Sylwia Gwoździewicz
Wydział Administracji i Bezpieczeństwa Narodowego
Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim

PROBLEMATYKA KSZTAŁCENIA SPECJALISTÓW DO SPRAW ZWALCZANIA CYBERPRZESTĘPCZOŚCI

Problems of cybercrime specialists' education

Diagnoza problematyki cyberprzestępczości

Problematyka przestępstw komputerowych mimo swojego wzrastającego znaczenia nie cieszy się należytym zainteresowaniem polskiej doktryny. Zjawisko to w zasadzie nie doczekało się również zbyt wielu badań empirycznych. Analiza danych pochodzących z oficjalnych statystyk przestępczości ujawnionej (statystyka policyjna), których przedmiotem były przestępstwa stypizowane jako przestępstwa komputerowe i przeciwko ochronie informacji w ustawie z dnia 6 czerwca 1997 r. – Kodeks karny, okazuje się aktualnie (z różnych przyczyn) mało miarodajna[1].

Niemniej jednak dzięki większej świadomości społecznej oraz powołaniu licznych instytucji i organizacji działających w obrębie cyberbezpieczeństwa i cyberprzestępczości (np. NASK-CERT-PL) powstają coraz to nowsze raporty branżowe, dzięki którym nie sposób nie zgodzić się ze stwierdzeniem, że cyberprzestępczość należy traktować jako jedno z największych zjawisk przestępczych dzisiejszych czasów. Mając na uwadze prognozy[2], że do 2020 r. na świecie w projekty IoT[3] będzie zaangażowanych ponad 4 miliony przedsiębior-

---

1 Por. F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Wolters Kluwer, Warszawa 2016, s. 22–23.

2 Szerzej w: DLP Expert, „Data Leak Prevention" (kwartalnik) 2017, nr 4 (23), styczeń 2018, s. 9.

3 IoT – Internet rzeczy (również Internet przedmiotów, ang. Internet of Things) – koncepcja, wedle której jednoznacznie identyfikowalne przedmioty mogą pośrednio albo bezpośrednio gromadzić, przetwarzać lub wymieniać dane za pośrednictwem instalacji elektrycznej inteligentnej KNX lub sieci komputerowej. Podstawowym celem IoT jest stworzenie inteligent-

ców, innowatorów i programistów, a Komisja Europejska szacuje, że kompetencje z zakresu technologii cyfrowych będą wymagane w 90%, to należy postawić hipotezę, że cyberprzestępczość nie będzie również malała.

Zgodnie z aktualnymi szacunkami łączna wartość globalnych strat ponoszonych na skutek popełniania cyberprzestępstw już od kilku lat jest porównywalna do wartości całego rynku narkotykowego i plasuje się na poziomie 388 mld dolarów rocznie. Jak wynika z przeprowadzonych badań, ofiarami wszelkich form nielegalnej działalności w Internecie (w tym także związanej z rozsiewaniem wirusów komputerowych oraz innych typów złośliwego oprogramowania) pada rocznie pół miliarda ludzi, co w skali światowej daje średnią około 14 ofiar tego typu bezprawnej aktywności na sekundę. W Polsce w 2010 r., według oficjalnych danych Policji, zgłoszono prawie 8 tys. przestępstw popełnionych w sieci, z czego ponad 6 tys. oszustw. W 2012 r. ogólna liczba przestępstw komputerowych oscylowała już na poziomie 19 tys. (około 3/4 przypadków oszustw), aby w 2015 r. przekroczyć 20 tys. Specyfika przestępstw popełnianych w cyberprzestrzeni powoduje bowiem, że wiele tego typu czynów pozostaje niewykrytych lub nie są one poprawnie identyfikowane jako przestępstwa[4]. Zgodnie z *Raportem rocznym z działalności CERT Polska za 2016 rok* głównym zauważalnym motywem przestępstw komputerowych w 2016 r. była (podobnie jak w latach poprzednich) chęć kradzieży środków pieniężnych należących do użytkowników Internetu. Oprócz phishingów dostrzegalny był także wzrost liczby prób oszustw w odniesieniu do klientów bankowości mobilnej. Nie można przemilczeć również kilku kampanii, które miały na celu podszycie się pod duże spółki z branży telekomunikacyjnej i energetycznej. W ramach tych kampanii rozsyłane były dobrze spreparowane maile, rzekomo zawierające e-fakturę za usługi. W praktyce za ich pomocą dystrybuowane były w postaci załącznika różne warianty oprogramowania szyfrującego dysk ofiary i wymuszającego niemałą opłatę za udostępnienie klucza odszyfrowującego (*ransomware*). Ofiarami tego typu ataków padały osoby prywatne, ale również kilka instytucji państwowych[5].

