłego lub specjalisty w czynnościach zabezpieczania śladów elektronicznych wskazywano konieczność utrwalania danych wyświetlonych na monitorach oraz połączeń między urządzeniami poprzez wykonanie zdjęć, sporządzenie kopii nośników itp.[11] Obecnie od biegłego/specjalisty wymaga się znacznie więcej, ponieważ zabezpieczanie dowodów elektronicznych wymaga bardzo dobrej znajomości systemów teleinformatycznych oraz oprogramowania. Dlatego też należy uznać, że udział biegłego z zakresu badań informatycznych lub specjalisty jest konieczny w każdym przypadku zabezpieczania dowodów cyfrowych. Wynika to z konieczności wstępnego sprawdzenia zasobów systemowych i określenia na tej podstawie właściwej metodyki postępowania, która pozwoli na zabezpieczenie danych w sposób właściwy.

Jak wspomniano na początku artykułu, w Polsce brak jest regulacji dotyczących zabezpieczania dowodów elektronicznych. Istnieją jednak międzynarodowe standardy wskazujące sposób zabezpieczania dowodów elektronicznych, które opisane zostały w dokumencie *Good Practise Guide for Computer – Based Electronic Evidence*[12], opracowanym przez Stowarzyszenie Komendantów Policji (*Association of Chief Police Officers* – ACPO). Pierwsza zasada zawarta w tym dokumencie mówi o tym, że żadne działania podejmowane przez organy ścigania lub osoby uprawnione do zabezpieczenia materiału dowodowego nie powinny modyfikować danych przechowywanych w komputerze lub na innym nośniku pamięci, ponieważ mogą mieć one istotne znaczenie w postępowaniu. Kolejna zasada przewiduje jednak dostęp do danych oryginalnych, przy czym czynności te muszą być wykonane przez osobę posiadającą odpowiednie uprawnienia i umiejętności, która powinna również podać powód i cel swoich działań. Zgodnie z trzecią zasadą, wszelkie czynności związane z uzyskiwaniem i zabezpieczaniem dowodów elektronicznych powinny być udokumentowane. Ostatnia reguła mówi o tym, że osoba wykonująca wyżej wymienione czynności związane z zabezpieczaniem dowodów elektronicznych ponosi całkowitą odpowiedzialność za przestrzeganie obowiązujących przepisów prawa oraz realizację czynności zgodnie z wyżej wymienionymi zasadami. Podkreślić należy, że proponowane założenia nowego podejścia do zabezpieczania dowodów cyfrowych, uwzględniające zabezpieczanie danych ulotnych, są zgodne z regułami wskazanymi w dokumencie *Good Practise Guide for Computer – Based Electronic Evidence*.

Wśród krajowych opracowań również można znaleźć propozycje, które zawierają elementy (etapy postępowania) doskonale wpisujące się w proponowane założenia. Przykładem jest chociażby procedura podkreślająca, że informacje cyfrowe zabezpiecza się w kolejności od najbardziej ulotnych do najmniej ulotnych[13]. W przypadku pozostałych propozycji można mieć jednak pewne wątpliwości. Przykładem niech będzie np. stwierdzenie, że zabezpieczanie informacji cyfrowych powinno przebiegać z wykorzystaniem rozwiązań technicznych uniemożliwiających modyfikację źródła. Zgodnie z wyżej wymienionym zapisem mamy do czynienia z pewną sugestią co do sposobu zabezpieczenia, a nie z postępowaniem, które ma być realizowane w sposób obligatoryjny. Wydaje się jednak, że wyżej wymieniona zasada powinna również uwzględniać rozwiązania programowe, a nie jedynie ograniczać się do środków technicznych.

Wracając do kwestii zabezpieczania sprzętu komputerowego, należy przyjąć, że właściwe podejście do zabezpieczania dowodów cyfrowych powinno uwzględniać dane ulotne, zapisane m.in. w pamięci RAM, która obecnie może mieć bardzo dużą pojemność i zawierać istotne informacje o znaczeniu dowodowym. Warto pamiętać, że wyłączenie urządzenia może mieć nieodwracalne skutki i w przypadku szyfrowania może doprowadzić do trwałej utraty dostępu do danych. Istnieje zatem potrzeba wprowadzenia zmian w funkcjonującym podejściu do zabezpieczania danych. Jest ona spowodowana przez dynamicznie zmieniające się środowisko pracy, czego przykładem są niżej wymienione sytuacje:

- aplikacje oraz systemy operacyjne mogą być instalowane w pamięciach przenośnych USB, a następnie uruchamiane w pamięci operacyjnej RAM bez pozostawiania jakichkolwiek śladów na dysku;

- złośliwe oprogramowanie może być przechowywane w pamięci RAM, bez jakichkolwiek śladów istnienia na dysku;
- użytkownicy mogą wykorzystywać dane zaszyfrowane lub ukryte;
- popularne przeglądarki internetowe oferują użytkownikowi możliwość zacierania śladów.

Innym przykładem sytuacji uzasadniającej natychmiastowe sprawdzenie zawartości systemu operacyjnego jest zabezpieczenie sprzętu w firmie finansowo-księgowej. Istnieje wysokie prawdopodobieństwo, że na dyskach twardych komputerów znajdujących się w takiej firmie jest zainstalowane specjalistyczne oprogramowanie, którego uruchomienie poza środowiskiem macierzystego systemu operacyjnego będzie znacznie utrudnione lub wręcz niemożliwe. Dotyczy to z reguły aplikacji operujących na złożonych zbiorach danych lub programów, do których uruchomienia niezbędne jest posiadanie indywidualnego klucza sprzętowego[14]. W przypadku identyfikacji tego rodzaju oprogramowania należy podjąć decyzję o zabezpieczeniu całej jednostki komputerowej oraz uwzględnić zasoby sieciowe, jeżeli system księgowy korzystał z tego rodzaju danych. Niezależnie od okoliczności i podjętych na miejscu zdarzenia decyzji w zakresie zabezpieczenia dowodów elektronicznych trzeba pamiętać, że wszelkie nieprawidłowości w sposobie zabezpieczania dowodów elektronicznych mogą doprowadzić do uznania tych dowodów za wadliwe i wykluczenia ich z materiału dowodowego. Stwierdzenie wadliwości dowodu może skutkować uchyleniem decyzji procesowych oraz doprowadzić do umorzenia postępowania, a nawet uniewinnienia oskarżonego[15].

WNIOSKI

Podsumowując, należy stwierdzić, że problematyka zabezpieczania dowodów cyfrowych jest tematem złożonym i trudnym, a przy tym bardzo istotnym. Niewłaściwe postępowanie podczas zabezpieczania sprzętu komputerowego może skutecznie i trwale uniemożliwić uzyskanie dostępu do danych i tym samym udaremnić przeprowadzenie badań komputerowych. Natychmiastowe odłączanie wtyczki zasilającej od sprzętu, który jest uruchomiony, należy uznać za niszczenie materiału dowodowego, ponieważ bardzo często skutkuje brakiem możliwości późniejszej analizy bądź w sposób znaczący przedłuża jej czas. Warto podkreślić, że przedstawione powyżej postępowanie może doprowadzić do utraty danych oraz narazić na odpowiedzialność cywilną z tytułu wyrządzonej szkody czy też na odpowiedzialność karną za przestępstwo z art. 231 kk[16]. Ponadto takie podejście nie uwzględnia kluczowych elementów, istotnych z punktu widzenia późniejszej analizy danych. Zaliczamy do nich:

- sprawdzenie, czy system korzysta z zasobów sieci lokalnej lub z Internetu;
- zidentyfikowanie, czy dane w systemie informatycznym są szyfrowane;
- weryfikację, czy dane przechowywane są w tzw. chmurze;
- ustalenie, czy w systemie zainstalowane jest oprogramowanie umożliwiające zdalne sterowanie za pomocą urządzenia mogącego znajdować się w dowolnej lokalizacji;
- sprawdzenie, czy w systemie znajdują się maszyny wirtualne, symulujące działanie dodatkowych komputerów;
- ustalenie, czy system operacyjny został uruchomiony z pamięci przenośnej USB lub z nośnika optycznego.

Natychmiastowe wyłączenie sprzętu komputerowego bez przeprowadzenia wstępnej identyfikacji środowiska informatycznego skutkuje trwałą i nieodwracalną utratą danych, gdyż informacje w powyższych przypadkach dostępne będą jedynie z poziomu uruchomionego systemu operacyjnego w chwili zabezpieczania sprzętu. Wyłączenie urządzenia spowoduje trwałą utratę informacji w nim przechowywanych, które mogą mieć ogromne znaczenie w prowadzonych postępowaniach.

Aby sprostać wyzwaniom ciągłego i dynamicznego rozwoju technologicznego, a co za tym idzie – zwiększającego się znaczenia dowodów elektronicznych w sprawach karnych, należy dokonać aktualizacji obecnego podejścia do zabezpieczania dowodów cyfrowych na miejscu zdarzenia poprzez uwzględnienie w tym procesie danych ulotnych.

[1] E. Casey, *Digital Evidence and Computer Crime, Third Edition: Forensic Science, Computers and the Internet,* Academic Press 2011, s. 7.
[2] *Elementy informatyki sądowej*, red. M. Szmit, Polskie Towarzystwo Informatyczne 2011, s. 28.
[3] P. Krejza, *Informatyka śledcza jako element reakcji na incydenty,* „Hakin9" 2008, nr 3, s. 54.
[4] Postuluje się również stosowanie pojęcia informatyka sądowa. Zob. M. Szmit, *Wybrane zagadnienia opiniowania sądowo-informatycznego*, Kraków 2014, s. 22.
[5] *Informatyka śledcza,* w: *Wikipedia*, https://pl.wikipedia.org/wiki/Informatyka_śledcza [dostęp: 16.11.2017 r.].
[6] M. Niebrzydowska, R. Kotowicz, *Wstęp do informatyki śledczej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 6, s. 62.
[7] Wyrok Sądu Najwyższego z dnia 20 czerwca 2013 r. (sygn. III KK 12/13), https://sip.legalis.pl/document-full.seam?documentId=mrswglrsgy2tmobwha2tg, [dostęp: 30.10.2017 r.].
[8] *Stan wstrzymania,* w: *Wikipedia,* https://pl.wikipedia.org/wiki/Stan_wstrzymania [dostęp: 29.10.2017 r.].
[9] P. Karasek, *Gdy dowodem są dane – czyli prawdy i mity związane z pozyskiwaniem dowodów cyfrowych,* http://www.edukacjaprawnicza.pl/gdy-dowodem-sa-dane-czyli-prawdy-i-mity-zwiazane-z-pozyskiwaniem-dowodow-cyfrowych/ [dostęp: 16.11.2017 r.].
[10] W. Kasprzak, *Ślady cyfrowe. Studium Prawno-Kryminalistyczne*, Warszawa 2015, s. 126.
[11] A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 134.
[12] *Good Practise Guide for Computer – Based Electronic Evidence,* http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf [dostęp: 16.11.2017 r.].
[13] M. Niebrzydowska, R. Kotowicz, *Wstęp do informatyki,* s. 62.
[14] A. Chrabkowski, K. Gwizdała, *Zabezpieczenie dowodów elektronicznych*, „Prokuratura i Prawo" 2015, nr 12, s. 167.
[15] Tamże, s. 178.
[16] A. Lach, *Dowody elektroniczne*, s. 120.

Summary

Practical aspects of handling computer hardware

This work explains existing doubts about the right approach for the acquire digital evidence. The author refers to the methods and procedures published in the literature of the subject which he considers to be inappropriate and out of date. According to the author, the challenges of continuous and dynamic technological development must be met, and hence the increasing importance of electronic evidence in criminal cases. In this case, the current approach needs to be updated to acquire digital evidence at the scene of the incident, by taking volatile data in this process. Author also organizes basic issues related to electronic evidence by defining the concept and presentation of its characteristic features.

Tłumaczenie: Renata Cedro

WSPARCIE PROGRAMISTYCZNE POLICJI

nadkom. Arkadiusz Sobolewski
Zastępca Naczelnika Wydziału Wsparcia Programistycznego
Biura Łączności i Informatyki KGP

mł. insp. Grażyna Ryszkowska
Naczelnik Wydziału Wsparcia Programistycznego
Biura Łączności i Informatyki KGP

Wydział Wsparcia Programistycznego realizuje działania integracyjne i standaryzacyjne w zakresie funkcjonowania systemów teleinformatycznych Policji, prowadzi prace optymalizacyjne w obszarach programistycznych i współdziała na linii interoperacyjności w zakresie systemów centralnych Policji. Szczególne zadania programistyczne dotyczą projektowania rozwiązań i ich wdrażania w systemach krytycznych Policji, które mimo realizowanych modyfikacji i działań rozwojowych muszą być w każdej chwili dostępne dla funkcjonariuszy Policji. Kolejnym obszarem działań, którym zajmuje się Wydział Wsparcia Programistycznego, jest prowadzenie czynności projektowych w zakresie wdrażanych modernizacji, takich jak przygotowanie, inicjowanie oraz modelowanie procesu zmian.

Wydział Wsparcia Programistycznego Biura Łączności i Informatyki Komendy Głównej Policji ma na celu wspieranie wydziałów Biura oraz innych jednostek i komórek organizacyjnych Policji w zakresie usług programistycznych. Jego zadania są określane przez bieżące potrzeby Biura Łączności i Informatyki KGP w odniesieniu do utrzymania i modernizacji centralnych systemów teleinformatycznych Policji.

Ponadto wydział realizuje zadania związane z prowadzeniem projektów teleinformatycznych, które obejmują zasięgiem obszar całego kraju oraz mają bezpośredni wpływ na codzienną pracę funkcjonariuszy Policji.

Wywodząc rodzaj realizowanych zadań od nazwy, należy podkreślić, że Wydział Wsparcia Programistycznego jest komórką Biura Łączności i Informatyki KGP, która działa w zakresie szeroko pojętych usług programistycznych. Zadania te są bardzo różnorodne i obejmują takie płaszczyzny, jak: modernizacja aplikacji pod kątem zmian interfejsu (tworzenie kodów źródłowych do istniejących już aplikacji), tworzenie nowych kodów źródłowych dla rozwijania i wspierania projektowanych funkcjonalności, tworzenie nowych aplikacji, analizowanie i ocena kierunków rozwoju informatyki oraz możliwości wykorzystania nowych narzędzi programistycznych w informatyce policyjnej.

Wskazany obszar realizowanych zadań jest bardzo szeroki i nie do końca zdefiniowany, gdyż jego możliwą do wskazania granicę stanowią po prostu wszystkie czynności programistyczne.

Wydział nie ogranicza się jedynie do wybranego rodzaju usług programistycznych i realizuje zadania we wszystkich językach programowania. Specjaliści wydziału tworzą kody źródłowe w takich językach, jak: Java, Visual Basic czy C++.

Szczególne zadania programistyczne dotyczą projektowania rozwiązań i ich wdrażania w systemach krytycznych Policji, które mimo realizowanych modyfikacji i działań rozwojowych muszą być w każdej chwili dostępne dla funkcjonariuszy Policji. Dlatego też programiści tworzą dodatkowe środowiska pozwalające (w sposób neutralny dla systemu) na testowanie zaprojektowanych zmian. Do takich rozwiązań należą obsługiwane przez WWP środowiska:

- developerskie (umożliwiające realizację prac programistycznych i testowych);
- testowe (umożliwiające obserwowanie systemu po wprowadzeniu zmian);
- szkolne (umożliwiające naukę nowych rozwiązań wdrożonych w systemie dla użytkowników końcowych).

Należy również zwrócić uwagę na liczne przedsięwzięcia wydziału, które dotyczą wspólnych działań z podmiotami zewnętrznymi. Stanowią one duże wyzwanie dla tak małego liczebnie wydziału, który musi się mierzyć z pełnymi zespołami programistycznymi producentów zewnętrznych przewyższających go nie tylko liczebnością kadr, ale także mobilnością oraz środkami finansowymi. Mimo to WWP,

stając na wysokości zadania, bierze udział w nowych projektach, które są realizowane w kooperacji m.in. z: grupą podmiotów Ministerstwa Spraw Wewnętrznych i Administracji (np. Strażą Graniczną), Ministerstwem Cyfryzacji, Inspektoratem Transportu Drogowego, Głównym Urzędem Geodezji i Kartografii.

Jednak wszystkie te zadania są determinowane poprzez zarządzanie projektami. Aby można było realizować postulowane zadania, konieczny jest wcześniejszy etap przygotowania, inicjowania oraz samego modelowania procesu zmian. Takie zadania spoczywają również na członkach projektowego zespołu programistycznego. Jest to drugi rodzaj działań, którym zajmuje się Wydział Wsparcia Programistycznego.

Obszar projektowania zmian jest niezwykle złożony i w ogromnym stopniu wpływa na dalszy ciąg procesu zmian, realizacji i wdrożenia zadań modernizacyjnych czy rozwojowych. Etap przygotowania postulowanych zmian to wszystkie wstępne ustalenia, które dotyczą aspektów merytorycznych. Zleceniodawca (komórka lub jednostka organizacyjna Policji) opisuje zmiany, których chce dokonać w odniesieniu do obecnych funkcjonalności aplikacji. Działania te, oprócz wstępnych ustaleń, koncentrują się na wytworzeniu karty projektu, która musi być zaakceptowania przez BŁiI KGP. Specjaliści WWP oceniają propozycję zmian pod kątem możliwości ich realizacji od strony technicznej, by na dalszym etapie inicjowania projektu potwierdzić je w dokumentach projektowych – w tym w Projekcie Technicznym, Studium Wykonalności czy notacjach BPMN, UML. Specjaliści WWP projektują architekturę rozwiązania logicznego czy fizycznego z uwzględnieniem obowiązujących strategii informatycznych dla Policji oraz dostosowania do projektów już realizowanych przez wymienione wyżej podmioty zewnętrzne.

W trakcie realizacji projektu jest dokonywanych wiele niezależnych od siebie, ale integralnych operacji wdrożeniowych w następujących przykładowych obszarach:

- polityka bezpieczeństwa;
- ochrona danych osobowych;
- analiza zgodności z normami prawnymi (resortowymi i cywilnymi);
- modelowanie przebiegu procesów biznesowych i przepływu danych;
- projektowanie założeń polityki i instrukcji bezpieczeństwa;
- założenie obszaru tematycznego na Policyjnej Platformie Wdrożeniowej (prowadzenie konsultacji);
- opracowanie założeń pionu analitycznego i programistycznego dla obszaru aplikacyjnego, bazodanowego i serwerowego;
- prace programistyczne;
- prace programistyczne dla środowisk testowych, szkolnych i produkcyjnych;
- modyfikacje programistyczne dla wersji finalnej programu;
- ciągłe testowanie programu w wybranych komórkach;
- nadzorowanie garnizonów w pracach w środowisku testowym;
- udzielanie wsparcia programistycznego dla wojewódzkich komórek IT;
- monitorowanie wybranych wskaźników prac wdrożeniowych;
- prowadzenie interaktywnych, ogólnopolskich wideokonferencji.

Zespół projektowy WWP opracowuje obecnie kilkadziesiąt projektów, w tym nową strategię rozwoju systemów teleinformatycznych dla Policji. Zadaniem tego zespołu, w którego skład wchodzą przedstawiciele wszystkich pionów służby policyjnej, jest analiza, opracowanie oraz przedstawienie kierunków zmian, które są konieczne w związku z nieustannym postępem w rozwoju techniki informatycznej, ewaluowania zagrożeń w obszarze cyberprzestępczości oraz interoperacyjności z wciąż powstającymi nowymi rozwiązaniami teleinformatycznymi w pionie administracji publicznej. Obecnie specjaliści z WWP dostosowują funkcjonujące systemy teleinformatyczne Policji do nowych rozwiązań i zmian legislacyjnych m.in. w takich systemach, jak:

- KSIP;
- ERCDŚ;
- SWD;
- SWOP;
- systemy międzynarodowe SIS2, VIS;
- systemy niejawne.

Do najważniejszych i największych projektów, które aktualnie prowadzi Wydział Wsparcia Programistycznego, należy zaliczyć:

1) projekt CEPIK 2.0 realizowany zgodnie z wytycznymi Ministerstwa Cyfryzacji;
2) mapę przestępstw o charakterze seksualnym; WWP zaprojektowało oraz wykonało dedykowane mechanizmy integracyjne umożliwiające współpracę z systemem Krajowego Rejestru Karnego w celu umożliwienia publikacji danych dotyczących miejsc przebywania sprawców popełniających przestępstwa na tym tle; dodatkowo zostaną wykonane niezbędne rozszerzenia wykorzystywanych w Policji aplikacji mobilnych, dające możliwość prowadzenia wyszukiwania w Krajowym Rejestrze Karnym;
3) centralizację w ramach optymalizacji Elektronicznego Rejestru Czynności Dochodzeniowo-Śledczych; ten system jest jednym z największych systemów policyjnych (obecnie ma ponad 35 000 użytkowników), przeznaczonym dla służby dochodzeniowo-śledczej, obejmuje cały kraj; projekt na obecnym etapie przewiduje migrację wszystkich baz ERCDŚ KWP do centralnego serwera i jego administrowanie z poziomu KGP;
4) modernizację Systemu Wspomagania Obsługi Policji; jest projektem, w którym dokonuje się zmian w funkcjonalnościach systemu; z jednej strony zespół projektowy uzgadnia, projektuje oraz wdraża zmiany modyfikujące system w poszczególnych modułach SWOP, a z drugiej – rozszerza jego obszar oddziaływania na kolejne komórki i jednostki organizacyjne Policji; obecnie odnotowano ponad 2 200 000 logowań w miesiącu do tego systemu informatycznego Policji;
5) rozwój Systemu Wspomagania Obsługi Policji; dotyczy projektowania nowych funkcjonalności dla SWOP; są konsultowane i zgłaszane nowe moduły i podmoduły Systemu Wspomagania Obsługi Policji; obecnie zespół WWP prowadzi 19 projektów w zakresie nowych rozwiązań dla SWOP, w tym m.in.: SWOP. BHP, SWOP. Medycyna Pracy, SWOP. KKOP, SWOP. Policyjna Izba Zatrzymań, SWOP. Elektroniczne L-4;
6) projekt wymiany danych systemu ERCDŚ z centralnym systemem Prokuratury Krajowej; w ramach projektowanych funkcjonalności jest m.in. możliwość dostępu przez funkcjonariuszy Policji do zeskanowanych akt postępowań przygotowawczych znajdujących się w komórkach prokuratorskich;
7) włączenie systemów policyjnych do ogólnopolskiej platformy eFaktury; zespół projektowy rozpoczął prace anali-

Wzór dowodu osobistego.
Źródło: http://www.mswia.gov.pl z dnia 18.12.2017 r.

tyczne nad zaprojektowaniem rozwiązań informatycznych systemu SWOP do połączenia z centralną platformą, przez którą będą przepływać wszystkie elektroniczne faktury; jest to związane z wejściem w życie Dyrektywy 2014/55/UE w sprawie elektronicznego fakturowania w dostawach publicznych;

8) projekt opracowania rekomendacji rozwoju systemów teleinformatycznych Policji; zespół analizuje i zbiera opinie oraz dane dotyczące wszystkich centralnych systemów teleinformatycznych Policji od użytkowników tych systemów; w skład zespołu wchodzą przedstawiciele wszystkich pionów służby policyjnej; na podstawie opracowanej metodologii zostanie sporządzona analiza przyszłych kierunków rozwoju, które są konieczne w związku z nieustannym postępem w rozwoju techniki informatycznej, ewaluowania zagrożeń w obszarze cyberprzestępczości oraz interoperacyjności z wciąż powstającymi nowymi rozwiązaniami teleinformatycznymi w pionie administracji publicznej;
9) Rejestr Dowodów Osobistych – przedmiotowe rozwiązanie zostało zaprojektowane z myślą o stworzeniu możliwości natychmiastowego uzyskania wizerunku sprawdzanej osoby na służbowym urządzeniu mobilnym; podsystem RDO na podstawie wprowadzonych danych osobowych kieruje zapytanie do Rejestru Dowodów Osobistych, a jego wynik prezentuje w postaci zapisanej w tym systemie fotografii, co pozwala na natychmiastowe porównanie wizerunku sprawdzanej przez funkcjonariusza osoby; oprócz korzystania z wersji mobilnej została zapewniona także możliwość pracy w podsystemie RDO w trybie stacjonarnym z użyciem standardowego komputera PC;

Samochody służbowe KGP. Fot. Katarzyna Lipińska.
Źródło: BŁiI KGP.

10) Elektroniczna Karta Zdarzenia Drogowego – dedykowana aplikacja przeznaczona do uruchamiania na terminalach mobilnych, umożliwiająca dokumentowanie wszelkich informacji związanych z zaistniałymi zdarzeniami drogowymi, istotnymi dla postępowań prowadzonych przez funkcjonariuszy Ruchu Drogowego.

Bardzo szybki postęp technologiczny stawia przed zespołami informatycznymi wiele wyzwań, które bardzo często nie zostały dostatecznie zdefiniowane w obszarach często pokrewnych dla samych działań programistycznych, np. w sferze legislacyjnej czy kadrowej. Stąd sama realizacja zadań przez programistów coraz częściej wiąże się z płaszczyznami dotąd traktowanymi jako autonomiczne: projektową, prawną lub sieciową. Determinanty prowadzenia prac programistycznych w coraz większym stopniu leżą po stronie komórek i jednostek Policji (np. biura KGP, KWP) czy nawet podmiotów zewnętrznych dla BŁiI KGP (np. ministerstwa). Wydział Wsparcia Programistycznego realizuje działania integracyjne i standaryzacyjne w zakresie funkcjonowania systemów teleinformatycznych Policji, prowadzi prace optymalizacyjne w obszarach programistycznych i współdziała na linii interoperacyjności w zakresie systemów centralnych Policji. Stąd niebagatelnym wyzwaniem będzie umiejętne wzbogacanie kompetencji własnych na płaszczyźnie wciąż rosnących wymagań użytkowników dyktowanych przez czynniki zewnętrzne, w tym również przez postęp techniczny.

Summary

Programming support of the Police

The Programming Support Department implements integration and standardization actions in functioning of ICT systems of the Police, conducts improvement works in programming areas and cooperates in the field of interoperability of the central systems of the Police. Specific programming tasks concern the design of solutions and their implementation in critical systems of the Police, which in spite of carried out modifications and development activities must be at any time available to police officers. Conducting design activities in implemented modernizations such as preparation, initiation and modeling of the process of changes, is the next area of action performed by the Programming Support Department.

Tłumaczenie: Renata Cedro

KRAJOWY SYSTEM BEZPIECZEŃSTWA MORSKIEGO

dr hab. inż. Tadeusz Stupak

Adiunkt
Akademia Morska w Gdyni
Katedra Nawigacji

Każdy statek musi posiadać wyposażenie radiowe umożliwiające w razie katastrofy wezwanie pomocy z lądu. Sprzęt radiowy ma umożliwić komunikację foniczną oraz automatyczne wysłanie alarmu. Rodzaj środków zależy od odległości statku od brzegu. Ponadto są używane radiopławy pozwalające wyznaczyć za pomocą satelitów miejsce katastrofy i transpondery do lokalizacji rozbitków w obszarze poszukiwań.

System Automatycznej Identyfikacji AIS oraz System Identyfikacji i Śledzenia dalekiego zasięgu LRIT monitorują ruch statków i wspomagają Krajowy System Bezpieczeństwa Morskiego (wchodzący w skład europejskiego systemu), który bazuje na obserwacji radarowej dla nadzoru nad ruchem statków wzdłuż naszych brzegów.

WSTĘP

Działania na morzu muszą spełniać wymagania międzynarodowe. Ratowanie życia na morzu jest obowiązkowe i zajmuje się tym służba poszukiwawczo-ratownicza SAR (Search and Rescue). W celu wezwania pomocy jest wykorzystywany Światowy System Łączności w Niebezpieczeństwie i Bezpieczeństwa – Global Maritime Distress and Safety System (GMDSS). Umożliwia on również komunikację eksploatacyjną i transmisje danych. Drugi problem to głównie ochrona środowiska morskiego przed zanieczyszczeniem spowodowanym katastrofą morską. Tym zajmuje się administracja morska – Urząd Morski. W naszym kraju zadanie to realizuje Krajowy System Bezpieczeństwa Morskiego (KSBM), zajmujący się monitorowaniem ruchu, jego organizacją, ostrzeżeniami itp. Dane zbierane przez ten system są na bieżąco przekazywane do europejskiej agencji bezpieczeństwa morskiego.

1. System Łączności w Niebezpieczeństwie i Bezpieczeństwa – GMDSS

System Łączności w Niebezpieczeństwie i Bezpieczeństwa (Global Maritime Distress and Safety System) wprowadzano na statki w latach 1980–1999. Trwało to tak długo, ponieważ należało przebudować mostki nawigacyjne i wymienić całe wyposażenie radiowe na wszystkich statkach, natomiast operatorem, zamiast specjalnego radiooficera, zostawał oficer wachtowy, który musiał odbyć dodatkowe przeszkolenie. Według założeń tego systemu statek (niezależnie od wielkości) musi posiadać działające równocześnie dwa niezależne od siebie systemy łączności z lądem. Akcje poszukiwawczo-ratownicze są koordynowane przez ośrodki lądowe. Całe terytorium mórz i oceanów podzielono na 4 obszary według

wykorzystywanych urządzeń łączności. Wyposażenie radiowe statku zależy od tego, w których akwenach on nawiguje. System nie tylko umożliwia priorytetową komunikację w niebezpieczeństwie, ale także jest wykorzystywany do celów bieżącej eksploatacji i zarządzania statkiem. Akcję pomocy statkowi w niebezpieczeństwie planuje i koordynuje ośrodek lądowy (morskie ratownicze centrum koordynacyjne – MROK), który otrzymuje dane o ruchu statków od administracji morskiej, dysponuje statkami i lotnictwem ratowniczym.

W skład GMDSS wchodzą następujące podsystemy [1]:

- radiotelefonia FM w paśmie ultrakrótkofalowym – VHF;
- radiotelefonia SSB w paśmie fal pośrednich i krótkich – MF i HF;
- system cyfrowego selektywnego wywołania – DSC w paśmie VHF, MF i HF;
- satelitarny system radiokomunikacji morskiej – INMARSAT;
- satelitarny system alarmowania i lokalizacji obiektów na morzu COSPAS – SARSAT;
- satelitarne radiopławy awaryjne EPIRB umożliwiające lokalizację miejsca wysłania alarmu i transpondery radarowe SART, które pokazują pozycje rozbitka na ekranie statkowego radaru;
- radiotelegrafia dalekopisowa NBDP;
- systemy transmisji ostrzeżeń nawigacyjnych i meteorologicznych NAVTEX działające w obszarach NAVAREA o promieniu 400 mil morskich od nadawczych stacji brzegowych systemu;
- satelitarny system wywołania grupowego EGC działający w sieci INMARSAT.

Poszczególne **podsystemy GMDSS umożliwiają** realizację zadań określonych w Konwencji SOLAS [4]. Należą do nich:

- alarmowanie o wystąpieniu niebezpieczeństwa na morzu;
- koordynacja i prowadzenie akcji ratunkowej;
- lokalizowanie miejsca katastrofy morskiej;
- rozpowszechnianie informacji o katastrofie i o zagrożeniu bezpieczeństwa żeglugi.

W systemie GMDSS wyróżnia się następujące obszary [2]:

A1 – obszar morski będący w zasięgu przynajmniej jednej stacji nadbrzeżnej ultrakrótkofalowej VHF, pracującej w paśmie morskim 156–174 MHz, z której jest możliwa ciągła i skuteczna łączność alarmowania za pomocą cyfrowego selektywnego wywołania – DSC (ang. *Digital Selective Calling*) na kanale 70 (156,525 MHz); zasięg działania tego obszaru wynosi średnio 20–30 mil morskich (Mm); mila morska odpowiada jednej minucie szerokości geograficznej (około 1852 m), dlatego ta jednostka jest przydatna, gdy posługujemy się współrzędnymi geograficznymi;

A2 – obszar morski, poza akwenem A1, będący w zasięgu stacji nadbrzeżnej pośrednio falowej MF z wyłączeniem obszaru A1, z której jest możliwe alarmowanie za pomocą DSC na częstotliwości 2187,5 kHz; zasięg działania tego obszaru wynosi średnio do 150 mil morskich;

A3 – obszar morski z wyłączeniem obszaru A1 i A2, z którego jest możliwe alarmowanie za pomocą morskiego satelitarnego systemu radiokomunikacyjnego INMARSAT, pracującego z wykorzystaniem 4 satelitów geostacjonarnych. Zasięg działania tego obszaru przyjęto określać między 70. równoleżnikiem szerokości geograficznej północnej i południowej;

A4 – obszar morski poza obszarami A1 A2 i A3, a więc obejmujący obszary podbiegunowe; prowadzona jest tu radiokomunikacja na falach krótkich w paśmie 4÷30 MHz z użyciem systemu teleksowego ARQ (NBDP) i FEC, DSC, radiotelefonii SSB.

Radiopławy pracujące w paśmie VHF

Radiopławy w paśmie VHF systemu DSC-EPIRB (Digital Selective Calling) pracują w paśmie VHF na kanale 70 (156,525 MHz). Sygnały mogą zostać odebrane przez inny statek lub stację brzegową. Takie radiopławy efektywnie mogą być wykorzystywane w strefie morza A1, dla automatycznego wysyłania sygnałów wzywania pomocy [1]. Pojemność baterii powinna zapewnić pracę przez co najmniej 48 godzin.

Częstotliwości wykorzystywane w obszarze A2

Do zapewnienia koordynacji akcji poszukiwawczej służą zwykłe częstotliwości niebezpieczeństwa w paśmie fal pośrednich na częstotliwości 2187,5 kHz i VHF. Łączność z samolotami na miejscu akcji prowadzi się zwykle na częstotliwości 3023; 4125; 5680 kHz oraz z lotnictwem SAR na częstotliwościach 2182 kHz; 156,8 MHz, lub 121,5 MHz [3].
Częstotliwość 2182 kHz została przypisana łączności radiotelefonicznej w niebezpieczeństwie oraz dla zapewnienia łączności na miejscu akcji, a częstotliwość 2174,5 kHz – łączności radioteleksowej (NBDP).

Środki łączności dalekiego zasięgu

Łączność dalekiego zasięgu na falach krótkich jest stosowana w obszarze A4 w pasmach 4, 6, 8, 12 i 16 MHz, natomiast w rejonie A3 – system satelitarny INMARSAT.
Łączność w niebezpieczeństwie oraz w celu zapewnienia bezpieczeństwa prowadzona po wywołaniu DSC jest realizowana za pomocą radiotelefonu lub radioteleksu (NBDP).

Satelitarne środki łączności

W ramach systemu GMDSS (Global Maritime Distress and Safety System) na oceanach jest używana łączność satelitarna oparta na 4 satelitach geostacjonarnych. Natomiast celem zapewnienia określania miejsca katastrofy ustanowiono system satelitarny Cospas-Sarsat, w ramach którego na podstawie pomiarów dopplerowskich sygnałów z radiopław EPIRB (Emergency Position Indication Radio Beacon) jest wyznaczana pozycja rozbitka [3].

System ten powstał w 1982 r. w wyniku połączenia amerykańskiego systemu SARSAT (Search and Rescue Satellites) oraz rosyjskiego (wówczas radzieckiego) COSPAS (Kosmiczeskaja Sistemma Poiska Awarijnych Sudien) [8]. Segment kosmiczny składa się z satelitów utrzymywanych przez Rosję (typ Nadieżda) i Stany Zjednoczone (NOAA typu Tiros); niektóre komponenty są produkowane przez Kanadę i Francję. Satelity amerykańskie NOAA (National Oceanic and Atmospheric Administration) obiegają Ziemię raz na 100 minut po orbicie o inklinacji 89° względem równika i wysokości 849 km. Przenoszenie przekaźników systemu SARSAT jest funkcją dodatkową dla satelitów NOAA. Ich główne zadanie stanowi praca w systemie zbierania danych środowiskowych Argos. Satelity rosyjskie serii Nadieżda mają czas obiegu 105 minut, a ich orbita ma inklinację 83° i wysokość 999 km. Każdy satelita systemu posiada odbiornik sygnałów radiowych o częstotliwości 406,025 MHz z procesorem i pamięcią oraz nadajnik pracujący na częstotliwości 1544,5 MHz.

Lokalizacja radiopławy z wykorzystaniem odbiornika nawigacyjnego jest możliwa z dokładnością kilkunastu metrów, natomiast **pomiary dopplerowskie** (ze względu na niską stabilność sygnału pławy) pozwalają określać jej położenie z **dokładnością do około 5 kilometrów**. System jest mało dokładny, ale zapewnia niezawodność lokalizacji.

Oprócz wymienionych satelitów, przekaźniki SARSAT są zamontowane na geostacjonarnych satelitach GOES 8, GOES 9 i GOES 10 (projekt GEOSAR – Geostationary Satellite SAR). Satelity te nie mogą lokalizować nadajników metodą dopplerowską – są tylko przekaźnikami pozycji podawanej przez pławę z jej odbiornika nawigacyjnego. Na podstawie transmitowanej pozycji pławy powiadamia się właściwą stację ratowniczą − RCC. Lokalnych stacji odbiorczych LUT jest 38 w 21 krajach. Nowe satelity systemów GPS i Galileo mają mieć możliwość retransmisji tych sygnałów.

Transponder ratowniczy SART

W ramach systemu łączności w niebezpieczeństwie GMDSS wprowadzono procedury automatycznego powiadamiania o katastrofie za pomocą radiopławy, a następnie przewidziano wyposażenie statku w urządzenia umożliwiające lokalizację rozbitka z wykorzystaniem radaru w obszarze prowadzenia akcji. Jest to transponder ratowniczy SART, który należy do obowiązkowego wyposażenia statku. Również polskie kutry rybackie łowiące na Bałtyku mają posiadać jeden transponder. Planuje się ich wprowadzenie na jednostki rekreacyjno-sportowe. Po uruchomieniu ma on gwarantować pracę, oczekując na sygnał radaru przez 96 godzin, a następnie 8 godzin współpracować z radarami [9]. Jego sygnał pokazany na ekranie radaru jako ciąg 12 kropek ma być rejestrowany z odległości nie mniejszej niż 6 mil morskich.
Od 1 stycznia 2010 r. jako równorzędne wprowadzono transpondery oparte na systemie AIS, nazwane AIS-SART, które pracują w paśmie VHF i są odporne na zakłócenia hydrometeorologiczne [5].

Modernizacja radiokomunikacji morskiej VHF w polskiej strefie ekonomicznej

Obecnie Straż Graniczna posiada własny system łączności VHF na morzu składający się z 11 stacji rozmieszczonych wzdłuż polskiego wybrzeża, ale planuje się zwiększenie liczby stacji.
W Polsce, na potrzeby systemu GMDSS, pracuje satelitarna stacja w Psarach (Góry Świętokrzyskie) dla obszaru A3, stacja pośrednio falowa dla obszaru A2 w Rekowie i wynośne stacje VHF w LM (latarnia morska) Kikut, LM Gąski, LM Czołpino, LM Rozewie, LM Krynica Morska i na platformie Baltic Beta. Zainstalowanie radiotelefonów VHF na platformie Beta powiększa obszar A1 do granic polskiej strefy ekonomicznej [11]. Każda stacja VHF jest wyposażona w dwa zdalnie obsługiwane radiotelefony typu MX 800 firmy Spectra i manipulator MinikomIP firmy Elvys dla potrzeb SAR i taki sam zestaw pracujący dla potrzeb operatorów KSBM. Główne centrum zarządzania systemem zlokalizowano w siedzibie Morskiego Ratowniczego Centrum Koordynacyjnego (MRCK) w Gdyni, natomiast centrum pomocnicze w Morskim Pomocniczym Centrum Koordynacyjnym (MPCK) w Świnoujściu. Oba centra zarządzania i stacje lądowe są ze sobą połączone poprzez sieci WAN urzędów morskich oraz na wypadek awarii sieci są dzierżawione łącza radiowe pomiędzy centrami VTS.
Do celów transmisji danych służy łączność satelitarna. Powoduje to, że ich przechwytywanie jest trudne choćby z tego powodu, iż odległości pomiędzy statkami są duże. Pozyskanie danych o przewożonym ładunku, które mogą być ważne np. dla piratów, jest łatwiejsze w porcie. Dlatego te problemy ochrony transmisji danych na morzu nie są jeszcze istotne.

2. Systemy monitorowania ruchu statków

System Automatycznej Identyfikacji Statków (AIS)

Na statki o pojemności 300 T w żegludze międzynarodowej, 500 w krajowej i wszystkie pasażerskie wprowadzono od 2006 r. urządzenia Systemu Automatycznej Identyfikacji – AIS (Automatic Identification System), w ramach którego nadają one automatycznie wskazania przyrządów o swojej pozycji, kursie i prędkości oraz dane identyfikacyjne z częstością zależną od swojej prędkości. Dla potrzeb systemu przeznaczono w paśmie VHF kanały AIS 1 = 161,975 MHz (kanał 87B) i AIS 2 = 162,025 MHz (kanał 88B). Zapewnia to zasięgi łączności do około 30 Mm. W systemie są przesyłane głównie dane dynamiczne statków (pozycja, kurs, prędkość i numer identyfikacyjny – MMSI), dane statyczne (wymiary, typ, nazwa, sygnał wywoławczy), dotyczące podróży (klasa ładunku niebezpiecznego, port przeznaczenia, liczba osób), ale również informacje pogodowe, ostrzeżenia nawigacyjne, dane o oznakowaniu nawigacyjnym. Wciąż są wprowadzane nowe pakiety transmitowanych danych. Dane dynamiczne są przesyłane z częstotliwością w zależności od prędkości danej jednostki, dane identyfikacyjne – z częstotliwością co 6 minut, a także po każdej zmianie danych [6].