---

nych przestrzeni, tj. inteligentnych miast, transportu, produktów, budynków, systemów energetycznych, systemów zdrowia czy związanych z życiem codziennym. Podstawą rozwoju IoT jest dostarczenie technologii, która zapewni ich realizację. Według Business Insider (BI), rozwój IoT na dobre rozpoczął się w roku 2010. W 2018 r. urządzeń tego typu ma być już 9 mld. Jeszcze innymi dziedzinami, które według ekspertów zostaną w pełni zsieciowane, są zarządzanie ruchem miejskim i poborem opłat, monitoring utylizacji odpadów – https://www.computerworld.pl [dostęp: 26.05.2018].

[4] J. Wasilewski, *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15 (8), s. 149.

[5] *Raport roczny z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego Internetu 2016*, NASK/CERT Polska, Warszawa 2016, s. 12.

Sporządzony przez CERT-NASK Polska raport pt. *Krajobraz bezpieczeństwa polskiego Internetu 2016* jednoznacznie potwierdza hipotezę o rosnącej skali dokonywanych cyberprzestępstw, wskazując następujące zjawiska:

- wraz ze wzrostem wartości kryptowalut rośnie liczba i skala ataków na serwisy zajmujące się ich przechowywaniem i wymianą, a także motywacja przestępców do takich działań. Wartość środków skradzionych w ten sposób w 2016 r. jest liczona w dziesiątkach milionów dolarów;
- wciąż nierozwiązanym problemem – istotnym zwłaszcza w kontekście ataków o wielkiej skali, takich jak kradzież pieniędzy z systemu SWIFT czy domniemana ingerencja w wybory prezydenckie w USA – pozostaje kwestia atrybucji[6];
- zdecydowanie najczęstszym typem incydentu obsługiwanym przez CERT Polska był phishing, stanowiący ponad połowę wszystkich przypadków. Były to przede wszystkim zgłoszenia fałszywych stron zagranicznych serwisów, umieszczonych na przejętych stronach lub wykupionych serwerach w polskich sieciach bądź w domenie .pl. Znacznie rzadziej phishing dotyczył podszywania się pod bank;
- w kategorii przestępstwa kradzieży tożsamości, podszycia się, które obejmuje phishing, CERT Polska zaobserwował wzrost liczby incydentów w stosunku do poprzedniego roku aż o 106% (495 w 2015 r., 1069 w 2016 r.), a więc znacząco przewyższający wzrost liczby incydentów w pozostałych kategoriach.

Należy również zaznaczyć, że ogromna liczba cyberprzestępstw pozostaje ukryta w szarej strefie i wymyka się wszelkim statystykom lub też do tej pory nie była ujawniana, np. przez przedsiębiorstwa czy instytucje finansowe, głównie ze względu na obawę przed stratą klientów czy możliwością występowania przez nich o odszkodowania.

Prawnokarna klasyfikacja terminu cyberprzestępczość

Termin cyberprzestępczość powstał jeszcze na początku lat 90. XX w. Oficjalnie został użyty przez tzw. Grupę z Lyonu, działającą w ramach grupy G8, której zadaniem było prowadzenie prac analitycznych nad nowymi formami przestępczości[7]. Należy zgodzić się z dokonaną przez Janusza Wasilew-

[6] CERT Polska poświęcił temu zagadnieniu część pracy w ramach projektu CyberROAD.

[7] Por. J. Wasilewski, op. cit., s. 150 (za: S. Perrin, *Cybercrime*, w: A. Ambrosi, V. Peugeot, D. Pimienta, *Word Matters: Multicultural Perspectives on Information Societies*, C & F éditions, Caen 2005). A. Adamski zwraca uwagę na zastosowanie omawianego terminu w 1996 r. przez L.E. Quarantiello, w: tejże, *Cyber Crime: How to Protect Yourself from Computer Criminals*, Limelight Books, Wisconsin 1996; A. Adamski, *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000, s. 30 i n.

skiego analizą zagadnień definicyjnych przestępczości w cyberprzestrzeni[8] i stwierdzeniem, że ze względu na specyfikę oraz konieczność tworzenia i poprawnego stosowania prawa zapewnienie skutecznego zwalczania zagrożeń w cyberprzestrzeni uzasadnia prowadzenie szerokiej analizy całej gałęzi związanej z tą dziedziną działalności przestępnej i pojęć odnoszących się do czynów wchodzących w jej skład, a wręcz jej wymaga. Pojęcie cyberprzestępczości, pomimo że wciąż nie stanowi kategorii prawnej, z uwagi na szeroki zakres znaczeniowy jest stosowane obecnie szeroko w piśmiennictwie i strategicznych dokumentach dotyczących bezpieczeństwa cyberprzestrzeni w odniesieniu do przestępczości komputerowej.

Należy podzielić zdanie Macieja Sawickiego[9], że pojęcia cyberprzestępstwa nie powinno się utożsamiać i stosować zamiennie z określeniem „przestępstwo internetowe", obejmującym jedyne grupę czynów, które mogą być popełniane tylko w Internecie (np. wprowadzenie w błąd co do nadawcy e-maila, aby uzyskać dane osobowe) lub za jego pomocą (np. zniesławienie z wykorzystaniem strony www). W odniesieniu do sprawców cyberprzestępstw w piśmiennictwie na określenie sprawców przestępstw komputerowych, godzących w funkcjonowanie sieci komputerowych, używa się pojęcia „hakerzy". Postępują tak nawet ci autorzy, którzy starają się przestrzegać wskazanej wyżej konwencji językowej i przez pojęcie hakingu rozumieją jedynie uzyskanie nielegalnego dostępu do systemu komputerowego (czy sieci komputerowej) lub danych komputerowych[10].