Po wprowadzeniu AIS zwiększyło się bezpieczeństwo – szczególnie na akwenach ograniczonych, trudnych pod względem nawigacyjnym i o dużym natężeniu ruchu. Informacje są przesyłane i zobrazowane na wskaźnikach operatorskich w centrach VTS w sposób automatyczny. Problem stanowi powszechny dostęp do tych danych. Dla własnego bezpieczeństwa możemy wyłączyć urządzenie AIS, dlatego te dane nie mogą być podstawą do unikania kolizji.

Na potrzeby mniejszych statków wprowadzono urządzenie klasy B, które transmituje mniejszą mocą (zasięg do około 8 Mm) i z mniejszą częstością mniej informacji. Szczególnie cenne są te urządzenia dla małych jednostek, ponieważ istnieją trudności z ich wykryciem za pomocą radaru statkowego [10].

Skład systemu AIS PL

Aktualnie wzdłuż wybrzeża Polski pracuje sieć składająca się z trzech obszarów terytorialnych zarządzanych przez urzędy morskie w Gdyni, Słupsku i Szczecinie.

- Do UM Gdynia należą 4 stacje brzegowe, główny system zarządzania siecią komputerową wraz z krajową bazą danych oraz serwerem międzynarodowym w Gdyni.
- Do UM Słupsk należą 3 stacje brzegowe.
- Do UM Szczecin należą 2 stacje śródlądowe na Odrze i 3 stacje morskie.

Urząd Morski w Gdyni (UMG) pełni funkcję Krajowego Koordynatora sieci AIS-PL, który administruje zasobami AIS PL w taki sposób, aby zapewnić właściwe funkcjonowanie oraz dostęp do jej zasobów informatycznych.

System Identyfikacji i Śledzenia Dalekiego Zasięgu (LRIT)

Na obszarach poza zasięgiem brzegowych stacji AIS pracuje System Identyfikacji i Śledzenia Dalekiego Zasięgu – LRIT (Long Range Identification and Tracking). Statki automatycznie wysyłają pozycje i numer identyfikacji według częstości ustalonej przez satelitarną stację brzegową. W tym celu jest wykorzystywany system transmisji satelitarnych INMATSAR lub IRYDIUM. Dane o statkach bandery państwa lub zmierzających do portów danego kraju są następnie transmitowane za pomocą kodowanego Internetu. Informacje o statkach płynących do naszego akwenu musimy znać z wyprzedzeniem, ponieważ możemy się nie zgodzić na wejście w nasz obszar wód ekonomicznych statku, który może stwarzać zagrożenie ekologiczne. System LRIT jest obowiązkowy dla:

- wszystkich statków pasażerskich,
- jednostek High Speed Craft,
- ruchomych platform wiertniczych,
- wszystkich statków powyżej 300 GT.

Informacje z systemu LRIT mają prawo otrzymywać:

- państwo bandery statku – zawsze, niezależnie od pozycji ich statków;
- państwo portu, do którego zmierza statek; informacje mają dotyczyć wszystkich statków płynących do ich portu, znajdujących się poza wodami wewnętrznymi innych państw;
- państwa nabrzeżne; informacje mają dotyczyć wszystkich statków znajdujących się w odległości do 1000 mil od ich brzegu i poza wodami wewnętrznymi innego państwa;
- służba SAR – o wszystkich statkach znajdujących się w obszarze poszukiwań koordynowanych przez tę służbę.

Jednostki te wysyłają jednocześnie sygnał do bazy w Polsce, a także do Międzynarodowego Centrum Danych LRIT.

3. Krajowy system wymiany informacji SafeSeaNet

Krajowy system SafeSeaNet został utworzony dla potrzeb wymiany informacji morskiej i zabezpieczenia jej przed nieautoryzowanym dostępem. Nadzór nad siecią SafeSeaNet objęła od 2004 r. Europejska Agencja Bezpieczeństwa Morskiego. Aplikację sytemu wykonała belgijska firma Getronics. Strona główna aplikacji przedstawia trzy możliwości korzystania z sytemu: wyszukiwanie danych, wprowadzanie danych oraz pobieranie plików w formacie Word [13].

Ze systemu SafeSeaNet mogą korzystać:

- pracownicy administracji morskiej (instytucji służb morskich),
- Straż Graniczna,
- Służba Celna,
- armatorzy,
- agenci statkowi,
- inspektorzy:
  - sanitarni,
  - ochrony środowiska,
  - ochrony rybołówstwa,
- upoważnione służby państwowe [6].

System SafeSeaNet zapewnia wymianę informacji o statkach lub zdarzeniach, stanowiących potencjalne niebezpieczeństwo dla żeglugi lub zagrożenie bezpieczeństwa na morzu, bezpieczeństwa ludzi lub środowiska morskiego, których skutki mogą objąć polskie obszary morskie lub obszary morskie innych państw członkowskich Unii Europejskiej. Ponadto system monitoruje ruch statków, zarządzając nim i pełniąc nad nim nadzór [13].

Elementami zapewniającymi stałe działanie systemu są:

- infrastruktura techniczna,
- Koordynator SafeSeaNet,
- podmioty, które są uprawnione do otrzymywania lub dostarczania informacji do systemu.

W skład infrastruktury technicznej wchodzą podsystemy dotyczące przekazywania informacji. Noszą one nazwę:

- system kontrolno-informacyjny dla polskich portów (PHICS – Polish Harbours Information & Control System),
- system wymiany informacji bezpieczeństwa żeglugi (SWIBŻ).

System wyszukuje informacje o statkach na podstawie numeru IMO, numeru MMSI, sygnału wywoławczego lub jego nazwy. Dane prezentowane przez system obejmują:
- stan statku w ostatnim porcie;
- system raportowania;
- system HAZMAT;
- informacje bezpieczeństwa.

Dane mogą być wprowadzone tylko przez odpowiednie organy państw członkowskich. Po autoryzacji użytkownik może wprowadzić informacje dotyczące statku, portu lub regionu. Jeśli przekazuje informacje w ramach systemu HAZMAT (o przewożonych ładunkach niebezpiecznych) oraz PASSANGER (o pasażerach), identyfikuje statek i udostępnia szczegółowe dane: telefon oraz fax [13].

4. Krajowy System Bezpieczeństwa Morskiego

W Polsce od kilkunastu lat funkcjonuje służba kotroli ruchu statków (VTS − Vessel Traffic Service) nadzorująca ruch statków na torze Szczecin – Świnoujście i Zatoce Gdańskiej. Systemy te bazują na radarach brzegowych i są wspomagane przez stacje pomiarów hydro-meteorologicznych oraz obserwacje kamer CCTV. W latach 2012–2014 te systemy zmodernizowano i włączono do Krajowego Systemu Bezpieczeństwa Morskiego, który pokrywa cały obszar morski wzdłuż naszego wybrzeża. W jego skład wchodzą również stacje DGPS w Dziwnowie i Rozewiu transmitujące na falach długich poprawki do pomiarów GPS, mogą one również wysyłać poprawki do rosyjskiego systemu GLONASS, oraz stacje RTK (Real Time Kinematic). Technika RTK umożliwia uzyskiwanie dużych dokładności lokalizacji na małym obszarze, co jest wykorzystywane podczas prac hydrograficznych i geodezyjnych na morzu. Obecnie stacje RTK pracują na latarni morskiej Hel, w kapitanacie Portu Północnego i na Zatoce Pomorskiej. Urzędy morskie dysponują również aparaturą przenośną, która może być użyta w innych lokalizacjach.

Sieć przesyłu zawiera 3 serwery regionalne zbierające dane ze stacji bazowych AIS. Z nich dane surowe są przekazywane siecią internetu do serwera sumującego strumienie krajowe i do serwera krajowego w CBM Gdynia. Stąd dane trafiają w trybie czasu rzeczywistego do dwóch urzędów morskich w Szczecinie i Słupsku.

W ramach projektu KSBM wykonano wiele inwestycji mających zapewnić wysoki poziom bezpieczeństwa żeglugi na naszych obszarach. Obejmują one:
- montaż radarów brzegowych dalekiego zasięgu: Ustka (na skutek protestów zainstalowano na LM Hel), LM Świnoujście oraz na platformie Baltic Beta,
- montaż radarów portowych (Gdańsk – Nowy Port, Gdynia-S, Hel-SW, Władysławowo, Łeba, Ustka, Darłowo, Kołobrzeg) o zasięgu minimum 12 mil morskich,
- instalacja 6 nowych stacji radarowych i wymiana 6 radarów w ramach modernizacji systemu VTMS Szczecin − Świnoujście,
- montaż 26 kamer wizyjnych CCTV: Gdańsk (3), Gdynia, Hel (2), Władysławowo, Łeba, Ustka, Darłowo, Kołobrzeg (2), Dziwnów i stacje VTMS Świnoujście – Szczecin (13);
- montaż stacji hydrometeorologicznych, w tym: 12 stacji brzegowych, 2 stacje nawodne, wymiana 12 wiatromierzy;
- zakończenie budowy Krajowej Sieci Stacji Bazowych Systemu Automatycznej Identyfikacji Statków (AIS-PL) wraz z Morską Krajową Siecią DGPS [7].

Działanie systemu opiera się na sieci informatycznej, którą opisują następujące punkty [16]:
1) obszary podległe (obszary podległych sensorów), specyfikują obszary geograficzne pozostające pod kontrolą konkretnego serwera;
2) domeny; specyfikują, jaka jest architektura domeny oraz jej związek z obszarem geograficznym;
3) serwery główne i serwery stacji; opisują relacje pomiędzy nimi oraz standardowe i awaryjne procedury operacyjne;
4) stacje robocze; dostosowują system operacyjny i procedury operacyjne dla klienta.

> Każdy sensor, który należy do danego obszaru podległego, jest zarządzany poprzez własny „kontroler sensora" zlokalizowany w serwerze stacji tego obszaru podległego. Wszystkie te „kontrolery sensorów" są również podłączone do serwera głównego centrum VTS, z uwagi na fakt, iż serwer główny centralizuje wszystkie te procesy.

Serwery stacji zapewniają współpracę z centrami, a w czasie uszkodzenia połączenia przejmują lokalną pracę systemu, również rejestrują dane lokalnych sensorów. Serwery główne będą rejestrować dane sensorów przynależących do ich obszarów podległych, a także dane z reszty systemu z wyjątkiem danych video ze zdalnych urządzeń CCTV oraz radarów, które będą rejestrowane w zdalnych serwerach stacji, zgodnie z wymaganiami SOPZ [12].

Jako serwer główny (ang. *main server*) definiuje się obudowę Power Edge M1000e wraz ze wszystkimi w niej zainstalowanymi serwerami Blade. Serwery Blade to rozwiązanie polegające na umieszczeniu od kilku do kilkunastu serwerów w jednej obudowie. W przeciwieństwie do standardowych serwerów, wyposażonych we własny zasilacz, wentylatory, podłączenie myszy, klawiatury i monitora oraz interfejsy komunikacyjne, w przypadku rozwiązania Blade te elementy są wspólne w ramach jednej obudowy [7].

Serwery główne są hostowane na serwerach blade w następujących lokalizacjach:
- Gdynia Centrum VTS,
- Centrum zapasowe w Gdyni,
- Centrum VTS Ustka,
- Centrum VTMS Szczecin,
- Centrum VTMS Świnoujście.

Serwery stacji sterują pracą lokalnych czujników i stacji roboczej, a także pełnią następujące funkcje:
- rejestracja danych wszystkich sensorów lokalnych,
- hostowanie kontrolerów sensorów lokalnych,
- praca awaryjna w sytuacji utraty połączenia z serwerem głównym.

Pomorska Magistrala Telekomunikacyjna

Zgodnie z projektem KSBM etap IIA całe polskie wybrzeże Bałtyku zostało wyposażone w nowoczesny system łączności. Od Mierzei Wiślanej do Szczecina ułożono w ziemi światło-

wód, który zintegrował ważne dla bezpieczeństwa morskiego placówki, czyli państwowe służby bezpieczeństwa, Marynarkę Wojenną RP, Morski Oddział Straży Granicznej oraz SAR – Morską Służbę Poszukiwania i Ratownictwa.
W ramach tego projektu wykonano instalację kabla światłowodowego o pojemności 144 włókien, ułożonego w wybudowanej kanalizacji teletechnicznej na potrzeby rdzenia sieci, instalację kabla światłowodowego o pojemności 24 włókien na potrzeby przyłączy do punktów końcowych, instalację kabla światłowodowego podmorskiego o pojemności 144 włókien ułożonego na odcinku Gdynia – Hel, oraz budowę 19 punktów węzłowych sieci i 23 dodatkowych obiektów końcowych. Pomorska Magistrala Teleinformatyczna, ze względu na swoje przeznaczenie i wykorzystanie, jest magistralą światłowodową budowaną jako niezależne medium transmisyjne i zapewnia większe pasmo przenoszenia – nawet do 3 Tb/s [14].

ZAKOŃCZENIE

W celu zabezpieczenia transportu morskiego, zapewnienia pomocy rozbitkom i minimalizacji prawdopodobieństwa katastrofy powodującej ogromne zanieczyszczenie środowiska powstało wiele międzynarodowych systemów. Proces wprowadzania nowych technologii jest ciągły.
Projekt KSBM zapewnia Polsce spełnienie wymagań Europejskiej Agencji Bezpieczeństwa Morskiego i dostarczy system, który na lata zagwarantuje bezpieczny transport morski wzdłuż naszych wybrzeży.
System ten wykorzystuje najnowsze technologicznie urządzenia, a jego struktura gwarantuje niezawodność pracy dzięki zapewnieniu nadmiarowości i równoległych transmisjach danych.
IMO wprowadziła koncepcję e-nawigacji, w ramach której są realizowane programy mające wprowadzić na morzu naziemny szerokopasmowy Internet. W tym celu statki i oznakowanie nawigacyjne zostaną wyposażone w routery zapewniające znaczne zasięgi (praktycznie od około 6 Mm). Zagwarantuje to bieżącą wymianę danych o sytuacji nawodnej pomiędzy pływającymi jednostkami morskimi i służbami lądowymi, jednak wówczas pojawi się problem autoryzacji danych i ich ochrony.

Na statkach systemy sterowania nie mają połączenia z urządzeniami komunikacji radiowej, co zabezpiecza je przed nieautoryzowanym dostępem, ale istnieją systemy zdalnego monitorowania, co może doprowadzić do groźnych sytuacji.

Literatura

1. Bojarski P., Korcz K., *Radiotelefoniczna łączność statków morskich*, SDK S.C. WSM Gdynia 1996.
2. Czajkowski J., *Światowy morski system łączności alarmowej i bezpieczeństwa*, GMDSS, PWP SKRYBA, Gdańsk 1996.
3. IAMSAR (International Aeronautical and Maritime Search and Rescue Manual), *Międzynarodowy lotniczy i morski poradnik poszukiwania i ratowania*, tom II, *Środki mobilne*, TRADEMAR, Gdynia 2001.
4. Konwencja SOLAS, tekst ujednolicony, Polski Rejestr Statków, Gdańsk 1998.
5. Królikowski A., Stupak T., Wawruch R., *System radarowy administracji morskiej wzdłuż wybrzeża polskiego – aspekty techniczne*. „Logistyka" 2015, nr 4, część 4, s. 4296–4302.
6. Królikowski A., Stupak T., Wawruch R., *System bezpieczeństwa morskiego na polskich wodach morskich*, „Logistyka" 2015, nr 4, część 5, s. 7773–7781,
7. Królikowski A., Stupak T., Wawruch R.: *Realizacja Krajowego Systemu Bezpieczeństwa Morskiego. Polskie porty morskie w procesie przemian europejskiego rynku usług portowych*, red. Salmonowicz H., Szczecin, s. 247–258.
8. Muszyński R., *Metody poszukiwania i lokalizacji wypadków morskich w polskim obszarze morza A1*, Praca dyplomowa, Gdynia 2002.
9. Rezolucja MSC.246(83), "Adoption of Performance Standards for Survival Craft AIS Search And Rescue Transmitters (AIS-SART) for use in Search And Rescue Operations", London 2007.
10. Rezolucja MSC.256(84),"Adoption of Amendments to the International Convention for the Safety of Life at Sea, 1974, as amended", 2008.
11. Stupak T. *Modernizacja systemu SART*, „Przegląd telekomunikacyjny" 2009, nr 1, s. 30–33.
12. *Telecommunication infrastructure of the Polish national maritime safety system*, "Archives of Transport System Telematics", Volume 9, Issue 4, November 2016, pp 27–1.
13. Ustawa z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim (Dz. U. z 2016 r. poz. 281, z późn. zm.).
14. http://www.maritech.com/epirb-gpirb.htm.
15. http://www.saabgroup.com.
16. http://www.umgdy.gov.pl/architekturasystemuksbm.

Summary

National Maritime Security System

Every ship must be equipped with a radio enabling to call for an assistance from the land in case of a maritime disaster. The radio equipment is supposed to enable the audio communication and automatic sending of the alarm. The type of measures depends on the distance of the ship from the coastline. Moreover, there are also used EPIRB (Emergency Position Indicating Radio Beacon), which allow for setting the place of a maritime disaster by means of satellites as well as transponders to locate shipwrecked persons in the area of the search. The systems AIS and LRIT monitor the traffic of ships and support the National Maritime Security System (being included in a European system), which is based on a radar observation to supervise the traffic of ships along our coastline.

Tłumaczenie: Renata Cedro

CYBERBEZPIECZEŃSTWO

Minileksykon

SYSTEMY TELEINFORMATYCZNE (policyjne i pozapolicyjne)

SMI (System Meldunku Informacyjnego) – centralny zbiór informacji, którego celem jest gromadzenie i przetwarzanie informacji uzyskanych przez policjantów w toku wykonywania czynności służbowych.

SWD Policji (System Wspomagania Dowodzenia Policji) – teleinformatyczny system wspomagający pracę oraz działania operacyjne Policji. Stanowi integralny moduł, który tworzy jednorodną platformę teleinformatyczną wspierającą obsługę zgłoszeń, zdarzeń oraz koordynację działań służb ratowniczych i porządkowych.

PESEL (Powszechny Elektroniczny System Ewidencji Ludności) – system informacyjny, który zawiera dane osób przebywających stale na terytorium RP, zameldowanych na pobyt stały lub czasowy trwający ponad 3 miesiące, a także osób ubiegających się o wydanie dowodu osobistego lub paszportu oraz osób, dla których odrębne przepisy przewidują potrzebę posiadania numeru PESEL.

CEPiK (Centralna Ewidencja Pojazdów i Kierowców) – system informacyjny gromadzący dane o pojazdach, ich właścicielach i posiadaczach oraz osobach posiadających uprawnienia do kierowania pojazdami oraz informacje o zawarciu obowiązkowego ubezpieczenia (funkcjonuje jako moduł w KSIP).

Noe.NET (Osadzony) – scentralizowany system informacyjny przechowujący dane o osobach skazanych na pozbawienie wolności oraz tymczasowo aresztowanych, ich zachowaniach, historii pobytu oraz przepustkach. Zgromadzone dane nie tylko ułatwiają pracę zarządzającym placówkami penitencjarnymi, ale także pomagają zdobywać Policji i prokuraturze informacje o podejrzanych w prowadzonych przez te instytucje sprawach.

KRK (Krajowy Rejestr Karny) – jest prowadzony przez Biuro Informacyjne Krajowego Rejestru Karnego wchodzące w skład Ministerstwa Sprawiedliwości. Do zadań biura należy m.in. przetwarzanie danych osobowych oraz danych o podmiotach zbiorowych, podlegających gromadzeniu w rejestrze.

KRS (Krajowy Rejestr Sądowy) – scentralizowana, informatyczna baza danych składająca się z trzech osobnych rejestrów: rejestru przedsiębiorców; rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz publicznych zakładów opieki zdrowotnej; rejestru dłużników niewypłacalnych.

REGON (Rejestr Gospodarki Narodowej) – jest bieżąco aktualizowanym zbiorem informacji o podmiotach gospodarki narodowej, prowadzonym w systemie informatycznym, w postaci centralnej bazy danych oraz terenowych baz danych.

POBYT – system, który obsługuje procedury administracyjne dla prowadzenia rejestrów i ewidencji cudzoziemców w zakresie osiedlenia, uchodźstwa, azylantów, osób ubiegających się o wizy, wydaleń cudzoziemców, zaproszeń, jak również osób związanych procedurą repatriacyjną.

KSIP (Krajowy System Informacyjny Policji) – system informatyczny, w którym przetwarza się informacje ze zbiorów danych Osoba, Fakt, Rzecz oraz Podmiot. Umożliwia otrzymanie informacji o czynnych rejestracjach obiektów zarejestrowanych w systemie.

AFIS – automatyczny System Identyfikacji Daktyloskopijnej będący zbiorem danych daktyloskopijnych, w którym są gromadzone i przetwarzane informacje o odciskach linii papilarnych osób, niezidentyfikowanych śladach linii papilarnych z miejsc przestępstw oraz śladach linii papilarnych, które mogą pochodzić od osób zaginionych, o którym mowa w art. 21h ust. 1 pkt 2 ustawy o Policji.

Aplikacja Klient Mobilny SWD – aplikacja funkcjonująca na mobilnych terminalach noszonych (MTN) lub mobilnych terminalach przewoźnych (MTP), zapewniająca dostęp do systemów teleinformatycznych KSIP za pośrednictwem Systemu Poszukiwawczego Policji w zakresie informacji o osobach lub rzeczach przetwarzanych w zbiorach danych KSIP i zbiorach pozapolicyjnych.

SPP – System Poszukiwawczy Policji stanowiący funkcjonalność (mechanizm) systemów teleinformatycznych KSIP przeznaczony do wyszukiwania oraz sprawdzania informacji o osobach lub rzeczach w zbiorach danych KSIP oraz w dostępnych poprzez systemy teleinformatyczne KSIP zbiorach policyjnych oraz pozapolicyjnych.

Terminal MTN / MTP – mobilny terminal noszony/przewoźny będący stanowiskiem dostępowym do systemów teleinformatycznych KSIP, wykorzystywany do przetwarzania informacji poprzez aplikację Patrol lub aplikację Klienta Mobilnego SWD, a także wymieniający informacje z SWD.

CYBERBEZPIECZEŃSTWO – TERMINOLOGIA

Cyberprzemoc (agresja elektroniczna) – stosowanie przemocy poprzez: prześladowanie, zastraszanie, nękanie, wyśmiewanie innych osób z wykorzystaniem Internetu i narzędzi elektronicznych, takich jak: SMS, e-mail, witryny internetowe, fora dyskusyjne w internecie, portale społecznościowe i inne. Osobę dopuszczającą się takich czynów określa się stalkerem[1].

Mowa nienawiści (ang. *hate speech*) – negatywne emocjonalnie wypowiedzi, powstałe ze względu na domniemaną lub faktyczną przynależność do grupy, tworzone na podstawie uprzedzeń.
Narzędzie rozpowszechniania antyspołecznych uprzedzeń, stereotypów i dyskryminacji ze względu na rozmaite cechy, takie jak: rasa (rasizm), pochodzenie etniczne (ksenofobia), narodowość (szowinizm), płeć (seksizm), tożsamość płciowa (transfobia), orientacja psychoseksualna (homofobia, heterofobia), wiek (ageizm, adultyzm), światopogląd religijny[2].

„Hejt" – obraźliwy lub pełen agresji komentarz zamieszczony w Internecie, działanie w Internecie przejawiające złość, wrogość, nienawiść wobec kogoś[3].

Trollowanie (trolling) – antyspołeczne zachowanie charakterystyczne dla forów dyskusyjnych i innych miejsc w Internecie, w których prowadzi się dyskusje. Osoby uprawiające trollowanie nazywane są trollami.
Trollowanie polega na zamierzonym wpływaniu na innych użytkowników w celu ich ośmieszenia lub obrażenia (czego następstwem jest wywołanie kłótni) poprzez wysyłanie napastliwych, kontrowersyjnych, często nieprawdziwych przekazów czy też poprzez stosowanie różnego typu zabiegów erystycznych. Podstawą tego działania jest upublicznianie tego typu wiadomości jako przynęty, która mogłaby doprowadzić do wywołania dyskusji.
Typowe miejsca działania trolli to grupy i listy dyskusyjne, fora internetowe, czaty itp. Trollowanie jest złamaniem jednej z podstawowych zasad netykiety. Jego efektem jest dezorganizacja danego miejsca w Internecie, w którym prowadzi się dyskusję, i skupienie uwagi na trollującej osobie[4].

Stalking – termin pochodzący z języka angielskiego, który oznacza „podchody" lub „skradanie się". Pod koniec lat 80. XX wieku stalking zyskał dodatkowe negatywne znaczenie na skutek nowego zjawiska społecznego, jakim było obsesyjne podążanie fanów za gwiazdami filmowymi Hollywood. Obecnie stalking jest definiowany jako „złośliwe i powtarzające się nagabywanie, naprzykrzanie się czy prześladowanie zagrażające czyjemuś bezpieczeństwu"[5].

Child grooming (tłum. z ang.: uwodzenie dziecka) – działania podejmowane w celu zaprzyjaźnienia się i nawiązania więzi emocjonalnej z dzieckiem, aby zmniejszyć jego opory i później je seksualnie wykorzystać. Jest to także mechanizm używany, by nakłonić dziecko do prostytucji czy udziału w pornografii dziecięcej. Potocznie poprzez child grooming rozumie się uwodzenie dzieci przez Internet[6].

Sexting (także seksting) – forma komunikacji elektronicznej, w której przekazem jest seksualnie sugestywny obraz lub treść. Termin powstał w pierwszych latach XXI w. jako zrost angielskich słów sex (seks) i texting (czynność wysyłania wiadomości sms). Z czasem jego znaczenie poszerzyło się na wysyłanie podobnych komunikatów także za pomocą innych mediów, na przykład komunikatorów internetowych, wiadomości mms czy portali społecznościowych[7].

Hacking komputerowy – uzyskanie nieautoryzowanego dostępu do zasobów sieci komputerowej lub systemu komputerowego poprzez ominięcie jego zabezpieczeń.

Podsłuch komputerowy – nieuprawnione przechwycenie wszelkich informacji (obejmuje także uzyskanie danych stanowiących tajemnicę państwową lub służbową).

Sabotaż komputerowy – zakłócanie lub paraliżowanie funkcjonowania systemów informatycznych o istotnym znaczeniu dla bezpieczeństwa państwa i jego obywateli.

Szpiegostwo komputerowe – polega na włączeniu się do sieci komputerowej w celu uzyskania wiadomości o charakterze tajemnicy państwowej lub służbowej, której udzielenie obcemu wywiadowi może wyrządzić szkodę RP.

Bezprawne niszczenie informacji – naruszenie integralności komputerowego zapisu informacji, które może nastąpić w wyniku bezprawnego niszczenia, uszkadzania, usuwania lub zmiany zapisu istotnej informacji albo udaremniania czy utrudniania osobie uprawnionej zapoznanie się z nią.

Zakłócenie automatycznego przetwarzania informacji związane ze sprowadzeniem niebezpieczeństwa powszechnego – dotyczące większej liczby osób lub mienia w znacznych rozmiarach.

Fałszerstwo komputerowe – polega na przerabianiu lub podrabianiu dokumentów (elektronicznych) w formie zapisu elektromagnetycznego przez wyspecjalizowane urządzenia. *(Dokumentem jest każdy przedmiot lub zapis na komputerowym nośniku informacji, z którym jest związane określone prawo albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne).*

Oszustwo komputerowe – polega na osiągnięciu korzyści majątkowej lub wyrządzeniu innej osobie szkody przez wpływ na automatyczne przetwarzanie, gromadzenie albo przesyłanie informacji. Formy działania mogą być zróżnicowane i polegać na zmianie, usunięciu lub na wprowadzeniu nowego zapisu na komputerowym nośniku informacji.

Oszustwo telekomunikacyjne – włączenie się do urządzenia telekomunikacyjnego i generowanie na cudzy rachunek impulsów telefonicznych.

Klonowanie numerów IMEI telefonów komórkowych – najczęściej występuje w przypadku telefonów pochodzących z kradzieży. Realizowane może być z wykorzystaniem programów komputerowych (połączenie telefonu z komputerem za pomocą odpowiedniego kabla łączącego lub bezprzewodowo). Zmiana numeru IMEI pozwala na dalsze użytkowanie skradzionego telefonu pomimo blokady dokonanej przez operatora telekomunikacyjnego.

Kradzież impulsów telefonicznych – poprzez nieupoważnione podłączenie kablami do linii abonenckiej lub skrzynki telekomunikacyjnej. Najczęściej realizowane jako przyłączenie zewnętrznego aparatu telefonicznego do skrzynki telekomunikacyjnej zlokalizowanej w odosobnionym miejscu (np. piwnicy) i wykonywanie połączeń na koszt jednego z abonentów.

Nielegalne współdzielenie łączy internetowych – wbrew zawartej umowie z providerem internetowym. Legalny abonent usługi internetowej udostępnia innym osobom Internet poprzez współdzielenie łącza – szybkość połączenia dzielona jest na wszystkich użytkowników. Często osoby współdzielące łącze dzielą się również płatnościami.

Doładowanie kart telefonicznych (magnetycznych i chipowych) i kart pre-paid – zużyte magnetyczne karty telefoniczne mogą być doładowywane z wykorzystaniem programatorów. Karty chipowe (elektroniczne) doładowywane są poprzez wykorzystanie programatorów połączonych z komputerem ze specjalnym oprogramowaniem komputerowym pozwalającym na usunięcie zabezpieczeń karty.

Przełamania centrali telefonicznych – najczęściej wykorzystywane do generowania ruchu telekomunikacyjnego. Przełamania są możliwe ze względu na stosowanie standardowych haseł serwisowych czy braku zabezpieczeń linii telekomunikacyjnych (np. brak systemu analizy łączy na okoliczność nielegalnego podłączenia).

Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań.

Botnet – grupa komputerów zainfekowanych złośliwym oprogramowaniem pozostającym w ukryciu przed użytkownikiem i pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami w ramach botnetu.

Keylogger – rodzaj oprogramowania lub urządzenia rejestrującego klawisze naciskane przez użytkownika.

Wirus komputerowy – program komputerowy posiadający zdolność powielania się, tak jak prawdziwy wirus, stąd jego nazwa. Wirus do swojego działania potrzebuje i wykorzystuje system operacyjny, aplikacje oraz tożsamość użytkownika komputera. Wirusa komputerowego zalicza się do złośliwego oprogramowania. Do zwalczania i zabezpieczania się przed wirusami komputerowymi stosuje się programy antywirusowe oraz bieżące aktualizacje systemów i oprogramowania.

Robak komputerowy – samoreplikujący się program komputerowy, podobny do wirusa komputerowego. Główną różnicą między wirusem a robakiem jest to, że podczas gdy wirus potrzebuje nosiciela – zwykle jakiegoś pliku wykonywalnego (chociaż istnieją wirusy pisane w językach skryptowych podczepiające się pod dokument lub arkusz kalkulacyjny), który modyfikuje, doczepiając do niego swój kod wykonywalny, to robak jest pod tym względem samodzielny, a rozprzestrzenia się we wszystkich sieciach podłączonych do zarażonego komputera poprzez wykorzystanie luk w systemie operacyjnym lub naiwności użytkownika. Oprócz replikacji robak może pełnić dodatkowe funkcje, takie jak niszczenie plików, wysyłanie poczty (z reguły spam) lub pełnienie roli backdoora lub konia trojańskiego[8].

Przestępstwa internetowe

art. 190a § 2	– podszywanie się pod inną osobę, fałszywe profile,
art. 202 kk	– dot. treści pedofilskich,
art. 256 kk	– ekstremizm polityczny – treści faszystowskie,
art. 267 § 1 kk	– nieuprawnione uzyskanie informacji (hacking),
art. 267 § 2 kk	– podsłuch komputerowy (sniffing),
art. 268 § 2 kk	– udaremnienie uzyskania informacji,
art. 268a kk	– udaremnienie dostępu do danych informatycznych,
art. 269 § 1 i 2 kk	– sabotaż komputerowy,
art. 269a kk	– rozpowszechnianie złośliwych programów oraz cracking,
art. 269b kk	– tzw. „narzędzia hackerskie”,
art. 271 kk	– handel fikcyjnymi kosztami,
art. 286 kk	– oszustwo popełniane za pośrednictwem Internetu,
art. 287 kk	– oszustwo komputerowe (phishing).

asp. szt. Artur Rogowski, mł. asp. Łukasz Subocz
Zakład Służby Kryminalnej CSP

[1] https://pl.wikipedia.org/wiki/Cyberprzemoc.
[2] Antysemityzm, chrystianofobia, islamofobia, w: https://pl.wikipedia.org/wiki/Mowa_nienawi%C5%9Bci.
[3] https://pl.wiktionary.org/wiki/hejt.
[4] https://pl.wikipedia.org/wiki/Trollowanie.
[5] https://pl.wikipedia.org/wiki/Stalking.
[6] https://pl.wikipedia.org/wiki/Child_grooming.
[7] https://pl.wikipedia.org/wiki/Sexting.
[8] https://pl.wikipedia.org/wiki/Robak_komputerowy.

CYBERBEZPIECZEŃSTWO. SYSTEMY TELEINFORMATYCZNE (POLICYJNE I POZAPOLICYJNE)

CYBERSECURITY. COMMUNICATION AND INFORMATION SYSTEMS (POLICE AND NON-POLICE)

aplikacja Klient Mobilny SWD	**Mobile Client SWD application**
bezpieczeństwo klienta bankowego	**security of a bank client**
bezprawne niszczenie informacji	**unlawful destruction of information**
botnet	**botnet**
cyberprzemoc (agresja elektroniczna)	**cyber bulling (electronic aggression)**
cyberprzestrzeń	**cyberspace**
doładowanie kart telefonicznych (magnetycznych i chipowych) i kart pre-paid	**top-up of telephone cards (magnetic and microchip) and pre-paid cards**
dostępność	**availability**
fałszerstwo komputerowe	**computer forgery**
hacking komputerowy	**computer hacking**
hejt	**hate**
integralność	**integrity**
keylogger	**keylogger**
klonowanie numerów IMEI telefonów komórkowych	**cloning of IMEI mobile phone numbers**
kradzież impulsów telefonicznych	**theft of call units**
Krajowy System Informacyjny Policji	**National Police Information System**
Kryptografia	**Cryptography**
Kryptologia	**Cryptology**
mowa nienawiści	**hate speech**
Mobilny Terminal Noszony/ Mobilny Terminal Przewoźny	**Mobile Worn Terminal / Mobile Transportable Terminal**
nielegalne współdzielenie łączy internetowych	**illegal sharing of Internet connections**
oprogramowanie szpiegujące	**spyware**
oszustwo komputerowe	**computer fraud**
oszustwo telekomunikacyjne	**telecommunications fraud**
phishing	**phishing**
podsłuch komputerowy	**computer wiretap**
poufność	**confidentiality**
robak komputerowy	**computer bug**
sabotaż komputerowy	**computer sabotage**
seksting	**sexting**
stalking Child grooming	**stalking Child grooming**
System Poszukiwawczy Policji	**Police Search System**
szpiegostwo komputerowe	**computer espionage**
środki płatnicze	**legal tenders**
terminal	**terminal**
trollowanie	**Internet troll / trolling**
wirus komputerowy	**computer virus**
wyciek danych	**data leakage**
zakłócenie automatycznego przetwarzania informacji związane za sprowadzeniem niebezpieczeństwa powszechnego	**disruption of automatic processing of information connected with bringing public danger**

Renata Cedro

PRZESŁUCHANIE Z UDZIAŁEM BIEGŁEGO SĄDOWEGO Z ZAKRESU PSYCHOLOGII

jako element programu doskonalenia zawodowego dla policjantów

mł. insp. Grzegorz Perz
Kierownik
Zakładu Służby Prewencyjnej CSP

Wojciech Brejnak
Biegły sądowy z zakresu psychologii
sądów okręgowych dla Warszawy i Warszawy-Pragi

Artykuł jest odpowiedzią na zainteresowanie przedmiotową problematyką, które zgłaszają słuchacze kursu specjalistycznego dla policjantów w zakresie przeciwdziałania demoralizacji i przestępczości nieletnich oraz działań podejmowanych na rzecz małoletnich. Ta tematyka była już co prawda szeroko omawiana w pierwszym numerze w 2007 r., ale w związku z utrudnioną dostępnością do tego numeru, niniejsza problematyka została omówiona ponownie w niniejszym numerze „Kwartalnika Policyjnego". Zdecydowana większość artykułu opiera się na doświadczeniach własnych biegłego sądowego z zakresu psychologii Wojciecha Brejnaka i stanowi cenne źródło wiedzy, z którym mogą się zapoznać i wykorzystać je w pracy zawodowej wszyscy policjanci zajmujący się na co dzień problematyką nieletnich.

Centrum Szkolenia Policji jest jednostką organizacyjną Policji, której zadanie stanowi między innymi realizacja zajęć dydaktycznych na szkoleniach zawodowych podstawowych i kursach specjalistycznych. Jednym z takich doskonaleń zawodowych organizowanych centralnie, przygotowujących policjantów do wykonywania zadań specjalistycznych, jest kurs specjalistyczny dla policjantów w zakresie przeciwdziałania demoralizacji i przestępczości nieletnich oraz działań podejmowanych na rzecz małoletnich. Jego program wielokrotnie ewoluował, dostosowując swoje treści do aktualnie występujących potrzeb w tym zakresie.

Początki tego kursu sięgają 1997 r., kiedy to w Centrum Szkolenia Policji w Legionowie rozpoczęto realizację programu doskonalenia zawodowego dla policjantów do spraw nieletnich. Od 2007 r., po uwzględnieniu zmian w przepisach resortowych dotyczących szkolnictwa policyjnego, Komendant Główny Policji wprowadził do realizacji program kursu specjalistycznego dla policjantów do spraw nieletnich. Po 2007 r. był on kilkukrotnie nowelizowany, w obecnym kształcie jest realizowany od 7 grudnia 2016 r. Na podkreślenie zasługuje także fakt, iż do sierpnia 2011 r. Centrum Szkolenia Policji było jedyną szkołą policyjną, której powierzono do realizacji ten kurs specjalistyczny. Należy także zauważyć, że program nauczania na tym kursie obejmuje rozległą wiedzę interdyscyplinarną, niezbędną do wykształcenia u słuchaczy konkretnych umiejętności i stosowania ich w praktyce.

Aktualnie realizowany program zajęć

Obecnie zajęcia dotyczące przesłuchania z udziałem biegłego sądowego z zakresu psychologii są realizowane według następującego planu:

Część teoretyczna (wykładowa)

I. Rola i zadania biegłego psychologa

a) w ramach pracy w opiniodawczym zespole sądowych specjalistów (nazywanych przed 2016 r. rodzinnym ośrodkiem diagnostyczno-konsultacyjnym),
b) jako biegłego z listy prezesa sądu okręgowego.

Słuchaczom jest przekazywana wiedza o pracy biegłego sądowego z zakresu psychologii oraz formalnoprawne aspekty powoływania i ogólne zasady współpracy przesłuchującego z biegłym. Dzięki temu będą umieli właściwie przygotować się do realizacji postanowienia o dopuszczeniu dowodu z opinii biegłego psychologa (wydawanego przez prokuratora). Poznają także przykładowe rodzaje postanowień – w zależności od:

– rodzaju sprawy (np. udział przy przesłuchaniu, w czynności okazania, w czasie wizji lokalnej),
– wieku przesłuchiwanego (bardzo małe dziecko, niepełnoletni, dzieci i młodzież z zaburzeniami zachowania oraz opóźnieniami i zaburzeniami w rozwoju psychofizycznym),
– charakteru, w jakim występuje przesłuchiwany (nieletni sprawca czynu karalnego czy małoletni świadek).

II. Psychologiczno-prawne aspekty i zasady przesłuchania

Słuchacze poznają m.in. różnice w czynności przesłuchania:

a) bardzo małych dzieci (nieczytających i niepiszących),
b) dzieci i młodzieży o sprzężonych zaburzeniach rozwoju psychoruchowego,
c) osób bardzo silnie skrzywdzonych (incydentalnie lub długoterminowo),
d) w obecności osób trzecich (np. rodzica, adwokata, kuratora, prokuratora).

III. Fazy przesłuchania

Podczas zajęć są omówione następujące fazy przesłuchania (nieletniego sprawcy czynu karalnego i małoletniego świadka):

A. Faza poprzedzająca przesłuchanie

Słuchacze zostaną poinformowani o potrzebie:

1) zapoznania biegłego ze sprawą (łącznie z pisemnym uzyskaniem zgody od prokuratora na umożliwienie psychologowi wglądu w akta),
2) ustalenia zasad współdziałania policjanta i biegłego w czasie przesłuchania,
3) umożliwienia biegłemu zebrania informacji o przesłuchiwanym (w formie wywiadu anamnestycznego z rodzicem, rozmowy kierowanej z nieletnim/małoletnim czy wywiadu z opiekunem z danej placówki, jeśli dziecko nie przebywa w domu rodzinnym).

B. Faza wstępna

Słuchaczom jest zwracana uwaga m.in. na potrzebę dobrego rozeznania, czy przesłuchiwany wie, w jakim charakterze przystępuje do przesłuchania, czy właściwie zrozumiał pouczenia. Słuchacze są informowani o skutecznych sposobach nawiązywania prawidłowych relacji z przesłuchiwanym, a także formach swobodnej rozmowy w fazie wstępnego kontaktu.