Obowiązującymi środkami prawnokarnymi zwalczania cyberprzestępczości w Polsce są ustawa z dnia 6 czerwca 1997 r. – Kodeks karny i wiele innych ustaw szczegółowych (np. ustawa o ochronie danych osobowych[11], ustawa o prawie autorskim i prawach pokrewnych[12]), a przede wszystkim ratyfikowana przez Polskę w maju 2015 r. Konwencja Rady Europy o cyberprzestępczości z 2001 r.[13] (znana również jako konwencja budapeszteńska), której ustanowie-

[8] Por. J. Wasilewski, op. cit., s. 149–173.

[9] M. Sawicki, *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013, s. 20.

[10] F. Radoniewicz, op. cit., s. 22 (za: S.W. Brenner, w: R.D. Clifford (red.), *Cybercrime. The Investigation, Prosecution and Defense of a Computer-related Crime*, Carolina Academic Press, Durham 2011, s. 18; J. Erickson, *Hacking. Sztuka penetracji*, Helion, Gliwice 2004, s. 9–13; D.L. Shinder, E. Tittel, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Helion, Gliwice 2005, s. 301; U. Sieber, *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, „Przegląd Policyjny" 1995, nr 3, s. 12; M. Siwicki, op. cit., s. 158).

[11] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133, poz. 883).

[12] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 Nr 24, poz. 83).

[13] Por. Konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r.

nie było ważnym krokiem w rozwoju pojęcia i opisu problematyki zwalczania cyberprzestępczości. Konwencja stanowiła w 2015 r. wzór dla ustawodawstwa krajowego w dziedzinie cyberprzestępczości i była podstawą współpracy międzynarodowej z państwami trzecimi w tym zakresie. Przedstawiona w niej unijna wizja opierała się na pięciu strategicznych priorytetach: osiągnięciu odporności na zagrożenia cybernetyczne; radykalnym ograniczeniu cyberprzestępczości; opracowaniu polityki obronnej i rozbudowie zdolności w dziedzinie bezpieczeństwa cybernetycznego w powiązaniu ze wspólną polityką bezpieczeństwa i obrony (WPBiO); rozbudowie zasobów przemysłowych i technologicznych na potrzeby bezpieczeństwa cybernetycznego; ustanowieniu spójnej polityki międzynarodowej w zakresie cyberprzestrzeni dla Unii Europejskiej i promowaniu podstawowych wartości Unii Europejskiej. Konwencja Rady Europy jest pierwszym i obecnie jedynym w Polsce aktem dotyczącym środków prawa karnego w zwalczaniu cyberprzestępczości. Jako zbiór standardów prawnych służy współpracy międzynarodowej w dziedzinie ścigania przestępstw transgranicznych popełnianych z wykorzystaniem technologii informatycznych. Konwencja wywarła istotny wpływ na ustawodawstwa karne państw europejskich i pozaeuropejskich. Dzięki jej przyjęciu uczyniono istotny krok w kierunku przyjęcia uniwersalnych standardów w zakresie podejścia do problematyki przestępstw popełnianych przy zastosowaniu technologii informatycznych (np. podjęto definicję czynów zabronionych i norm dotyczących współpracy międzynarodowej w ich ściganiu). W akcie tym znajdują się przepisy prawa karnego materialnego – zawierające definicje pojęć i określające znamiona przestępstw, prawa karnego procesowego – określające normy i procedury postępowania w sprawach dotyczących przestępstw określonych w konwencji i innych przestępstw popełnionych przy wykorzystaniu systemu informatycznego oraz zbierania dowodów w formie elektronicznej odnoszących się do przestępstw, a także regulacje dotyczące jurysdykcji nad przestępstwami w niej określonymi i postanowienia dotyczące współpracy międzynarodowej odnoszące się do ekstradycji i wzajemnej pomocy prawnej oraz wymiany informacji[14]. Jednak mając na uwadze wzrastającą stale skalę cyberprzestępczości i nieskuteczność w praktyce wielu założeń konwencji, należałoby przyjąć hipotezę, że brakuje nadal wiążących środków prawnokarnych i odpowiednich kadr, aby skuteczniej przeciwdziałać temu zjawisku.

[14] Szerzej za: S. Gwoździewicz, *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej oraz Strategia na rzecz lepszego internetu dla dzieci w działaniach prawnych Unii Europejskiej na lata 2014–2020 (The European Union Cybersecurity Strategy and better Internet for children in European Union Legal Action for 2014–2020)*, w: *Принципи і тенденції застосування приватного права ЄС і пострадянських країн* (*Zasady i tendencje stosowania prawa prywatnego UE w krajach postradzieckich*), Taras Shevchenko National University of Kyiv, Faculty of Law, Department of Civil Law, Kyiv 2018, s. 109–113.