C. Faza zasadnicza

1) słuchacze poznają sposoby zobowiązywania przesłuchiwanego do składania spontanicznych zeznań (przykładowo: *jeśli już wiesz, w jakiej sprawie zostałeś/łaś zaproszony/a, to powiedz – co wiesz w tej sprawie?*);
2) uświadomiona jest im rola tzw. podfazy pytań (ze szczególnym zwróceniem uwagi na wystrzeganie się tzw. pytań sugerujących);
3) słuchaczom zwraca się uwagę, że tzw. podfaza końcowa jest często niewłaściwie przeprowadzana bądź wręcz pomijana; staramy się tu uwypuklać słuchaczom takie czynności, jak:
   – zapytanie przesłuchiwanego, czy chciałby jeszcze coś dodać – co jego zdaniem – jest ważne w danej sprawie, a o co nie był dotychczas pytany,
   – zapoznanie przesłuchiwanego z protokółem (czyta sam albo jest mu czytany); oczywiście zaznaczamy, że jeśli przesłuchanie dziecka ma być prowadzone przez sąd w trybie art. 185a i 185b kpk, nie należy odczytywać dziecku protokołu przesłuchania oraz odbierać podpisu pod protokołem),
   – dokonanie poprawek i uzupełnień, a także podpisanie wypełnionego protokółu jako zgodnego z tym co świadek mówił,
   – podziękowanie przesłuchiwanemu i pożegnanie z nim.

IV. Rodzaje dokumentowania przesłuchania

Słuchacze zostają zapoznani z rodzajami dokumentowania przesłuchania:

1) pisemny protokół z przesłuchania – jako podstawowy środek utrwalania zeznań przesłuchiwanego (z podkreśleniem, że mają to być dosłowne wypowiedzi przesłuchiwanego oraz zaznaczone szczególne tzw. reakcje pozawerbalne, np. płacz, unikanie kontaktu wzrokowego, długotrwałe milczenie, ironiczne uśmiechy czy obsceniczne gesty),
2) inne formy dokumentowania przesłuchania (w sytuacjach szczególnych):
   – tzw. przesłuchanie na dyktafon (np. w przypadku wyraźnie zauważanych w rozmowie wstępnej zaburzeń osobowości lub zaburzeń zdrowia psychicznego),
   – pisemny opis zdarzeń oraz pisemna odpowiedź na zadawane pytania (np. w przypadku poważnej wady wymowy, bardzo silnej nerwicy zaburzającej mowę),
   – przesłuchanie z użyciem różnych pomocy (np. lalek anatomicznych czy misiów – w przypadku dzieci silnie skrzywdzonych, z cechami mutyzmu wybiórczego),
   – psychorysunku (np. w przypadku małych dzieci lub dzieci mało spontanicznych w wypowiedziach).

V. Rodzaje i struktura opinii psychologicznych dotyczących osób składających zeznania

Słuchaczom są przedstawiane i omawiane przykładowe (5–8) opinie psychologiczne dotyczące osób składających zeznania z udziałem psychologa (m.in. małoletnich świadków, małoletnich ofiar różnego rodzaju przemocy, nieletnich sprawców czynów karalnych). Ponadto omawiane są kryteria oceny tych opinii, po to, aby słuchacz potrafił ocenić, czy biegły wywiązał się z zadania określonego w postanowieniu, a także ocenić rachunek biegłego za wykonane czynności (zgodnie z tzw. kartą pracy biegłego).

VI. Literatura

Proponujemy słuchaczom literaturę z zakresu psychologicznych prawidłowości rozwojowych dzieci i młodzieży oraz popularnonaukową, związaną z tematem zajęć, tj. z psychologią zeznań.

Część warsztatowa (praktyczna)

Są to praktyczne ćwiczenia z odgrywaniem określonych ról przez słuchaczy. W ramach tych warsztatów słuchacze powinni posiąść umiejętność właściwego nawiązywania kontaktu z przesłuchiwanym, nauczyć się poprawnie sporządzać proto-

koły z przesłuchań, praktycznie poznać role biegłego i przesłuchującego we wszystkich typach i fazach przesłuchania, m.in.:
– przesłuchania bardzo małego dziecka (4–5-letniego w obecności rodzica i bez niego),
– przesłuchania 10-letniego chłopca, któremu ukradziono rower,
– przesłuchania nieletniego, który wraz z innymi kolegami okradał domki na działkach,
– przesłuchania nieletniego upośledzonego umysłowo,
– przesłuchania z użyciem dyktafonu.

Ćwiczenia warsztatowe są prowadzone za zgodą słuchaczy, którzy dobrowolnie zgłaszają się do poszczególnych ćwiczeń. Przebieg warsztatów jest nagrywany na dyktafon po to, aby pod koniec zajęć omówić istotne aspekty tych ćwiczeń. Słuchacze na początku są informowani, że każdorazowo po zajęciach warsztatowych nagrania te będą kasowane.
Od 11 kwietnia 2007 r. powyższy program jest realizowany w wymiarze 8 godzin dydaktycznych (wcześniej był realizowany w znacznie „okrojonej formie" – w wymiarze 5 godzin dydaktycznych).

Zanim jednak przejdziemy do podzielenia się naszymi spostrzeżeniami z już dwudziestoletniego doświadczenia w realizacji tych zajęć specjalistycznych przez kadrę dydaktyczną Zakładu Służby Prewencyjnej Centrum Szkolenia Policji w Legionowie, pozwolimy sobie zabrać głos na temat problemów dzieci w związku z toczącymi się sprawami sądowymi, w których mogą one uczestniczyć (być przesłuchiwane) w trzech rolach: 1) jako świadek jakiegoś zdarzenia, 2) jako osoba pokrzywdzona – ofiara pewnych zdarzeń, 3) jako nieletni sprawca czynu karalnego. Będzie to głos głównie z pozycji biegłego sądowego z zakresu psychologii.

Dzieci przed sądem[1]

W przypadku rażących zaniedbań opiekuńczo-wychowawczych – zgodnie z Kodeksem rodzinnym i opiekuńczym – interweniuje sąd. Jednak problemy dziecka są często rozstrzygane przez sądy, bez jego bezpośredniej obecności na rozprawach. Tak dzieje się w przypadku niektórych spraw opiekuńczych (np. adopcyjnych, o ograniczenie czy pozbawienie praw rodzicielskich), w przypadku spraw alimentacyjnych, a także w przypadku spraw rozwodowych (na których rozstrzyga się również, z kim dziecko będzie mieszkać po rozwodzie rodziców, oraz ustala się formy kontaktów z dzieckiem tego rodzica, z którym dziecko nie będzie mieszkać).
W wielu sprawach opiekuńczych i rozwodowych, a także niekiedy i w sprawach karnych (np. o znęcanie się nad rodziną) sądy, przed wydaniem wyroku, zasięgają opinii specjalistów – biegłych sądowych (pedagogów, psychologów, lekarzy) odnośnie do problemów rodziny i dziecka. Z zasady sądy zwracają się o takie opinie do opiniodawczych zespołów sądowych specjalistów (nazywanych do niedawna rodzinnymi ośrodkami diagnostyczno-konsultacyjnymi). Bywa, że zwracają się też do innych specjalistycznych placówek (Instytutu Ekspertyz Sądowych czy do różnego typu placówek specjalistycznych: poradni zdrowia psychicznego, poradni psychologiczno-pedagogicznych, pogotowi opiekuńczych, domów dziecka). Sąd może też skorzystać z opinii tzw. biegłego sądowego z listy prezesa sądu okręgowego. Biegli sądowi, we wszystkich tego typu sprawach, przy sporządzaniu swoich opinii są zobowiązani kierować się dobrem małoletnich dzieci. Dość często sądy i prokuratury zwracają się o pomoc do Policji. W przypadku, gdy interesu dziecka nie mogą bronić rodzice (bo np. są czasowo niezdolni, przebywają w szpitalu lub mają odebraną władzę rodzicielską), dobra małoletniego broni jego prawny opiekun lub ustanowiony przez sąd kurator zawodowy.

Małoletni świadek w sprawie

Prawo w zasadzie nie określa granicy wieku, poniżej której małoletni nie mogą składać zeznań i tylko w sytuacjach wyjątkowych są przesłuchiwani w sądzie w charakterze świadka. W tym charakterze występują głównie tylko wtedy, gdy byli jedynymi uczestnikami (świadkami) rozpatrywanych przez sąd zdarzeń. Sąd może uznać za konieczne przesłuchanie małoletniego, gdy był on np. jedynym świadkiem zdarzenia (wypadku) ze skutkiem śmiertelnym. Innym przykładem powoływania dziecka na świadka są tragedie rodzinne rozgrywające się w „czterech ścianach" domu rodzinnego. W sprawach karnych o znęcanie się moralne i fizyczne nad rodziną dzieci jako świadków zgłaszają często sami pokrzywdzeni (zazwyczaj matki), gdy nie mają innych świadków.
Rodzice (opiekunowie) nie mają prawa zakazać dziecku występowania w charakterze świadka. Składania zeznań może odmówić natomiast samo dziecko, jeżeli w procesie stronami są jego rodzice, rodzeństwo, dziadkowie czy inne osoby bliskie. Małoletni ma też prawo powiedzieć: „Nie odpowiem na to pytanie". Może się tak zachować, jeżeli jego zeznania mogłyby poniżać lub narażać na odpowiedzialność karną jego samego lub jego najbliższych.

> Małoletni świadek, jeśli ma skończone trzynaście lat, może być powołany na świadka we wszystkich sprawach – zarówno cywilnych, jak i karnych, a jego zeznania mają taką samą wartość dowodową jak zeznania osób dorosłych, mimo że małoletni (tj. do 17. roku życia) nie składają przysięgi. Są tylko pouczani o obowiązku mówienia prawdy. Małoletni do lat trzynastu nie ponoszą odpowiedzialności karnej za złożenie fałszywych zeznań. Ci małoletni, którzy są świadkami po ukończeniu 13. roku życia, ale przed ukończeniem 17., odpowiadają za fałszywe zeznania według procedury dla nieletnich.

W większości spraw wystąpienie małoletniego przed sądem i składanie zeznań w charakterze świadka jest poprzedzone ich złożeniem na etapie postępowania dowodowego przygotowawczego, prowadzonego przez organy ścigania (Policję i prokuraturę). W przypadku, gdy przesłuchiwany jest małoletni, przy jego przesłuchaniu powinien uczestniczyć biegły sądowy z zakresu psychologii. Zadaniem biegłego psychologa jest ocena zeznań małoletniego świadka: czy jego zeznania są psychologicznie prawdopodobne czy też nieprawdopodobne?

W tzw. sprawach o znęcanie się nad rodziną udział biegłego psychologa (a nie rodzica) w przesłuchaniu ważny jest również z innego powodu. W przypadku, gdy np. małoletni został wskazany jako świadek przez jednego z rodziców, w celu złożenia zeznań przeciwko komukolwiek z rodziny, to może on – jako osoba najbliższa – skorzystać z przysługującego mu prawa odmowy zeznań. W obecności rodzica proces decyzyjny małoletniego może być zaburzony, a obecność i zachowanie pokrzywdzonego rodzica – silnie sugestywne.
Udział w przesłuchaniu (składaniu zeznań) prowadzonym przez organy ścigania (Policję i prokuraturę), a zwłaszcza w rozprawach sądowych, stanowi dla małoletnich zawsze silne przeżycie. Szczególnie traumatyczne jest składanie zeznań obciążających najbliższych. Rolą biegłego psychologa jest więc również takie kontrolowanie przebiegu postępowania dowodowego, aby małoletni czuł się bezpieczny. Jednocześnie w sytuacji zaobserwowania – zgodnie ze swymi kompetencjami zawodowymi – sytuacji silnie urazowych, obowiązkiem biegłego jest ochrona małoletniego, np. przez zgłaszanie przesłuchującemu organowi stosownych wniosków dotyczących stanu psychicznego świadka (np.: zarządzenie kilkuminutowej przerwy, celem „wyrównania emocji" dziecka).

Małoletni jako ofiary przemocy

Dziecięce dramaty nie zawsze trafiają na wokandę sądową. Omawiamy więc te tragedie, które przez nas – dorosłych – bywają niezauważalne, niekiedy bagatelizowane czy wręcz niezrozumiałe, a które potrafią pozostawić trwały uraz psychiczny, nawet na całe życie.
Warte podkreślenia jest to, że każde dziecko na swój sposób przeżywa trudne dla niego sytuacje. Różne są również formy przeżywania tych nieszczęść na poszczególnych etapach (stadiach) rozwojowych dziecka. Może ono manifestować swe przeżycia płaczem, buntem, agresją, ucieczką czy przeciwnie – biernym podporządkowaniem się, a nawet psychiczną izolacją.
Każde dziecko przeżywa dramat, gdy ma czegoś rażąco mało, a także, gdy ma czegoś w nadmiarze. Dzieci cierpią nie tylko w przypadku braku rodzicielskiej miłości, ale także, gdy rodzice są zbyt ambitni i otaczają dziecko przesadną troskliwością i nadopiekuńczością. Podajemy przykład dziewczynki, która znienawidziła matkę za to, że zawsze rano, przed wyjściem do przedszkola, zmuszała ją do wypicia duszkiem ciepłego, bardzo słodkiego kakao z kożuchami. W czasie przesłuchania opowiadała, że gdy była już trochę starsza, wypijała kakao i szła do łazienki, aby je zwymiotować. Z kolei pewien młodzieniec mówił, że dla matki nie robi niczego spontanicznie. Robi tylko to, o co go ona poprosi, i musi jeszcze koniecznie określić, jak ma to być zrobione. Wspomina, że gdy był jeszcze bardzo mały, chciał w Dniu Matki pozmywać naczynia i stłukł jeden talerz. Matka go za to zbiła. Do dziś ma do niej żal, że cenniejszy był dla niej talerz niż jego chęć pomocy.
Dzieci przeżywają dramaty, gdy są publicznie upokarzane lub wyśmiewane, zwłaszcza jeśli jest to czynione przez tzw. osoby znaczące z najbliższego otoczenia. A jakże często zdarza się nam publiczne zwracanie się do dziecka w następujący sposób: „ty mazgaju", „maminsynku", „fajtłapo", „głąbie", „cymbale" itp. Epitetowanie i drwiny dorosłych dotkliwie przeżywają zwłaszcza dzieci wkraczające w okres dojrzewania. Taki – niby nic nieznaczący dla rodziców żart – może być dla dziecka powodem do poważnych rozterek.
Dramatem dla dorastających dzieci jest też brutalne wkraczanie w ich intymny świat. Jedna z przesłuchiwanych dziewcząt uciekła z domu i nawet wkroczyła na drogę przestępstwa (zresztą dość przypadkowo) – po tym, jak matka znalazła jej pamiętnik i publicznie, przy gościach, zaczęła go odczytywać, śmiejąc się przy tym niemal z każdego zdania.

Z wieloletniego doświadczenia wiemy, że nawet tak drastyczne przykłady znęcania się (maltretowania) psychicznego nie zawsze trafiają na wokandę sądową. Chociaż powszechnie uważa się, że wszelkie zachowania dorosłych, które odbierają dziecku poczucie godności i bezpieczeństwa, które narażają je na lęk, rozpacz czy samotność, a także doprowadzają do emocjonalnego odtrącenia lub izolowania, skutkują nerwicą, depresją czy myślami, a nawet próbami samobójczymi – są społecznie naganne i powinny być karane.

Poza maltretowaniem psychicznym może występować (niekiedy równolegle) maltretowanie fizyczne. Najczęstszym przejawem znęcania się fizycznego nad dzieckiem jest bicie. Wśród metod oddziaływania wychowawczego bicie dzieci stanowi powszechnie akceptowaną metodę oddziaływania wychowawczego. Biją nie tylko ojcowie, ale i matki, choć podobno ojcowie częściej i dotkliwiej. Do szpitali trafia rocznie wiele dzieci maltretowanych; kilkanaście z tego powodu umiera.
Proponujemy słuchaczom sięgnięcie do literatury pomagającej rozpoznać zespół dziecka maltretowanego. Uczulamy przy tym, że w przypadkach fizycznego maltretowania dziecka opis zdarzeń prezentowanych przez agresora z zasady nie jest jasny, a wyjaśnienia nieadekwatne.
Specyficznym rodzajem znęcania się nad dzieckiem jest przemoc seksualna, która występuje w dwóch formach: jako zachowania pedofilne oraz kazirodcze. Problemy te omawiamy jednak w znacznym skrócie, w stosunku do tego, jak często się zdarzają. Podkreślamy jednak, że dzieci seksualnie wykorzystywane z powodu wstydu i poczucia winy, w czasie przesłuchań skrzętnie ukrywają tę tajemnicę. Czasami milczą i wyrażają „pozorną zgodę" na bycie wykorzystywanym seksualnie przez dłuższy czas, bo są szantażowane lub psychicznie i fizycznie zastraszane, a także w przeróżny sposób „kupowane".
Jednocześnie uświadamiamy słuchaczom, że nie tylko dzieci ukrywają fakt seksualnego wykorzystywania. Znane są przypadki, kiedy to matki – w obawie przed rozbiciem rodziny lub utratą domowej stabilizacji – przez długi czas nie ujawniały faktu współżycia męża (konkubenta) z córką.
Należy też wiedzieć, że ofiarami seksualnych nadużyć są nie tylko dziewczynki, ale również i chłopcy, którzy bywają napastowani przez homoseksualnych pedofilów.
Dziecko może być skrzywdzone incydentalnie (np. w parku czy w windzie). Z przypadkami krzywdzenia długotrwałego, ciągłego mamy najczęściej do czynienia w rodzinie lub najbliższym środowisku małoletniego.

Zważywszy na fakt, że skutki krzywdzenia są zawsze szkodliwe dla dziecka, powinniśmy natychmiast reagować i przychodzić takiemu dziecku z bezpośrednią, konkretną pomocą. I poświęcić więcej miejsca tej problematyce na szkoleniach policjantów.

Dziecko jako ofiara niewydolnej wychowawczo rodziny

Wielu rodziców, którzy już dawno przestali być w stosunku do siebie kochającymi partnerami, decyduje się mieszkać pod jednym dachem ze względu na dziecko. Niekiedy wręcz mówią, że poświęcają się dla dobra dziecka. Ale czy taka sytuacja jest rzeczywiście dla niego korzystna?[2]

Dziecko widzi, iż rodzice, mimo że mieszkają razem, nie są wobec siebie tacy sami jak dawniej, z zasady nie są uśmiechnięci, pogodni, zadowoleni z życia. Atmosfera stale wzmożonego napięcia, naburmuszenia towarzyszy niemal wszystkim ich poczynaniom i udziela się członkom rodziny – również dzieciom. Brak porozumienia i zgodności jest dominującą cechą tych rodzin.

Niekiedy rodzice „wmontowują" dziecko w tzw. konflikt lojalności, kiedy to dziecko ma się wypowiedzieć, czyim jest sojusznikiem w małżeńskiej walce. Gdy walka się zaostrza, a strony usztywniają swoje stanowiska, dochodzi bardzo często do agresji i przemocy (zarówno fizycznej, jak i psychicznej) w stosunku do współmałżonka, no i oczywiście – dziecka. I tak – mężowie z zemsty za porzucenie najczęściej straszą swe byłe żony porwaniem lub prawnym odebraniem jej dziecka. Matki zaś – w konsekwencji małżeńskiego konfliktu – bardzo często utrudniają lub wręcz uniemożliwiają ojcom kontakt z dziećmi. Ci z kolei przestają płacić alimenty na dzieci.

Często, właśnie w sytuacji przedrozwodowej, rodzice najbardziej „uaktywniają" Policję, składając stosowne doniesienia i wnioskując o przesłuchanie nawet małoletnich dzieci.

Przed wydziałami cywilnymi sądów okręgowych oraz wydziałami rodzinnymi i nieletnich sądów rejonowych, sprawy rozwodowe i opiekuńcze (przede wszystkim o kontakty z dziećmi) niekiedy toczą się latami. Zwykle po rozwodzie rodziców dziecko zamieszkuje razem z matką. Już z tego powodu ogranicza to kontakt z ojcem, lecz tylko niewielki procent dzieci nie chce z nim kontaktów. Z zasady spotkań z ojcem unikają dzieci, których rodzice byli silnie i długo skłóceni, jeszcze w okresie trwania związku małżeńskiego, a dziecko stanowiło przedmiot walki przedrozwodowej (niekiedy i porozwodowej). We wszystkich innych sytuacjach dzieci bardzo pragną kontaktów z ojcem, wspólnych wyjazdów, spacerów, prezentów. A utrudnienie, czy wręcz odmowa przez matkę kontaktu dziecka z ojcem przybiera różne formy. Najczęściej bywa to kategoryczne stwierdzenie typu: *twój ojciec jest nieodpowiedzialny, nie mogę więc puścić cię z nim na wczasy, bo jeszcze cię tam zdemoralizuje*. Na ograniczanie kontaktów ma również wpływ różnego rodzaju „obrzydzanie" ojca: *Widzisz, jaki z twego ojca potwór, na tę...* (i tu seria epitetów) *to wydaje pieniądze, a tobie nie chce kupić komputera*. Zdarza się też odmowa „manipulacyjna", czyli zawsze, gdy tata ma się spotkać z dzieckiem, ono ma zaplanowane przez matkę atrakcyjne zajęcie. Wtedy dziecko niby odmawia i nie chce iść z ojcem: *Dziś z tobą nie mogę się spotkać, bo idę z mamą kupić sobie nowe dżinsy*.

Zdaniem autorów, wielu rodziców podejmuje zbyt pochopnie decyzję o rozwodzie, kierując się niekiedy wyłącznie silnymi emocjami. O rozejściu się małżonków decyduje czasem jedno zdarzenie, a nawet jedno niepotrzebne słowo. Słowo, po którym zabrakło innego – „przepraszam".