W 2013 r. w przedstawionej przez Komisję Europejską *Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*[15] pojawia się pojęcie cyberprzestępczości w odniesieniu do założeń, że państwa członkowskie powinny utworzyć w wyniku niniejszej strategii struktury przeznaczone do działań w zakresie odporności cybernetycznej, cyberprzestępczości i cyberobrony; powinny też osiągnąć poziom zdolności wymagany do celów reagowania na incydenty cybernetyczne[16]. Jeśli chodzi o cyberbezpieczeństwo RP, obecnie rząd pracuje nad projektem ustawy o krajowym systemie cyberbezpieczeństwa, natomiast oficjalnie (wg projektu ustawy) *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej* zostanie przyjęta do dnia 31 października 2019 r.[17] Do czasu przyjęcia strategii jej funkcję pełnią przyjęte przez Radę Ministrów uchwałą nr 52/2017 z dnia 27 kwietnia 2017 r. *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*[18], który to dokument w ramach drugiego celu szczegółowego zakłada zwiększenie zdolności do zwalczania cyberprzestępczości i cyberszpiegostwa przez wymianę informacji, współpracę międzynarodową i lepszą koordynację działań między różnymi instytucjami.

Tworzenie nowych działów i biur do walki z cyberprzestępczością

Minister sprawiedliwości w kwietniu 2016 r. na podstawie § 27 i § 29 Regulaminu wewnętrznego urzędowania powszechnych jednostek organizacyjnych[19] ustanowił możliwość tworzenia w prokuraturze regionalnej i okręgowej działów obejmujących zakresem swojej właściwości prowadzenie i nadzoro-

[15] Komunikat Wspólny Komisji Europejskiej, Wysokiego Przedstawiciela UE do spraw Zagranicznych i Polityki Bezpieczeństwa do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 07.02.2013 r., *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*. Bruksela 2013, s. 9, 12, 18.

[16] S. Gwoździewicz, s. 109–110.

[17] Należy zwrócić uwagę na nieścisłość w projektach ogłaszanych na stronach internetowych Ministerstwa Cyfryzacji (początkowo w 2016 r. umieszczony był dokument pt. *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016–2020: poszanowanie praw i wolności w cyberprzestrzeni, kompleksowe podejście do cyberbezpieczeństwa istotnym elementem polityki państwa*, Ministerstwo Cyfryzacji, Warszawa 2016 (strategia ta nie została przyjęta przez Radę Ministrów). Następnie w 2017 r. ukazał się dokument o tej samej treści, ale już pod innym tytułem: *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, który został przyjęty uchwałą Rady Ministrów nr 52/2017 9 maja 2017 r.

[18] *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej*…, op. cit. zastąpiły *Politykę Ochrony Cyberprzestrzeni RP*, opracowaną przez ówczesne Ministerstwo Administracji i Cyfryzacji oraz Agencję Bezpieczeństwa Wewnętrznego, przyjętą przez rząd w czerwcu 2013 r.

[19] Rozporządzenie Ministra Sprawiedliwości z dnia 7 kwietnia 2016 r. – Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury (Dz.U. 2016, poz. 508).

wanie wieloosobowych spraw o poważne przestępstwa z wykorzystaniem Internetu oraz zaawansowanych technologii i systemów informatycznych (cyberprzestępczość) o skomplikowanym stanie faktycznym lub jeżeli wartość szkody wyrządzonej przestępstwem przekracza kwotę (wskazaną w art. 115 § 6 k.k.). Rozporządzenie wskazuje również, że jeżeli w prokuraturze pionu regionalnego lub okręgowego nie został utworzony dział do spraw cyberprzestępczości i przestępstw z wykorzystaniem Internetu, to prokurator może powierzyć prowadzenie i nadzorowanie tego spraw tego działu jednemu lub kilku prokuratorom.