> Z udziału przy przesłuchaniu małoletnich, a także na podstawie znanych nam badań i mediacji możemy stwierdzić, że wielu rozwodzących się rodziców charakteryzuje ogromny upór, zawziętość, stanowczość osądów i decyzji, brak tolerancji w ocenie postępowania współmałżonka, brak gotowości wybaczania. Obserwuje się też niemal całkowity brak umiejętności (zdolności) do proszenia o wybaczenie. Takie postawy utrudniają, a niekiedy wręcz uniemożliwiają, rzeczową rodzinną dyskusję czy mediację – doprowadzające do pojednania.

W życiu jednak może się zdarzyć i tak, że decyzja o rozwodzie jest jedynym i najsłuszniejszym rozwiązaniem. Dla dobra dziecka, dla jego właściwego rozwoju należy wtedy przełamać swój egoizm i uczyć je poszanowania oraz poprawnych relacji z drugim rodzicem. Ale uczyć należy nie poprzez słowa, lecz dając przykład, utrzymując na bieżąco właściwe kontakty we wszystkich sprawach związanych z rozwojem, wychowaniem i planowaniem przyszłości wspólnego dziecka. Tylko wtedy – i tak silnie traumatyczna dla dziecka decyzja rodziców o rozstaniu – uczyni w psychice dziecka znacznie mniejszy chaos. Trzeba bowiem pamiętać, iż mimo że przestaje się być mężem i żoną, nigdy nie przestaje się być w stosunku do swych dzieci ojcem i matką. Zwaśnionych rodziców nasi słuchacze powinni informować o dezyderacie nr 4 Komisji Do Spraw Petycji w sprawie podjęcia działań przeciwdziałających alienacji rodzicielskiej z 12.05.2016 r. (pismo Ministerstwa Sprawiedliwości z 15.07.2016 r. nr DSRIN-II-071-1/16).

Wielu rodzinom w sytuacji kryzysowej jest potrzebna specjalistyczna pomoc: lekarska, psychologiczno-pedagogiczna, prawna itp. Jej celem powinno być szybkie reagowanie w przypadku zauważenia pierwszych objawów kryzysu rodziny. Fachowa pomoc zapewne zapobiegłaby degradacji rodzin i wiele dzieci nie trafiałoby do domów dziecka czy innych placówek opieki całkowitej. W domach dziecka przebywa zaledwie niewielki procent naturalnych sierot. Pozostałe dzieci znajdują się tam na mocy postanowień sądów rodzinnych i nieletnich, gdyż pochodzą z rodzin zdemoralizowanych, niewydolnych wychowawczo czy też nieumiejących sobie poradzić z problemami materialnymi.

Apelujemy więc w części wykładowej do słuchaczy uczestniczących w szkoleniach w Centrum Szkolenia Policji w Legionowie o więcej serdeczności i zrozumienia dla problemów ludzi w kryzysie, potrzebujących pomocy, a zwłaszcza psychopedagogicznych problemów dzieci. Podanie w porę ręki może pomóc wyjść z dołka niemocy i osamotnienia. Wiele dzieci mogłoby powrócić z placówek do swoich „wyleczonych rodzin" dzięki takiej pomocy. Dzieci wychowywane w instytucjach są

pozbawione rodzicielskiej miłości oraz możliwości uczenia się podstawowych ról społecznych – ojca i matki. Tego nie można nauczyć się poza rodziną. To trzeba przeżyć i można jedynie odwzorowywać.

Dobro dziecka[3]

Ze słuchaczami omawiamy termin „dobro dziecka", gdyż mimo że jest dość powszechnie używany, to niejednoznacznie rozumiany. Jego znaczenia można jedynie się domyślać z użycia w określonych kontekstach. Częściej natomiast definiuje się pojęcie „dobra", które traktuje się jako wartość ocenianą dodatnio, stanowiącą przedmiot i cel ludzkich dążeń oraz pragnień. Dobrem określa się również to, co jest oceniane jako pomyślne, pożyteczne, wartościowe, a także łagodność i życzliwość. Za dobro uważa się też wszelkie środki, wartości potrzebne dla rozwoju człowieka i sprzyjające temu rozwojowi. Ponadto dobro to interes, pomyślność, szczęście, pożytek, korzyść.

Dobro dziecka dość często występuje również w przepisach prawa. Jednakże i w tym przypadku nie jest ono jednolicie rozumiane. Ustawodawca – mimo że w polskim Kodeksie rodzinnym i opiekuńczym często się do niego odwołuje – też nie podaje definicji. Ogranicza się jedynie do określenia jego znaczenia poprzez użycie w określonych kontekstach. Dla pracowników sądownictwa (sędziów, biegłych sądowych, kuratorów zawodowych) termin „dobro dziecka" zazwyczaj oznacza: zespół warunków mających zapewnić dziecku prawidłowy rozwój fizyczny i duchowy, bądź sam rozwój tego dziecka, a więc pewne cechy dziecka.

W polskiej doktrynie prawnej podejmowano – nieliczne wprawdzie – próby wyjaśniania znaczenia terminu „dobro dziecka". Najczęściej podkreśla się, że jest to zespół wartości (duchowych i materialnych) niezbędnych do zapewnienia dziecku prawidłowego rozwoju fizycznego i duchowego.
Rzeczową definicję podaje W. Stojanowska, która stwierdza, że „termin «dobro dziecka» w rozumieniu przepisów prawa rodzinnego oznacza kompleks wartości o charakterze niematerialnym i materialnym niezbędnych do zapewnienia prawidłowego rozwoju fizycznego i duchowego dziecka oraz należytego przygotowania go do pracy odpowiednio do jego uzdolnień, przy czym wartości te są zdeterminowane przez wiele różnorodnych czynników, których struktura zależy od treści stosowanej normy prawnej i konkretnej, aktualnie istniejącej sytuacji dziecka, zakładając zbieżność tak pojętego «dobra dziecka» z interesem społecznym"[4].

Nieletni przed sądem

Z historii i literatury wiemy, że młodzi zawsze się buntowali przeciwko zastanym formom i normom życia dorosłych, a rodzice narzekali na brak porozumienia z dorastającymi dziećmi i młodzieżą. Nigdy jednak to skłócenie pokoleń nie przybierało tak dużych rozmiarów i nie przejawiało się w tak drastycznych, a nawet wyrafinowanych formach protestu, jakie obserwuje się w ostatnim dwudziestoleciu. Wcześniej dzieci i młodzież z tzw. problemami wychowawczymi lub przystosowawczymi (nazywane często nieprzystosowanymi społecznie) były z zasady lękliwe, niezaradne, szukające zastępczo zaspokojenia potrzeb w skrajnie oralnych reakcjach (obgryzanie paznokci, obżarstwo itp.) oraz w agresji pośredniej (jak np. kłamstwo, kradzieże, podpalenia). Natomiast wśród dzieci i młodzieży przełomu XX i XXI wieku dominują zaburzenia zachowania związane z agresją i destrukcją, którym towarzyszą egoizm i bezwzględność. Nie mając wpojonego szacunku do prawa, młodzi łamią je bez oporów, czyniąc krzywdę innym, gdyż nie mają wyrobionego poczucia empatii, tj. umiejętności wczuwania się w emocje innych i rozumienia ich przeżyć. Nabywanie bowiem wzorców zachowania w znacznej mierze dzieje się za sprawą naśladownictwa. Potwierdzają to liczne wywiady prowadzone przez biegłych sądowych, z których wynika, że znaczny procent agresywnych dzieci pochodzi z rodzin, w których agresja była sposobem rozwiązywania problemów. Dotyczy to nie tylko kar fizycznych stosowanych wobec dzieci, ale także stosunków panujących między rodzicami. Dezintegracja rodziny, jej niewłaściwie pojmowane i realizowane normy, wartości i standardy moralne mają bardzo istotny wpływ na powstawanie u dzieci przejawów niedostosowania i demoralizacji (wielu przestępców wychowywało się w rodzinach rozbitych – bez ojca).
Z praktyki psychologicznej opiniowania sądowego w sprawach nieletnich wiadomo, że wśród form tzw. nieprzystosowania społecznego dzieci i młodzieży najczęściej spotykamy się z używaniem przez dzieci nieprzyzwoitego lub nawet wręcz wulgarnego słownictwa, z kłamstwem, bójkami między rówieśnikami, zbieraniem haraczu od młodszych i słabszych kolegów, kradzieżami, wagarami szkolnymi i ucieczkami z domu, piciem alkoholu i zażywaniem środków odurzających (leków lub narkotyków), udziałem w negatywnych grupach nieformalnych (bandach, gangach, grupach subkulturowych).
Dolna granica odpowiedzialności prawnej to 13. rok życia. Z chwilą ukończenia 17. roku życia następuje odpowiedzialność karna za wszelkie przestępstwa, na tych samych zasadach, według których traktowani są dorośli (tj. na podstawie obowiązujących przepisów prawa karnego). W stosunku do nieletnich nadal funkcjonuje przedwojenna reguła kodeksowa – zgodnie z nią sąd może orzec wobec nieletniego co najwyżej zakład poprawczy, w którym nieletni może przebywać najdalej do ukończenia dwudziestu jeden lat. Nawet wtedy, gdy skazano go za popełnienie najcięższej zbrodni – wychodzi na wolność. Z dniem 1 września 1998 r. próg pełnej odpowiedzialności karnej za najcięższe przestępstwa (zabójstwa, gwałty, rozboje) został obniżony z szesnastu do piętnastu lat. Pozwala to sądom na orzekanie kary więzienia w stosunku do nieletnich już w tym wieku. W przypadku orzeczenia przez sąd kary więzienia nieletni powinien ją odbywać w specjalnym oddziale dla młodocianych, a nie z dorosłymi recydywistami.
Dla jasności powyższych informacji pragniemy przypomnieć, że w świetle obowiązującej ustawy z 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz. U. z 2016 r. poz. 1654, z późn. zm.) pojęcie „nieletni" jest stosowane wobec trzech kategorii młodzieży: 1) w zakresie zapobiegania i zwalczania demoralizacji – wobec jednostek, które nie ukończyły osiemnastu lat; 2) w postępowaniu w sprawach

o czyny karalne – w stosunku do młodzieży, która dopuściła się takiego czynu po ukończeniu trzynastu lat, ale nie ukończyła jeszcze siedemnastu lat; 3) wszystkie osoby do dwudziestu jeden lat, wobec których jest zalecane wykonywanie środków wychowawczych lub poprawczych – nie dłużej jednak niż do 21. roku życia.

Ze słuchaczami szkoleń w CSP podejmowaliśmy też warsztatowe analizy problemów dziecka krzywdzonego oraz omawialiśmy kwestie związane z jego przesłuchiwaniem.

Były to:

- dylematy etyczne psychologa sądowego (m.in. konieczność łączenia pracy psychologa sądowego z innymi funkcjami jak np. mediatora, terapeuty, doradcy, świadka);
- etapy pracy biegłego (od analizy akt do obrony opinii w sądzie): 1) umiejętność analizy akt sprawy oraz rozmowa na temat sprawy i treści postanowienia powołującego biegłego psychologa – z przesłuchującym (policjantem lub prokuratorem); 2) udział psychologa sądowego w planowaniu przesłuchania (m.in. zebranie wywiadu anamnestycznego przed przesłuchaniem) i rozmowy kierowanej z małoletnim; 3) techniki przesłuchania; 4) formułowanie opinii i wniosków; 5) stawiennictwo w sądzie;
- budowanie kontaktu z dzieckiem ofiarą/świadkiem przestępstwa (zasady, warunki, sposób prowadzenia przesłuchania; fazy przesłuchania; dobór technik przesłuchania);
- opiniowanie w sprawach dotyczących oceny zeznań małoletnich świadków, trudności w opiniowaniu; wymogi formalne opinii; zasady formułowania opinii i wniosków opracowanych na podstawie udziału w przesłuchaniu; ocena sprawności intelektualnej i sprawności procesów poznawczych zgodnie z art. 192 § 2 kpk, czyli psychologiczna ocena zeznań dzieci ofiar/świadków przestępstw; pomocna rola Policji w opiniowaniu w sprawach rozwodowych i opiekuńczych z udziałem dzieci;
- charakterystyka zjawiska krzywdzenia dzieci; czynniki ryzyka krzywdzenia dzieci w rodzinie i poza nią; obraz psychologiczny rodziny przemocowej/kazirodczej;
- charakterystyka sprawców przemocy;
- obraz psychologiczny dziecka ofiary/świadka przestępstwa;
- charakterystyka funkcjonowania dziecka w sferze poznawczej, emocjonalnej, społecznej i seksualnej w kolejnych fazach rozwojowych, w kontekście udziału w procedurach prawnych;
- specyfika diagnozy sądowo-psychologicznej w przypadkach podejrzenia wykorzystania seksualnego dziecka.

Co wynika z dyskusji ze słuchaczami szkoleń w CSP?

W dyskusjach coraz częściej jest podnoszony problem, że młode pokolenie Polaków przełomu XX i XXI wieku coraz częściej wchodzi w kolizję z prawem. Przyczyny tego stanu rzeczy są złożone, a trzeba ich szukać przede wszystkim w patologii lub kryzysach w rodzinie, w niepowodzeniach szkolnych, w braku właściwego zagospodarowania wolnego czasu i wreszcie – w działalności różnego rodzaju negatywnych grup nieformalnych. Nasze doświadczenia – potwierdzane spostrzeżeniami słuchaczy tych szkoleń – wskazują, że zachowaniom o charakterze przestępczym, zwłaszcza dzieci poniżej 13. roku życia, z zasady towarzyszy dezintegracja rodziny. Dyskutujemy, dlaczego tak się dzieje, bo przecież rodziny patologiczne nie dominują w naszym społeczeństwie, a ponadto dość liczna grupa dzieci i młodzieży z tzw. porządnych, dobrych domów popełnia czyny karalne. Wielu słuchaczy – policjantów służby prewencyjnej o specjalności do spraw nieletnich wskazuje, że jeśli chłopak czy dziewczyna popełniają czyn karalny, to z zasady w takim domu są zaburzone relacje między członkami rodziny. Określenie „dobry dom" jest w tych przypadkach fasadą. Czasami te niby porządne, dobrze wykształcone i zamożne rodziny kryją problemy znacznie głębsze, trudniejsze w zdiagnozowaniu, niż w rodzinach patologicznych. Dzieci w takich domach żyją jakby w stanie remisji, wyciszenia. Wystarczy przypadkowy (np. na dyskotece) kontakt z alkoholem, narkotykami czy grupą przestępczą i zaczynają się problemy. Takim powodem może być również nawet incydentalne, ale silnie traumatyczne dla dorastającego dziecka zachowanie rodzica.

> Według naszych doświadczeń wśród głównych grzechów popełnianych przez rodziców wobec swoich dzieci wymieniane są przede wszystkim te, które wynikają z zaburzonych relacji rodzic – dziecko. Mimo niekiedy trudnego życia ze względów ekonomicznych, to większość tych dzieci nie odczuwa głodu i chłodu (w znaczeniu fizycznym). Brak jest im jednak oparcia w kimś bliskim, ciepła rodzinnego, są smutne i czują się osamotnione. U schyłku XX wieku zanikł bowiem model rodzica-przyjaciela. Przecież rodzice powinni być pierwszymi i bardzo ważnymi nauczycielami dobrego zachowania.

Jakże często są złymi nauczycielami. Bo – jak wykazują nasze analizy z dyskusji ze słuchaczami szkoleń w CSP – znaczny procent dzieci agresywnych pochodzi z rodzin, w których siła i agresja są sposobem rozwiązywania problemów. Z takich rodzin dzieci wynoszą przekonanie, że albo samemu trzeba być silnym, albo trzeba się podporządkować silniejszemu. I z taką postawą wchodzą w życie, gdzie stykając się np. z rówieśniczymi grupami przestępczymi, nie potrafią powiedzieć „nie". Wykonują narzucone im polecenia, bowiem nikt nie nauczył ich dyskutowania, przedstawiania i bronienia własnych racji. Nie nauczyli ich tego ani zapracowani i zmęczeni rodzice, ani szkoła, w której muszą się podporządkowywać dyrektywnemu stylowi wychowania. I wreszcie trzeba wymienić bardzo silne znamię naszych czasów: podwójną moralność – na użytek prywatny i publiczny (*czy musiałaś być taka szczera u babci?* – pyta podirytowany ojciec, po tym jak córka się skarżyła, że zbyt często przychodzi do domu pijany). Takie zachowania dorosłych powodują wielki chaos w emocjach młodzieży, wyzwalający ogromne napięcie psychiczne, którego najprostszym rozładowaniem jest schowanie się za tzw. maską (którą jakże trudno potem zdjąć).

Naszym założeniem jest zwrócić uczestniczącym w szkoleniu słuchaczom uwagę na fakt, że w wielu rodzinach ciągle jeszcze wychowuje się według zasady – mama/tata wie lepiej. Dziecko rośnie, a my wciąż wiemy lepiej. Im wrażliwsze dziecko, tym mocniej odbiera to jako lekceważenie jego osoby. Stres wywołany brakiem porozumienia z rodzicami objawia się różnie: wzmożoną pobudliwością psychoruchową u małego dziecka,

niepokojem, zaburzeniami snu, nocnym moczeniem, rozdrażnieniem, nieradzeniem sobie w trudnych sytuacjach, nieufnością w stosunku do dorosłych. Dziecko coraz bardziej zamyka się w sobie, a gdy jest starsze, izoluje się całkowicie, np. przebywając tylko w swoim pokoju. Gdy konflikt jest szczególnie ostry – jak sami mówią – „wystawiają pazury" i w formie buntu uciekają z domu, sięgają po alkohol i narkotyki, rozpoczynają przedwczesne i przypadkowe współżycie seksualne.

W sytuacji konfliktu w rodzinie zwykle panuje albo przeraźliwy wrzask i terror, albo długotrwałe milczenie. Dlatego w przypadku tzw. cichych dni w rodzinie proponujemy młodym napisanie listu do rodzica. A oto fragmenty takich niektórych listów:

Tato! Moim największym problemem jest to, że w ogóle nie można się z Tobą dogadać. Uważasz, że ja nie mam żadnych praw. Podejmujesz jakieś głupie decyzje, a gdy pytam – dlaczego? – słyszę tylko: bo tak ma być, bo ja tak chcę, bo ja ci każę.

Mamo! Nie wiesz, czy nie chcesz wiedzieć, że ja dorastam. Mam już własny pogląd na świat i już nie mogę pozwolić, żeby ktoś decydował za mnie w moich najbardziej osobistych sprawach. Starasz się decydować o moich uczuciach, m.in. o moich uczuciach do ojca. Czy dlatego, że rozwiedliście się, a ja mieszkam z Tobą, to mam Go nienawidzić?

Niekiedy dzięki takim listom udawało się z młodymi złapać wspólny język. Wówczas często się okazywało, że wewnętrznie są oni całkiem inni niż okazywali na zewnątrz. Z ich wypowiedzi wynikało niekiedy wprost błaganie: *zrozumcie mnie, proszę, kochajcie mnie, ale mądrze, ja chcę was oboje kochać, mimo że sobie, a pośrednio i mnie, wyrządzacie ogromną krzywdę*.

Naszym zdaniem bardzo trudne są te sprawy rodzinne, w których małoletni jest równocześnie świadkiem i pokrzywdzonym. Charakterystyczne wówczas jest nie tylko to, że dziecko jest wówczas ofiarą i świadkiem, ale też, że jest zwykle jedynym świadkiem. Bardzo często występuje również obarczanie siebie winą za zaistniałe zdarzenia, a niekiedy oskarżany rodzic potęguje i wzmacnia to poczucie winy.

Zawsze w takich sytuacjach (czyli w sytuacjach ostrego konfliktu rodzinnego) tłumaczymy słuchaczom, że nieumiejętne postępowanie kogokolwiek (policjanta, prokuratora, sędziego, adwokata czy biegłego) przy przesłuchaniu małoletniego może doprowadzić do bezpowrotnego zerwania więzi uczuciowych między dzieckiem-ofiarą i rodzicem-sprawcą. A w życiu, zarówno jednego, jak i drugiego, zachowana w miarę poprawna więź uczuciowa może mieć bardzo istotne znaczenie. Dlatego – według nas – obowiązkiem moralnym wobec słuchaczy, jest pokazanie roli policjanta i biegłego psychologa w tym, aby dziecko, nawet przy bardzo krytycznym stosunku do czynu czy zachowania rodzica, podjęło próbę dotarcia do przyczyn takiego postępowania i zachowało do niego w miarę pozytywny stosunek emocjonalny.