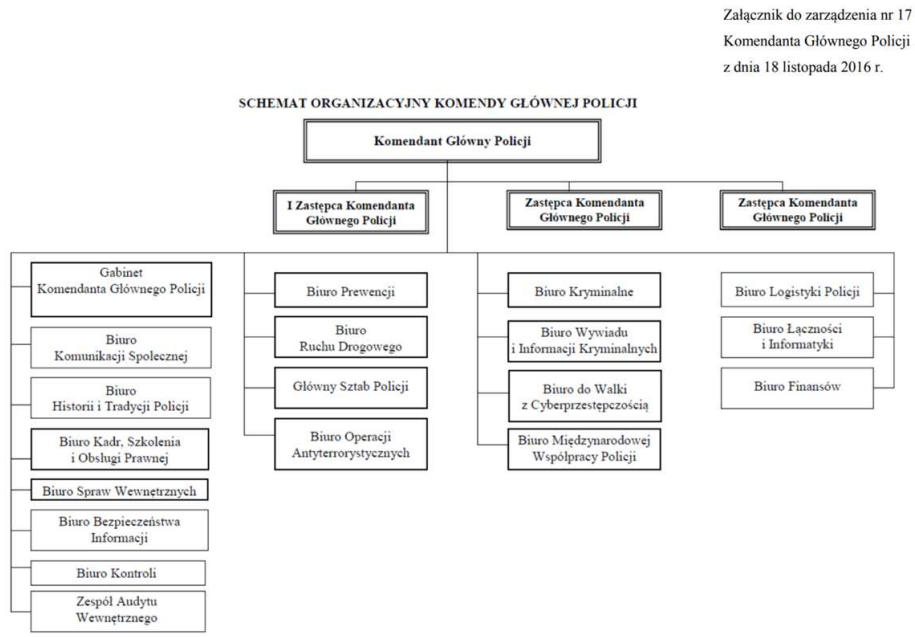
Z kolei w strukturach Policji pod koniec 2016 r. zostało powołane Biuro do Walki z Cyberprzestępczością (strukturę tę przedstawia ryc. 1), które realizuje zadania związane z tworzeniem warunków do efektywnego wykrywania sprawców przestępstw popełnionych przy użyciu nowoczesnych technologii teleinformatycznych. Biuro zostało powołane na podstawie zarządzenia Komendanta Głównego Policji z dnia 18 listopada 2016 r. zmieniającego zarządzenie w sprawie regulaminu Komendy Głównej Policji[20], które precyzuje również zadania biura; należy do nich w szczególności:

- nadzorowanie, koordynowanie i wspieranie ukierunkowanych na zwalczanie cyberprzestępczości działań prowadzonych przez komendy wojewódzkie (Stołeczną) Policji w zakresie czynności operacyjno-rozpoznawczych oraz współdziałanie z Centralnym Biurem Śledczym Policji w tym zakresie;
- prowadzenie czynności operacyjno-rozpoznawczych pozostających we właściwości biura;
- inicjowanie i prowadzenie współpracy z organami administracji rządowej, sądami, prokuraturami, instytucjami państwowymi, a także podmiotami prywatnymi w zakresie zadań pozostających we właściwości biura;
- prowadzenie współpracy międzynarodowej oraz współdziałanie z Biurem Międzynarodowej Współpracy Policji w zakresie zadań pozostających we właściwości biura;
- prowadzenie całodobowej służby mającej na celu koordynowanie działań Policji w zakresie zagrożeń przestępstwami w sieci Internet, ich zwalczania oraz współdziałania jednostek organizacyjnych Policji z krajowymi i zagranicznymi organami i podmiotami pozapolicyjnymi;

[20] Zarządzenie nr 17 Komendanta Głównego Policji z dnia 18 listopada 2016 r. zmieniające zarządzenie w sprawie regulaminu Komendy Głównej Policji (Dz. Urz. KGP z 2016 r., poz. 69).

- prowadzenie konsultacji technicznych, inicjowanie i wspieranie badań oraz projektów, a także współpraca z podmiotami krajowymi i zagranicznymi zmierzająca do rozpoznawania i implementowania nowoczesnych rozwiązań w walce z cyberprzestępczością[21].

Zadania stojące przed Biurem do Walki z Cyberprzestępczością może ono realizować w sposób jawny bądź niejawny za pomocą różnych czynności służbowych[22], takich jak: czynności operacyjno-rozpoznawcze[23], czynności dochodzeniowo-śledcze, czynności administracyjno-porządkowe.



Ryc. 1. Schemat organizacyjny KGP z nowym Biurem do Walki z Cyberprzestępczością

Źródło: Zarządzenie nr 17 Komendanta Głównego Policji z dnia 18 listopada 2016 r. zmieniające zarządzenie w sprawie regulaminu Komendy Głównej Policji.

[21] Art. 16a zarządzenia nr 17 Komendanta Głównego Policji z dnia 18 listopada 2016 r. zmieniającego zarządzenie w sprawie regulaminu Komendy Głównej Policji (Dz.Urz. KGP z 2016 r., poz. 69).

[22] Art. 15. Uprawnienia policjantów w trakcie wykonywania czynności służbowych ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. 2017.0.2067 t.j.).

[23] Czynności operacyjno-rozpoznawcze spełniają funkcję informacyjną, wykrywczą, profilaktyczną i dowodową. Są to czynności pozaprocesowe, do których zalicza się w szczególności: kontrolę operacyjną, zakup kontrolowany, prowokację policyjną, tajnego agenta Policji, niejawne nadzorowanie.

Biuro organizuje współpracę z różnymi instytucjami państwowymi opartą na: kompleksowym pozyskiwaniu informacji, wyszukiwaniu miejsc przestępstw; zdolności do współdziałania, umiejętności zespołowego wykonywania zadań i wspólnego rozwiązywania problemów nie tylko w strukturach państwowych, ale i międzynarodowych; dwudziestoczterogodzinnym wykonywaniu obowiązków przez funkcjonariuszy w celu zapewnienia harmonijnego i kompleksowego przebiegu działań Policji w zakresie zapobiegania zagrożeniom cyberprzestępstwami; udzielaniu rad i wyjaśnień dotyczących sposobu i wykonywania zadań oraz wspieraniu wszelkiego rodzaju doświadczeń dotyczących zagadnień i projektów związanych ze zwalczaniem cyberprzestępczości. Współpracuje ono również z podmiotami wewnętrznymi i zewnętrznymi w celu tworzenia i przystosowania nowoczesnych rozwiązań w walce z cyberprzestępczością oraz podejmowania działań profilaktycznych.