W sprawach karnych (np. o znęcanie się małżonka nad małżonkiem), czyli jeśli oskarżonym jest bardzo bliska osoba z rodziny, dziecku przysługuje prawo odmowy składania zeznań. Należy mu wyjaśnić, co w praktyce oznacza prawo do odmowy składania zeznań. Bardzo często formalne pouczenie jest z reguły dla dziecka niewystarczające. Dziecko wezwane na przesłuchanie, czuje się zobowiązane do zeznań, a często jest do tego wręcz zmuszane przez rodzica oskarżającego. Bywa też i tak, że dzieci są okłamywane przez rodzica, który zgłosił je jako świadka (czasem nieświadomie, częściej jednak świadomie). Na przykład mówi się im: „tylko raz o tym opowiesz i nikt się o tym nie dowie". Gdy jako biegły psycholog prowadzę rozmowy poprzedzające przesłuchanie, dzieci pytają: „A czy tatuś będzie czytał to, co ja teraz powiem?". Należy uświadomić dziecku, że jest to jego prawo, że nie ma obowiązku włączać się w sprawy rodziców i że nikt, nawet sąd, nie może mu tego nakazać. Psychologiczne doświadczenie podpowiada mi, iż dla dobra dziecka jest najkorzystniej, gdy korzysta ono z prawa odmowy składania zeznań obciążających rodzica.

Omawiając problematykę przesłuchania dziecka, zwracamy też uwagę słuchaczy na jeszcze jeden – naszym zdaniem – istotny psychologicznie szczegół. Otóż uważamy, że obowiązkiem przesłuchujących – w przypadku bardzo małych dzieci, a nawet starszych, ale o słabszych możliwościach intelektualnych – jest upewnić się, czy dziecko dobrze zrozumiało pouczenie: *masz obowiązek mówienia prawdy*. Dzieci z zasady odpowiadają, że wiedzą, co to znaczy mówić prawdę, i od razu dodają, że znaczy to, żeby nie kłamać. Wydawałoby się, iż taka odpowiedź powinna nam wystarczyć. Ja jednak zawsze proponuję słuchaczom, by dodali: *oczywiście, mówić prawdę, to nie kłamać, ale chcemy, abyś mówił tylko to, co sam widziałeś, sam słyszałeś, sam czułeś, a nie to, co ktoś ci mówił, żebyś mówił*. I w tym miejscu opowiadam słuchaczom o przesłuchaniu, w którym 6-letni chłopiec relacjonował, jak to tatuś pobił mamusię i popchnął ją tak mocno, że złamała się drewniana poręcz schodów, a mamusia spadła ze schodów i połamała sobie nogę i rękę. Opowieść była bardzo szczegółowa, a całe zdarzenie nadzwyczaj realistycznie opisywane, nawet z dopowiedzeniem, że do tej pory są ślady po reperowanej poręczy. Zasadniczy problem tego przesłuchania polegał na tym, że z analizy zaświadczeń lekarskich znajdujących się w aktach wynikało, iż mamusia tego chłopca rzeczywiście spadła ze schodów w czasie małżeńskiej awantury, ale dziecko miało wówczas niespełna półtora roku. Znało zatem szczegóły zdarzenia z wielokrotnych opowieści różnych członków rodziny, nieżyczliwych tatusiowi.

Dyskusyjny niekiedy staje się problem udziału biegłego psychologa przy przesłuchaniach dzieci w konfliktowych sprawach rodzinnych (rozwodowych, opiekuńczych czy karnych). Biegły – jak już wcześniej stwierdzaliśmy – ma zawsze reprezentować interes (dobro) dziecka. Powoduje to, że psycholog jest „wmontowywany" jak gdyby w odgrywanie dwóch ról zawodowych: bezstronnego biegłego sadowego oraz doradcy, któremu w zaufaniu przedstawia się pewne fakty, niekiedy nawet z jawnie oczekiwaną nadzieją, że uzyska się konkretną poradę, a nawet pomoc. Współpracujący z biegłymi (policjanci, prokuratorzy i sędziowie) muszą mieć świadomość, że pogodzenie tych dwóch ról jest bardzo trudne, a niekiedy nawet dwuznaczne z etycznego punktu widzenia. Bo oto na przykład, w rozpadającej się rodzinie często się zdarza, że interes dziecka jest zbieżny z interesem jednego z rodziców. Stąd biegły jakby automatycznie może się znaleźć po stronie tego rodzica. Stawia to niekiedy biegłego w trudnej sytuacji wobec organu prowadzącego dane postępowanie.

Uwagi końcowe

Pod koniec każdych zajęć jest ustalone, że – jako prowadzący te zajęcia – podejmuję zawsze ze słuchaczami podsumowującą dyskusję. Zdarzają się różne uwagi – zarówno dotyczące programu szkolenia, jak i nie najlepszych warunków pracy w macierzystych jednostkach.

Jeśli chodzi o program, to w zakresie treści przedstawianych przez nas w ramach przedmiotu: „Przesłuchanie z udziałem biegłego sądowego z zakresu psychologii" oczekiwanie jest tak duże, że w zasadzie 8–10 godzin wykładowych i 6–8 godzin warsztatowych nie byłoby za dużo.

W dyskusji zawsze podkreślamy potrzebę partnerskiej współpracy policjanta z biegłym psychologiem. Powinna być ona oparta na zasadach wzajemnej życzliwości, z uwzględnieniem kompetencji każdej z osób zaangażowanych w przesłuchanie. Interakcje policjanta i biegłego powinny być wspomagające, a nie rywalizujące. A zatem w szczególnych sytuacjach (np. przesłuchanie bardzo małego dziecka, dziecka silnie skrzywdzonego, upośledzonego umysłowo czy z zaburzeniami zachowania) biegły psycholog powinien być wprost proszony przez policjanta o bardziej aktywne uczestnictwo w przesłuchaniu. Nie powinno to być tylko uczestnictwo w przesłuchaniu, lecz przede wszystkim aktywny udział.

Słuchacze w czasie szkolenia oczekują na znacznie więcej przykładów „dobrych" postanowień o powołaniu biegłego psychologa. Stwierdzają, że prawie każda sprawa – jaka była im w czasie szkolenia przedstawiana – jest inna, a postanowienia są prawie zawsze takie same. A przecież od treści postanowienia zależą zarówno czynności biegłego, jak i pytania kierowane do dziecka przez przesłuchującego w danej sprawie.

Istnieje – naszym zdaniem – potrzeba analizy wielu protokołów z przesłuchań, gdyż ich zapisy budzą rozbieżne poglądy, nie tylko u słuchaczy (ale także niekiedy u ich przełożonych). Takim kontrowersyjnym problemem jest dosłowny zapis wypowiedzi osoby przesłuchiwanej, jak i odnotowania w protokóle szczególnych zachowań podczas przesłuchania (takich jak np. płacz, długie uporczywe milczenie czy różnego rodzaju reakcje psychosomatyczne – zawstydzenie, zaczerwienienie twarzy, spocenie się, drżenie rąk lub całego ciała). To prawda, że już coraz częściej w ostatnich latach odchodzi się od zapisu papierowego przy przesłuchaniu dzieci oraz osób upośledzonych umysłowo i chorych psychicznie (bez względu na wiek) i stosuje się przesłuchanie tych osób z zapisem foniczno-wizyjnym (co nie zwalnia przesłuchującego i protokolanta z wykonania choćby skrótowego zapisu przebiegu przesłuchania).

Słuchacze podkreślają pilną potrzebę przygotowania specjalnych pomieszczeń w jednostkach Policji do przesłuchania nieletnich i małoletnich. Wskazują, że taki pokój powstał w Centrum Szkolenia Policji w Legionowie i stanowił wzór do naśladowania.

Ponadto słuchacze zwracają uwagę na konieczność organizowania przez CSP stałych szkoleń doskonalących, o coraz szerszym zakresie, jak również szkoleń przywarsztatowych bezpośrednio w jednostkach Policji (np. udział w przesłuchaniu w charakterze protokolanta w obecności bardziej doświadczonego policjanta).

Padają nawet propozycje, żeby część szkoleń organizować wspólnie z przełożonymi, tak aby nie było drastycznych rozbieżności między wiedzą przekazywaną podczas szkoleń w CSP i wdrażaniem jej w zawodowe życie w jednostkach, a tym, czego wymagają od nich przełożeni.

Dwudziestoletnie doświadczenie kadry dydaktycznej Centrum Szkolenia Policji w Legionowie w realizacji kursów z zakresu problematyki nieletnich pozwalają stwierdzić, iż policjanci zajmujący się tą problematyką powinni posiadać szeroką wiedzę psychologiczno-pedagogiczną, a także prawniczą oraz odpowiednie doświadczenie życiowe i zawodowe (powinno być preferowane nawet posiadanie wyższego wykształcenia z zakresu pedagogiki, psychologii lub prawa). Nie bez znaczenia są też odpowiednie predyspozycje do pracy z dziećmi i młodzieżą. Istotnym elementem wpływającym na rozwój zawodowy absolwentów tych kursów specjalistycznych jest właściwe wykorzystanie ich profesjonalnego przygotowania zawodowego, a także obdarzenie ich zaufaniem w zakresie zdobytych kompetencji.

[1] Problemy te szerzej omawiane są w artykule W. Brejnaka, *Dziecko w sądzie – przesłuchanie z udziałem biegłego sądowego z zakresu psychologii*, w: „Kwartalnik Policyjny" 2007, nr 1, s. 14–21 oraz w rozdziale: W. Brejnaka – *Dziecko i jego problemy przed sądem*, w: *Dziecko niepełnosprawne, jego rodzina i edukacja*, red. K.J. Zabłocki, Wydawnictwo Akademickie „Żak", Warszawa 1999, s. 75–100.

[2] Problem ten jest szerzej omówiony w rozdziale W. Brejnaka, *Dziecko a rozwód rodziców*, w: *Pedagogika specjalna – kontynuacja tradycji dla przyszłości*, pod red. K.J. Zabłockiego i D. Gorajewskiej, Wydawnictwo Akademii Pedagogiki Specjalnej, Warszawa 2004, s. 97–110.

[3] Szerzej w: *Encyklopedia Pedagogiczna,* pod red. W. Pomykało, hasło: „Dobro dziecka" (opr. Wojciech Brejnak – s. 109–110), Fundacja Innowacja, Warszawa 1997.

[4] Szerzej w: W. Stojanowska, *Rozwód a dobro dziecka*, Wydawnictwo Prawnicze, Warszawa, 1979, s. 27–36.

Summary

Examination with the participation of an expert witness in psychology as an element of the in-service program for police officers

The article entitled *Examination with the participation of the expert witness in psychology as an element of the in-service program for police officers* is a reply to the interest in issues in question reported by trainees of a specialist course for police officers in matters of prevention of corruption and juvenile delinquency as well as actions taken in favour for minors. Admittedly this subject matter was widely discussed in the first issue of the *Police Quarterly* in 2007, but in relation to the straitened accessibility to that number of our publication, the present issues were discussed again in this edition of the *Police Quarterly*. The majority of the article is based on the experience of Wojciech Brejnak, an expert witness in psychology and constitutes a valuable source of knowledge, with which all police officers dealing with juvenile problems can familiarize and use in their professional careers.

Tłumaczenie: Renata Cedro

Środki dydaktyczne

mł. insp. Marek Hańczuk, podkom. Adam Przybylik
Zakład Kynologii Policyjnej CSP

Składnikiem racjonalnie przygotowanego i realizowanego procesu nauczania i uczenia się są środki kształcenia, nazywane również środkami dydaktycznymi. Są to przedmioty materialne, które dostarczają uczniom określonych bodźców wzrokowych, słuchowych, dotykowych i innych, dzięki czemu usprawniają proces kształcenia, a przez to wpływają korzystnie na jego przebieg i efekty[1].
Tak rozumiane środki dydaktyczne spełniają następujące funkcje:

- po pierwsze, **ułatwiają uczniom poznawanie rzeczy, zjawisk, wydarzeń i procesów** w sposób bezpośredni, to znaczy w drodze faktycznego kontaktu z nimi, lub pośredni, tj. poprzez kontakt z tymi rzeczami, zjawiskami, wydarzeniami i procesami za pomocą reprezentujących je zastępników;
- po drugie, **pobudzają i intensyfikują procesy myślowe u uczniów**, ułatwiając im analizowanie, syntetyzowanie i porównywanie poznawanych obiektów oraz formułowanie na tej podstawie stosownych uogólnień;
- po trzecie, **zastępują lub dopełniają czynności dydaktyczne nauczyciela** tam, gdzie jest to konieczne lub wskazane ze względów metodycznych, np. jako projekcje nagranych na taśmę wideo wykładów, filmów oświatowych, tekstów programowanych[2].

Przeprowadzane badania wykazują, że wykorzystywanie środków dydaktycznych w procesie nauczania, a do takich niewątpliwie zaliczymy prezentacje multimedialne oraz filmy dydaktyczne, znacząco ułatwia prowadzącemu zajęcia dotarcie do słuchacza, co powoduje, że zakres przyswojonej wiedzy przez odbiorców jest większy, a zatem osiągnięcie celu dydaktycznego jest bardziej prawdopodobne.

ZASADY OPRACOWYWANIA PREZENTACJI MULTIMEDIALNYCH

Prezentację multimedialną stosuje się najczęściej w celach informacyjnych, promocyjnych lub reklamowych. Powinna zawierać najważniejsze informacje na określony temat, przekazywać je w sposób ciekawy i atrakcyjny. Jest to możliwe dzięki wykorzystywanym w prezentacji mediom, takim jak: tekst, grafika, dźwięk czy film.
Niewłaściwa prezentacja multimedialna może zepsuć cały odbiór tego, co chcemy powiedzieć/przekazać. Migające literki pojawiające się znikąd, źle dobrana kolorystyka, np. żółty tekst na zielonym tle, niskiej jakości ilustracje, wykresy z nieczytelnymi legendami to często spotykane przykłady nieumiejętnie opracowanych prezentacji multimedialnych.
Pojęcie multimedia, a zwłaszcza przymiotnik: multimedialny, to słowa określające wytwory bardzo różnego typu, ponieważ multi znaczy wiele, a media to inaczej środki przekazu, multimedia i multimedialny oznaczałyby po prostu wielość środków przekazu użytych w jednym utworze. W pewnym sensie już średniowieczny ilustrowany kodeks jest multimedialny, posługuje się bowiem sztukami plastycznymi w wyrażaniu treści. Współcześnie chodzi jednak o takie zastosowanie różnych mediów, które będzie nie tylko prostą ilustracją tekstu, lecz stworzy nową, synergiczną w budowaniu znaczeń, jakość. W ten sposób multimedialność ma swoje konsekwencje zarówno na poziomie struktury przekazu, jak i na poziomie percepcji, wymuszając specyficzne sposoby odbioru […][3].
Przygotowując prezentację, pamiętaj o tym, że słuchacz jest najważniejszy. Określ, kto będzie stanowił audytorium. Zawsze uwzględniaj poziom wiedzy odbiorców na prezentowany temat[4]. Twoją myślą przewodnią powinno być: „Jak to powiedzieć, aby słuchacze dobrze to zrozumieli?".
Prezentacja multimedialna, która nie została dobrze przygotowana, nie tylko nie spełni swej funkcji, ale wręcz może zniweczyć Twoje plany: słuchacze mało zrozumieją z Twojego wystąpienia, nic nie zapamiętają, zmęczą się i w rezultacie będą mieli poczucie straconego czasu.
Zanim przystąpisz do komputerowego tworzenia prezentacji, sprecyzuj temat i cele, jakie zamierzasz osiągnąć. Następnie opracuj na papierze projekt prezentacji, czyli scenariusz, który powinien zawierać nie tylko liczbę slajdów (czas trwania prezentacji – możliwie krótki), ale także ich zawartość: zdjęcia, tekst, rysunki, tabele, wykresy, muzykę, filmy itp. Wszystkie te materiały przygotuj wcześniej i zgromadź w postaci plików w jednym folderze.

Zawartość informacyjną wybranego slajdu (treść) skonstruuj w taki sposób, aby odbiorca mógł w ciągu 15 sekund dokonać jej wstępnego oglądu, pozwalającego mu na zorientowanie się w jego zawartości. Bombardując słuchacza potokiem informacji, wywołasz sytuację, w której przestaje on słuchać i zapamiętywać wiadomości, a całą uwagę skupi na prezentowanym obrazie.
Tekst prezentowany na pojedynczym slajdzie powinien mieścić się w najwyżej 6 linijkach, a maksymalna liczba obiektów graficznych (zdjęć, rysunków, tabel, wykresów itp.) to 6. Treść slajdu nie może być dla Ciebie ściągawką, z której korzystasz, ponieważ nie miałeś czasu nauczyć się treści swojego wystąpienia.
Czcionka użyta w tekście powinna być o dość dużych rozmiarach, np. 24 pkt (min. 18 pkt), co pomaga w percepcji. Powinna być ona prosta i pozbawiona jakichkolwiek ozdobników. Do najczęściej używanych i uznawanych za najbardziej czytelne należą popularne czcionki Arial oraz Times New Roman. Zachowaj umiar w stosowaniu różnych czcionek w jednym tekście. Najlepiej trzymać się jednego lub dwóch rodzajów czcionki. Daje to wrażenie porządku. Unikaj także częstego stosowania pogrubiania, pochylania oraz podkreślania tekstu.
W sytuacji, gdy nastąpi potrzeba zawarcia na jednym slajdzie większej ilości tekstu (np. definicji), należy pamiętać o podziale tekstu na akapity. Zaleca się także wyrównanie tekstu do lewej strony lub ewentualnie obustronne wyjustowanie. Powinno się natomiast unikać wyrównywania tekstu do prawej strony, gdyż taki slajd jest mniej czytelny i wymaga od słuchacza poświęcenia większej uwagi do zlokalizowania nowego miejsca, w którym rozpoczyna się kolejna linijka tekstu.
Pamiętaj również o kierunku przekazywanej informacji (od lewej do prawej strony). Najbliżej lewej strony slajdu umieść te elementy, które są ważniejsze. Jeśli większe znaczenie ma np. ilustracja niż tekst, powinna ona znaleźć się po lewej stronie, natomiast tekst po prawej stronie slajdu.
Należy mocno ograniczyć używanie wielkich liter. Stosuj je tylko w wyjątkowych przypadkach. Trudno się je odczytuje. Nie chcesz przecież zmęczyć odbiorcy przed końcem prezentacji. Czcionka pochyła spowalnia czytanie, należy ją stosować tylko do wyróżnień informacji.
Często w prezentacjach wykorzystywane są tzw. cliparty. To takie ilustracje w „magazynie" programu PowerPoint. Stosując je, weź pod uwagę, czy widzowie już ich wielokrotnie nie widzieli i czy nie lepiej byłoby zilustrować slajd własnymi zdjęciami, np. kolegów „w akcji" niż tymi powszechnie znanymi rysunkami.
Nie przesadzaj zarówno z kolorem tła, jak i czcionki. Wybierz je i stosuj konsekwentnie w całej prezentacji. Kolory czcionki powinny kontrastować z tłem, np. żółta czcionka na niebieskim tle. Najbezpieczniejsze są czarne litery na jasnym (białym) tle – rzutniki w różny sposób odtwarzają barwy przekazane z komputera i może się okazać, że to, co było czytelne na ekranie komputera, będzie kompletnie nieczytelne na ekranie ściennym. Używanie koloru powinno mieć na celu wzmocnienie przekazu, a nie tylko dekorację – nadmiar barw może bowiem rozpraszać i drażnić. Chcąc podkreślić to, co ważne, „zaalarmować" odbiorcę i skupić jego uwagę, stosuj ciepłe kolory, takie jak: czerwony, pomarańczowy, żółty, natomiast dla przedstawienia informacji o charakterze neutralnym powinieneś wybierać kolory zimne: czarny, granatowy, szary, zielony. W celu uzyskania większej wyrazistości treści slajdu możesz też posłużyć się inwersją kolorów liter i tła, zamiast „czarno na białym" przedstawić informacje „biało na czarnym".
Oprócz treści innym ważnym elementem prezentacji multimedialnej, który ją wzbogaca i zwiększa jej atrakcyjność, przez co pomaga odbiorcom zrozumieć prezentowane informacje, jest zawartość graficzna, tj. rysunki, wykresy, tabele. Powinna ona być możliwie prosta i łatwa w zrozumieniu (zawierać tylko najważniejsze informacje). Ważne jest, aby rozmiar poszczególnych elementów był stosunkowo duży, a obraz wysokiej jakości, co zapewni lepszą czytelność.
Dobrym zwyczajem jest, aby ostatni slajd (bądź pierwszy) zawierał informacje o autorze.
Ważne składniki prezentacji to: slajd tytułowy, slajd z planem wystąpienia, slajd podsumowujący, bibliografia, slajd zamykający – podziękowanie słuchaczom. Odbiorcy najlepiej zapamiętują pierwsze i ostatnie słowa.
Trzeba jednak zaznaczyć, że prezentacja jest tylko instrumentem wspomagającym i ma być uzupełnieniem Twojego przekazu werbalnego. Weź pod uwagę, że słuchacze będą zadawać pytania. Wykorzystanie nawet najlepiej opracowanej prezentacji przez osobę, która nie jest przygotowana do prowadzenia zajęć z danego tematu, może się skończyć porażką.

PAMIĘTAJ, że prezentacja to element zajęć, a nie skrypt dla słuchacza lub ściągawka dla prowadzącego zajęcia.