Diagnoza potrzeb kształcenia specjalistów ds. zwalczania cyberprzestępczości w *Polityce Cyberbezpieczeństwa RP na lata 2017–2022*

Polityka Cyberbezpieczeństwa RP na lata 2017–2022[24] zakłada konieczność kształcenia specjalistów ds. cyberprzestępczości. W celu szczegółowym nr 2 przewiduje wzmocnienie zdolności do przeciwdziałania cyberzagrożeniom m.in. przez zwiększenie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym występujących w cyberprzestrzeni. W zakresie zwiększania zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa, zdarzeń o charakterze terrorystycznym oraz działań o charakterze hybrydowym, ważne jest zapewnienie wsparcia dla operatorów usług kluczowych, dostawców usług cyfrowych oraz operatorów infrastruktury krytycznej w wykrywaniu oraz zwalczaniu incydentów we wszystkich ich fazach. Wymagana jest współpraca oraz koordynacja działań organów ścigania niezależnie od motywów, którymi kierują się sprawcy przestępstw. Istotne znaczenie ma zabezpieczenie dowodów elektronicznych. Zwiększenie efektywności czynności procesowych lub operacyjnych wymaga także poszerzenia współdziałania organów ścigania z innymi podmiotami, które mogą posiadać wiedzę w zakresie ustalenia istoty przestępstwa lub mogą przyczynić się do ustalenia jego sprawcy. Dotyczy to współpracy z krajowymi

[24] *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022: poszanowanie praw i wolności w cyberprzestrzeni, kompleksowe podejście do cyberbezpieczeństwa istotnym elementem polityki państwa*, Ministerstwo Cyfryzacji, Warszawa 2017 – dokument został zatwierdzony uchwałą nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. (RM-111-52-17), https://www.gov.pl/documents/31305/0/rm-111-52-17_obieg_uchw_nr_52_rm_z_2017_r._cyberbezpieczenstwo_rp_2017-2022.pdf/3d6c4f6d-a278-81ad-5ff2-56693e55b23b [dostęp: 26.05.2018].

oraz międzynarodowymi podmiotami prywatnymi, szczególnie z sektora telekomunikacyjnego, bankowego oraz ubezpieczeniowego. Niezbędne jest zaangażowanie przedstawicieli organów ścigania, w tym Policji, w prace krajowych oraz międzynarodowych forów wymiany informacji o zagrożeniach i podatnościach na cyberataki.

Z uwagi na specyfikę cyberprzestrzeni zwalczanie cyberprzestępczości wymaga transgranicznej współpracy organów ścigania oraz podmiotów typu CERT/CSIRT. W czynnościach procesowych lub w procesie rozpoznania operacyjnego dotyczących przestępstw dokonywanych w cyberprzestrzeni krytyczny jest upływ czasu. Oznacza to, że konieczne są sprawne i zaufane kanały wymiany informacji pomiędzy organami ścigania różnych państw. Szybko zmieniające się metody popełniania przestępstw wymagają rozwijania badań naukowych w zakresie zwalczania cyberprzestępczości, których wyniki zapewnią wsparcie dla organów ścigania. Wyniki tych badań będą wykorzystywane w pracy organów ścigania i wymiaru sprawiedliwości, jak też będą stanowić materiał do opracowania działań profilaktycznych. Wdrożone zostaną skierowane do społeczeństwa programy informacyjne o zagrożeniach cyberprzestępczością oraz metodach unikania skutków tych zagrożeń, a także wskazane sposoby postępowania dla osób dotkniętych przestępstwem. Ważną rolę do odegrania w tego typu działalności będą mieli operatorzy usług kluczowych, dostawcy usług cyfrowych, dostawcy usługi dostępu do Internetu oraz organizacje pozarządowe.

Niezbędnym elementem omawianej polityki, zapewniającym skuteczną realizację jej założeń, jest zwiększanie kompetencji kadry podmiotów istotnych dla bezpieczeństwa cyberprzestrzeni, w tym walki z cyberprzestępczością. Jak wskazano w omawianym dokumencie, podnoszenie kwalifikacji kadry podmiotów istotnych dla bezpieczeństwa cyberprzestrzeni RP ma polegać na stworzeniu i wdrożeniu takiego modelu funkcjonowania systemu edukacji akademickiej i doskonalenia zawodowego, który zapewni odpowiedni do wyzwań poziom profesjonalizmu pracowników. Uczelnie będą zachęcane do tego, aby rozwijać specjalizacje interdyscyplinarne, obejmujące m.in. zarządzanie bezpieczeństwem informacji, ochronę danych osobowych, ochronę własności intelektualnej w Internecie oraz zagadnienia związane z rozwojem nowych technologii i wyzwaniami, które są tego pochodnymi. W ramach szeroko rozumianej edukacji eksperckiej, aby skuteczniej przeciwdziałać rozwijającej się cyberprzestępczości, zostanie wzmocniony system szkoleń dla wszystkich pracowników podmiotów istotnych dla funkcjonowania bezpieczeństwa w cyberprzestrzeni oraz dla przedstawicieli organów ścigania i wymiaru sprawiedliwości. W celu zatrzymania w administracji publicznej pracowników o wysokich kom-

petencjach, równolegle z wykorzystaniem innych instrumentów wspierających ich aktywność, uruchomione zostaną programy motywacyjne, w tym rządowy program „Złota Setka". Będzie on skierowany do specjalistów z obszaru IT i bezpieczeństwa teleinformatycznego, zatrudnionych w administracji publicznej, i ma na celu utrzymywanie i promowanie najlepiej wykwalifikowanych profesjonalistów. Za przygotowanie i wdrożenie programu odpowiadać będzie minister właściwy do spraw informatyzacji. W celu zapewnienia merytorycznego wsparcia dla kierowników jednostek administracji rządowej w zakresie zarządzania cyberbezpieczeństwem utrzymana zostanie zasada powoływania w tych jednostkach pełnomocników do spraw bezpieczeństwa cyberprzestrzeni. Aby zaś zapewnić optymalne wykorzystanie zasobów ludzkich w dziedzinie cyberbezpieczeństwa w Polsce, zostanie opracowany model zarządzania tymi zasobami.

Efektywne wdrażanie polityki cyberbezpieczeństwa i kształcenie przyszłych kadr nie jest możliwe bez odpowiednich działań profilaktycznych w dziedzinie edukacji na różnych szczeblach kształcenia. Edukację w zakresie cyberbezpieczeństwa należy rozpoczynać już na etapie kształcenia wczesnoszkolnego. Polityka cyberbezpieczeństwa RP zakłada opracowanie i wdrożenie zmian do podstaw programowych nauczania; opracowanie i uruchomienie kursów doszkalających dla nauczycieli informatyki oraz wdrożenie adekwatnych zmian w kształceniu podyplomowym nauczycieli. Równolegle, we współpracy z organizacjami pozarządowymi oraz ośrodkami akademickimi, administracja publiczna ma podejmować systemowe działania uwrażliwiające społeczeństwo na zagrożenia płynące z cyberprzestrzeni, a także działania edukacyjne w zakresie praw i wolności w środowisku cyfrowym. Uruchomione zostaną m.in. kampanie społeczne, skierowane do różnych grup docelowych (dzieci, rodziców, seniorów). We współpracy ze środowiskiem naukowo-akademickim zostaną opracowane programy badawcze mające na celu: ocenę skuteczności zabezpieczeń i odporności cyberprzestrzeni RP na cyberzagrożenia; ocenę skuteczności reagowania za zagrożenia; analizy tendencji w zakresie nowych cyberprzestępstw, cyberterroryzmu i metod ich zwalczania; badanie metod ataków i sposobów im przeciwdziałania. Do głównych zadań w tym zakresie należy zaliczyć m.in. badanie i opisywanie sposobów i metod ataków, badanie cyberprzestępstw, cyberterroryzmu, a także opracowywanie skutecznych metod przeciwdziałania. Zakłada się opracowanie rozwiązań umożliwiających: szybką identyfikację zagrożeń; usprawnienie systemu informowania o zagrożeniach; podniesienie efektywności zabezpieczeń proceduralno-organizacyjnych i technicznych; skuteczne informowanie użytkowników cyberprzestrzeni o zagroże-

niach; podnoszenie wiedzy informatycznej użytkowników cyberprzestrzeni; wypracowanie metod obrony przed zmasowanymi atakami z cyberprzestrzeni[25].

Oferta kształcenia specjalistów ds. cyberprzestępczości w polskich uczelniach

Zwiększająca się liczba różnych cyberprzestępstw i zagrożeń w Internecie zmusza instytucje, służby, organy ścigania zajmujące się cyberprzestępczością, ale i samych użytkowników Internetu do podejmowania różnych działań zapobiegawczych, w tym profilaktycznych i edukacyjnych, ponieważ w tej dziedzinie w parze z umacnianiem zabezpieczeń systemów powinno iść także stałe podnoszenie świadomości użytkowników Internetu w kwestii bezpieczeństwa oraz nowych typów i sposobów cyberataków.

Dlatego też celem niniejszego opracowania jest dokonanie analizy możliwości kształcenia specjalistów ds. cyberprzestępczości w polskim systemie szkolnictwa wyższego. Jej przedmiotem są oferty kształcenia dostępne w wyszukiwarkach internetowych i na wybranych losowo portalach internetowych uczelni w okresie od 1 marca do 31 maja 2018 r. Wyniki analizy przedstawiono w tabeli 1.