FILM W PROCESIE DYDAKTYCZNYM

Wśród wielu środków dydaktycznych, w tym materiałów audiowizualnych, niewątpliwie szczególną funkcję pełni film, który daje nieograniczone możliwości. Znacznie ułatwia osiągnięcie celu dydaktycznego. W wielu przypadkach może stanowić najcenniejszą pomoc dla prowadzącego zajęcia, bowiem najlepiej angażuje percepcję uczącego się. Film jest jedynym środkiem dydaktycznym, za pomocą którego możemy zaprezentować praktyczne sytuacje i umiejętności – z poziomu sali dydaktycznej.
Przemyślane wykorzystanie filmu dydaktycznego w procesie nauczania, z zachowaniem zasad dydaktyki, daje prowadzącemu zajęcia realną szansę wprowadzenia jakościowych zmian w realizacji celów kształcenia. Niewątpliwie, aby sprostać wymaganiom współczesnego nauczania, należy uwzględniać i wykorzystywać nowoczesne środki dydaktyczne. Nadanie informacjom zróżnicowanej i ciekawej formy sprzyja rozbudzaniu zainteresowań słuchaczy danym tematem. Wprowadzenie atrakcyjnego środka dydaktycznego, jakim jest film, działającego na wzrok, powoduje już wzrost zapamiętywania informacji z 10% do 20%. Stworzenie uczniom możliwości dyskusji i rozmowy zwiększa ilość zapamiętanych informacji do 40%. Natomiast umożliwienie uczniom uczenia się poprzez działanie powoduje, że zapamiętują 90% tego, co robią, gdyż w czasie wykonywania czynności angażują całych siebie: umysł, wolę, emocje i zmysły[5].
Film dydaktyczny, nazywany też oświatowym, to film, którego cechą jest cel poznawczy. Uwzględnia on szkolne programy nauczania i jest adresowany do wychowawców, nauczycieli oraz uczniów – jako pomoc w nauczaniu różnych przedmiotów w różnych typach szkół i na różnych poziomach nauczania (od przedszkola po wyższe uczelnie). Stanowi fragment lekcji, wykładu[6]. Jest zawsze cząstką składową jakiegoś określonego procesu dydaktycznego, nigdy nie występuje jako samodzielna całość.
Za filmy dydaktyczne uważa się także filmy popularnonaukowe, upowszechniające i popularyzujące wiedzę wśród szerokich krę-

gów odbiorców, a nawet każdy rodzaj filmu (fabularny, dokumentalny czy badawczy), który zostanie celowo i metodycznie wykorzystany w procesie dydaktycznym[7].
Oglądanie filmu to śledzenie ruchomych obrazów, z których każdy pojawia się na krótko na ekranie i już nie powraca. Stanowi to doskonałą okazję do rozwijania spostrzegawczości. Film ma właściwości „hipnotyczne", jest czymś, co urzeka i fascynuje odbiorcę. Zajęcia z filmem, jak pisze Adam Suchoński[8], pobudzają aktywność uczniów. Kształtują ich wyobraźnię i postawy, a dzięki wykorzystaniu możliwości techniki filmowej ilustrują i znacznie wzbogacają poznawane przez nich treści. Z tych powodów, a także ze względu na fakt, że film dydaktyczny daje prosty, szybki i zrozumiały przekaz, powinien on być doceniany i wykorzystywany w dydaktyce policyjnej.

TWORZENIE FILMU DYDAKTYCZNEGO

Tworząc materiał filmowy, który ma stanowić odpowiednią pomoc dydaktyczną, dopasuj jego treść oraz formę do poziomu wiedzy, dojrzałości odbiorców, programu szkolenia, celu nauczania i tempa przekazu.
Pierwszym krokiem po określeniu tematu filmu oraz rozpoznaniu, jakie zadania dydaktyczne powinien on spełniać, jest zastanowienie się nad budową scenariusza i scenopisu filmowego. Scenariusz to forma literacka przyszłego filmu, będąca podstawą jego realizacji. Zawiera szkic fabuły, charakterystykę postaci, opis miejsc, dialogi oraz uwagi odautorskie i reżyserskie. Może być przeróbką istniejącego dzieła literackiego (scenariusz adaptowany) lub stanowić oryginalną twórczość autora (scenariusz oryginalny)[9]. Na podstawie scenariusza jest opracowywany scenopis – szczegółowy opis każdego z ujęć filmu.
Planowanie włączenia filmu do przewidzianego programem przekazu określonej porcji informacji zaczyna się już w czasie opracowywania scenariusza filmu. Autor scenariusza musi widzieć miejsce projektowanego filmu w całym systemie pomocy dydaktycznych stosowanych w szkole. Zamysł scenarzysty wprowadzają w życie wszyscy realizatorzy filmu. Rolę, jaką twórcy przewidzieli dla filmu w procesie dydaktycznym, musi znać również użytkownik filmu, czyli Ty – nauczyciel policyjny. Należy zatem dążyć do opracowania wskazówek metodycznych do każdego filmu dydaktycznego.

Przewodnik metodyczny do filmu dydaktycznego powinien uwzględniać:

- ogólne wprowadzenie do tematu i uzasadnienie wyboru filmu jako środka przekazu informacji o danym materiale nauczania;
- krótki opis treści filmu;
- wskazówki metodyczne dotyczące wykorzystania filmu w procesie dydaktycznym;
- zakończenie i wskazówki bibliograficzne[10].

Film jest materiałem wyrażanym poprzez dwie płaszczyzny – obraz i dźwięk, przy czym obraz stanowi główny składnik, natomiast dźwięk – jego uzupełnienie. Na obraz składają się: ujęcia, sceny i sekwencje. Należy dodać, że ujęcia tworzą scenę, a sceny – sekwencję. Tworząc ujęcia, należy znać pojęcie planu filmowego oraz perspektywy. W skrócie – plan filmowy to odległość do głównego obiektu filmowego. Zmiana planu następuje, gdy filmowany obiekt oddala się lub przybliża oraz gdy następuje ruch kamery. Po nakręceniu materiału filmowego odbywa się montaż, inaczej mówiąc – sklejanie poszczególnych ujęć nagranych w różnych planach. Montaż w dużej mierze decyduje o wartości filmu. Dzisiejsze techniki dają duże możliwości. Dynamiczne przejścia, pokazanie kilku ujęć w jednym obrazie to tzw. efekty, które pomagają konstruować współczesny film dydaktyczny.
Dźwięk, jak wspomniano wcześniej, ma stanowić uzupełnienie obrazu. Nie znaczy to jednak, że tworząc film, nie należy przykładać wagi do tego elementu. Pamiętaj, że za pomocą dźwięku ułatwisz oglądającym odbiór. Dźwiękiem tworzymy nastrój, zaznaczamy najważniejsze sceny, aktywizujemy odbiorców. Dialogi w filmie dydaktycznym występują sporadycznie, szczególną funkcję pełni jednak komentarz, który często jest jego nieodzownym składnikiem. Nie może być zbyt długi, ma zwięźle informować i zwracać uwagę na najważniejsze rzeczy. Czasem lektor mówi o tym, czego nie widać lub czego nie może pokazać obraz. Pytania zadawane przez lektora mają natomiast stymulować oglądającego do myślenia lub sprowokować do zapamiętania pewnych informacji.

WYKORZYSTANIE FILMU JAKO ŚRODKA DYDAKTYCZNEGO

Warunkiem, aby film dydaktyczny mógł zostać dobrze przez Ciebie wykorzystany, jest wcześniejsze obejrzenie go. Przed prezentacją filmu przygotuj odbiorcę poprzez wprowadzenie w tematykę oraz ukierunkowanie uwagi na wybrane zagadnienia. Każde wykorzystanie filmu dydaktycznego wymaga pewnych uzupełnień ze strony prowadzącego. Obraz powinien być opatrzony Twoim wstępnym komentarzem słownym (opowiadaniem, zadawaniem pytań przypominających zagadnienia już znane słuchaczom, a powiązane z tematyką filmu). Wszystkie materiały powinny być starannie wyselekcjonowane przez Ciebie pod kątem przydatności do osiągnięcia celów nauczania. Czasem celowe jest, aby całość projekcji została podzielona na krótkie, kilkuminutowe fragmenty odpowiadające problemom omawianym w trakcie zajęć. Słuchacze powinni otrzymać np. zestaw pytań, na które można znaleźć odpowiedź w trakcie obserwacji materiału filmowego. Po prezentacji każdego fragmentu filmu konieczne go omów i podsumuj.
Prowadzący zajęcia zazwyczaj decyduje, jak i kiedy wykorzystać materiał dydaktyczny w postaci filmu. Możliwości jest wiele. Film może być uzupełnieniem tradycyjnej lekcji, bardzo często służy do utrwalenia omówionego materiału nauczania. Bywa wykorzystywany do pokazania odpowiednich sytuacji problemowych. Filmem możesz posłużyć się także do przeprowadzenia weryfikacji pomysłów rozwiązania. W tym przypadku wyświetl odpowiednio dobrany fragment filmu po zakończeniu pracy słuchaczy nad zadanym problemem. Pokazane na filmie rozwiązanie powinno wywołać dyskusję nad przydatnością sposobów zastosowanych przez słuchaczy i tych, które przedstawiono w filmie. Powinieneś podsu-

mować tę konfrontację, podkreślając zalety i wady sposobów rozwiązania proponowanych przez słuchaczy[11].
W procesie dydaktycznym realizowanym przez szkoły policyjne film często pokazuje błędy popełniane w codziennej służbie. W tym wypadku ma pobudzić do myślenia oraz sprowokować do zadawania pytań i wyciągnięcia odpowiednich wniosków.

SPRAWDŹ SAM SIEBIE

Co decyduje o właściwym odbiorze przez słuchacza środka dydaktycznego – prezentacji multimedialnej?

O właściwym odbiorze przez słuchacza prezentacji multimedialnej decyduje kilka elementów. Jednym z nich jest odpowiednia wizualizacja prezentacji, czyli zawartego w slajdach uporządkowanego tekstu, dostosowanego do poziomu słuchaczy. Drugim jest właściwie opracowana szata graficzna wzbogacona o zdjęcia, rysunki i wykresy. Trzecim – odpowiedni przekaz werbalny osoby przeprowadzającej prezentację, uzupełniający slajdy i wyjaśniający zagadnienia powiązane, na które zabrakło miejsca w samej prezentacji.

Wymień elementy odpowiedniej konstrukcji slajdu w prezentacji multimedialnej.

Do elementów odpowiedniej konstrukcji slajdu w prezentacji multimedialnej należą:
- *właściwie dobrana kolorystyka (tło i napisy),*
- *przemyślany układ slajdu,*
- *ilość tekstu nieprzekraczająca 6 linijek na slajd (hasła),*
- *prawidłowe używanie prostych czcionek (unikanie wykorzystywania wielu rodzajów czcionek oraz ich modyfikacji, a także stosowania wielkich liter),*
- *współgranie elementów graficznych z tekstem.*

Jakie czynniki wpływają na efektywność prezentacji multimedialnej?

Na efektywność prezentacji multimedialnej wpływają:
- *dostosowanie zakresu tematycznego prezentacji do poziomu wiedzy i umiejętności odbiorców,*
- *zapewnienie odpowiedniej konstrukcji slajdów,*
- *wiedza merytoryczna i umiejętności osoby wykorzystującej prezentację multimedialną.*

W jaki sposób trafnie przeprowadzić selekcję materiału do wykonania filmu?

Należy uwzględnić predyspozycje odbiorcy – poziom wiedzy oraz etap zaawansowania kursu. Materiał powinien zawierać najistotniejsze informacje – takie, które zostaną przyswojone i zrozumiane przez odbiorcę.

[1] C. Kupisiewicz, *Dydaktyka. Podręcznik akademicki*, Kraków 2012, s. 188.
[2] Tamże, s. 189, za: H. Glockel, *Vom Unterricht der allgemeinen Didaktik*, Bad Heilbrunn, Klinkhardt 1990, s. 39–40.
[3] R. Chymkowski, *Literatura na morzu i w sieci, czyli kim chce być czytelnik e-książek*, w: *Liternet. Literatura i Internet*, red. P. Marecki, Kraków 2005.
[4] P. Lenar, *Profesjonalna prezentacja multimedialna. Jak uniknąć 27 najczęściej popełnianych błędów*, Gliwice 2010.
[5] K. Rau, E. Ziętkiewicz, *Jak aktywizować uczniów*, Poznań 2000, s. 22.
[6] Na podstawie: http://www.akademia-kultury.edu.pl/slownik/f/251.html [dostęp: 22.10.2014 r.].
[7] W. Strykowski, *Struktura filmu naukowo-dydaktycznego*, Poznań 1973, s. 13.
[8] A. Suchoński, *Środki audiowizualne w nauczaniu i uczeniu się historii*, Warszawa 1987, s. 225.
[9] Na podstawie: http://www.plezantropia.fora.pl/b-kino-b,119/slowniczek-pojec-filmowych,4239.html [dostęp: 22.10.2014 r.].
[10] L. Siachowicz, M. Grzeszyk, *Film w procesie dydaktycznym*, „Kwartalnik Policyjny" 2013, nr 3, s. 16.
[11] L. Siachowicz, M. Grzeszyk, *Film w procesie dydaktycznym*, s. 17.

LITERATURA

Godlewski A., *Prezentacje multimedialne*, Szkoła Policji w Pile, Piła 2008.
Jacoby J., *Nowoczesne środki i materiały dydaktyczne*, WSiP, Warszawa 1980.
Jarmark S., *Film i przeźrocza w kształceniu zawodowym*, WSiP, Warszawa 1979.
Kupisiewicz C., *Dydaktyka. Podręcznik akademicki*, Impuls, Kraków 2012.
Lenar L., *Profesjonalna prezentacja multimedialna. Jak uniknąć 27 najczęściej popełnianych błędów*, Onepress, Gliwice 2010.
Marecki P., *Liternet. Literatura i Internet*, Rabid, Kraków 2005.
Okoń W., *U podstaw problemowego uczenia się*, PZWS, Warszawa 1965.
Plisiecki J., *Metodyka pracy z filmem wśród dzieci i młodzieży*, Centrum Animacji Kulturalnej, Warszawa 1993.
Puszczewicz B., *Tworzenie dydaktycznych komunikatów audiowizualnych*, Powszechna Wideoteka Edukacyjna, Warszawa 1997.
Płażewski J., *Język filmu*, WAiF, Warszawa 1961.
Rau K., Ziętkiewicz E., *Jak aktywizować uczniów*, Oficyna Wyd. G&P, Poznań 2000.
Siachowicz L., Grzeszyk M., *Film w procesie dydaktycznym*, „Kwartalnik Policyjny" 2013, nr 3.
Strykowski W., *Struktura filmu naukowo-dydaktycznego*, Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza, Poznań 1973.
Strykowski W., *Wstęp do teorii filmu dydaktycznego*, UAM, Poznań 1977.
Żurek E., *Sztuka prezentacji, czyli jak przemawiać obrazem*, Poltext, Warszawa 2003.

ZASADY PUBLIKOWANIA
w „Kwartalniku Policyjnym”

1. Redakcja przyjmuje teksty dotąd niepublikowane o charakterze zawodowym lub naukowym, dotyczące zagadnień związanych z funkcjonowaniem Policji, szeroko rozumianym bezpieczeństwem, a także praktyki policyjnej i współpracy formacji z innymi instytucjami ochrony porządku prawnego oraz z samorządem lokalnym.
2. Materiały do publikacji należy przesyłać pocztą elektroniczną na adres: kwartalnik@csp.edu.pl lub składać w sekretariacie Wydziału Wydawnictw i Poligrafii Centrum Szkolenia Policji (ul. Zegrzyńska 121, 05-119 Legionowo, tel. 22 605 33 72 lub 22 605 32 70).
3. Prace są kwalifikowane do druku przez zespół redakcyjny czasopisma. Redakcja zastrzega sobie prawo dokonywania skrótów i adiustacji tekstów oraz zmiany tytułów i śródtytułów.
4. W celu zapobiegania wszelkim przejawom nierzetelności, w tym zjawisku *ghostwriting* i *guest authorship*, redakcja wymaga ujawnienia przez autorów wkładu w powstanie publikacji.
5. Materiały są publikowane w „Kwartalniku Policyjnym” nieodpłatnie, po złożeniu przez autora pisemnego oświadczenia, zgodnie z otrzymanym od redakcji wzorem.
6. Nadesłanych materiałów do publikacji redakcja nie zwraca.
7. Wersją pierwotną (referencyjną) czasopisma jest wydanie papierowe. Ponadto poszczególne numery są również dostępne w wersji elektronicznej na stronie internetowej: www.kwartalnik.csp.edu.pl.
8. Wskazówki edytorskie dotyczące przygotowania materiału przez autorów:
   - format A4, czcionka Times New Roman, wielkość 12 punktów, interlinia 1,5 wiersza, marginesy – 2,5 cm;
   - na pierwszej stronie należy podać imię i nazwisko autora materiału, stopień (lub tytuł) naukowy (tytuł zawodowy), nazwę instytucji, w której autor jest zatrudniony, nr telefonu, adres e-mailowy;
   - do tekstu należy dołączyć streszczenie oraz tytuł pracy w języku angielskim;
   - materiał ilustracyjny powinien być dostarczony w oddzielnych plikach (rysunki lub fotografie w formacie jpg, rozdzielczość 300 dpi, minimalna wielkość 1,5 MB);
   - schematy i wykresy zamieszczone w publikacji muszą być edytowalne, tak aby można było nanieść korektę;
   - przypisy należy umieścić na dole strony lub na końcu pracy; przypisy wstawia się automatycznie i oznacza się cyframi arabskimi;
   - zgodnie z normami wydawniczymi przypis bibliograficzny powinien zawierać:
     – imię i nazwisko autora, tytuł, wydawcę, miejsce i rok wydania, numer strony:
     M. Olbrycht, J. Rutkowski, *Taktyka minersko-pirotechniczna w działaniach antyterrorystycznych*, Centrum Szkolenia Policji, Legionowo 2003, s. 35–36;
     – jeżeli dzieło jest pracą zbiorową:
     Nowy leksykon PWN, red. A. Dyczkowski, Warszawa 1998, s. 684;
     – jeżeli jest to artykuł w pracy zbiorowej:
     J. Szreniawski, *Prawo do dobrej administracji prawem podmiotowym obywatela*, w: *Dobra administracja. Teoria i praktyka*, red. J. Łukasiewicz, S. Wrzosek, Radom 2007, s. 256;
     – jeżeli jest to artykuł w czasopiśmie:
     B. Jankowska, *Odpowiedzialność karna osób prawnych*, „Państwo i Prawo” 1996, nr 7, s. 46;
     – jeżeli jest to akt prawny (należy wskazać publikator):
     Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2016 r. poz. 1782, z późn. zm.);
     – jeżeli jest to tekst opublikowany w Internecie:
     J. Kowalski, *Edukacja online*, www.gazeta.pl/forum?forumedukacyjne5645 [dostęp: 12 marca 2004 r.].

Zasady recenzowania artykułów

1. Artykuły o charakterze naukowym są recenzowane przez dwóch niezależnych recenzentów zewnętrznych, zgodnie z zasadami dotyczącymi tego rodzaju prac, w tym z Dobrymi praktykami w procedurach recenzyjnych w nauce opracowanymi przez Zespół do Spraw Etyki w Nauce pod przewodnictwem prof. dr. hab. Witolda Marciszewskiego, opublikowanymi na stronie internetowej: http://www.nauka.gov.pl/publikacje2/dobre-praktyki-w-procedurach-recenzyjnych-w-nauce.html.
2. Autorzy i recenzenci nie znają swoich tożsamości, w innych przypadkach recenzenci podpisują oświadczenie o niewystępowaniu konfliktu interesów między nimi a autorami, w tym m.in. bezpośrednich relacji osobistych, relacji podległości zawodowej, bezpośredniej współpracy.
3. Recenzja ma formę pisemną. Zawiera syntetyczną charakterystykę artykułu, część analityczną, ocenę ogólną i kończy się jednoznaczną konkluzją, tj. jest pozytywna, negatywna lub warunkowo pozytywna, jeśli recenzent wskazuje na konieczność wprowadzenia poprawek. Autorzy artykułów są zobowiązani do ustosunkowania się do uwag i uwzględnienia sugerowanych zmian.
4. Nazwiska recenzentów poszczególnych publikacji nie są ujawniane. Lista recenzentów współpracujących z czasopismem w każdym roku kalendarzowym jest publikowana w ostatnim numerze danego roku.

Fundacja Pomocy Wdowom i Sierotom po Poległych Policjantach

wspiera materialnie rodziny policjantów,
którzy stracili życie w związku ze służbą w Policji.
Udzielanie pomocy osieroconym rodzinom
jest możliwe dzięki Darczyńcom
przekazującym na rzecz Fundacji darowizny.
Dla zainteresowanych dokonaniem wpłaty
podajemy nr konta Fundacji:

PKO BP VI O/Warszawa nr

74 1020 1068 0000 1802 0059 9167

Można też wesprzeć Fundację,
deklarując w swoim zeznaniu podatkowym (**PIT**)
1% na rzecz Fundacji (**KRS 0000101309**).

CENTRUM SZKOLENIA POLICJI

05-119 Legionowo, ul. Zegrzyńska 121
www.csp.edu.pl

www.kwartalnik.csp.edu.pl