Tab. 1. Analiza oferty kształcenia specjalistów ds. cyberprzestępczości

Kształcenie akademickie	**Kierunek studiów**	**Proponowana specjalność/ścieżka kształcenia specjalistów ds. cyberprzestępczości**	**Uczelnia/koszt studiów**
Studia pierwszego stopnia	Kryminologia stosowana	**Zwalczanie cyberprzestępczości**	Wydział Administracji i Bezpieczeństwa Narodowego im. Jakuba z Paradyża w Gorzowie Wielkopolskim[26]
	Specjalność w zakresie zwalczania cyberprzestępczości na WA-iBN AJP w Gorzowie Wielkopolskim pozwoli studentowi zdobyć wiedzę, umiejętności i kompetencje społeczne dotyczące rozpo-		

[25] *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 poszanowanie praw i wolności w cyberprzestrzeni kompleksowe podejście do cyberbezpieczeństwa istotnym elementem polityki państw*a. Ministerstwo Cyfryzacji, Warszawa 2017.

[26] Zarządzenie nr 1/0101/2018 Rektora AJP z dnia 16 stycznia 2018 r. w sprawie powołania Zespołu ds. przygotowania wniosku o nadanie uprawnień do prowadzenia studiów pierwszego stopnia na kierunku kryminologia stosowana – profil praktyczny, http://bip.ajp.edu.pl/ [dostęp: 20.03.2018].

<table>
<tr><td></td><td colspan="3">znawania, diagnozowania, wykrywania oraz przeciwdziałania cyberprzestępczości, w szczególności w zakresie: przestępstw komputerowych i przeciwko ochronie informacji; technik i analizy kanałów społecznościowych w profilaktyce cyberprzestępczości; strategii cyberbezpieczeństwa RP i UE oraz wybranych państw świata; ujawniania i zwalczania przestępstw przy użyciu sieci; postępowań w przestępstwach komputerowych w zwalczaniu cyberprzestępstw; informatyki śledczej i dowodów w postaci elektronicznej w wykrywaniu cyberprzestępstw; technik włamania do sieci i systemów informatycznych, cyberataków; ochrony i bezpieczeństwa sieci i systemów informatycznych, a także podstaw programowania komputerowego oraz zagadnień prawnych dotyczących ochrony danych osobowych i prywatności w cyfrowym świecie. Absolwent kierunku kryminologia stosowana o specjalności zwalczanie cyberprzestępczości zostanie przygotowany do podjęcia pracy w służbach państwowych, organach ścigania, krajowych instytucjach i przedsiębiorstwach różnego szczebla mających na celu rozpoznawanie, diagnozę, a przede wszystkim zwalczanie cyberprzestępstw i cyberprzestępczości.
Studia (wg stanu na 24.05.2018 r.) planowane są do uruchomienia w roku akademickim 2018/2019 po otrzymaniu uprawnień Ministra Nauki i Szkolnictwa Wyższego[27].</td></tr>
<tr><td rowspan="2">Studia drugiego stopnia i/lub jednolite magisterskie</td><td>Bezpieczeństwo wewnętrzne</td><td>Cyberprzestępczość</td><td>Wyższa Szkoła Administracji i Biznesu im. E. Kwiatkowskiego w Gdyni
koszt: 410/360 zł miesięcznie[28]</td></tr>
<tr><td colspan="3">Celem studiów jest zapoznanie studentów z problematyką przestępczości komputerowej, będącej nielegalną działalnością skierowaną przeciwko systemom komputerowym lub wykonywaną za pomocą systemów komputerowych, Internetu czy sieci komputerowych, jako narzędzi służących do dokonania przestępstwa. Absolwent studiów uzyska specjalistyczną wiedzę w zakresie cyberprzestępczości, jej miejsca w hierarchii zagrożeń bezpieczeństwa międzynarodowego, sposobów jej zapobiegania i zwalczania. Ukończenie studiów ułatwi zatrudnienie w instytucjach analitycznych i badawczych, w służbach zwalczających tę formę przestępczości, w administracji państwowej, w bankowości, w organach wymiaru sprawiedliwości oraz w podmiotach gospodarczych zajmujących się branżą IT[29].</td></tr>
</table>

[27] Uchwała nr 23/000/2018 Senatu AJP z dnia 24 kwietnia 2018 r. w sprawie utworzenia studiów pierwszego stopnia na kierunku kryminologia stosowana – profil praktyczny, http://bip.ajp.edu.pl/ [dostęp: 24.05.2018].

[28] https://wsaib.pl/kandydaci/studia-ii-stopnia/bezpieczenstwo-wewnetrzne/cyberprzestepczosc [dostęp: 24.05.2018].

[29] Tamże.

	Prawo	**Cyberprzestępczość**	WSPiA Rzeszowska Szkoła Wyższa koszt: 2250/1800 zł za semestr[30] (studia trwają 5 lat)
	Celem kształcenia jest przygotowanie studenta kierunku prawo do rozpoznawania i wykrywania zachowań niezgodnych z prawem w cyberprzestrzeni oraz im przeciwdziałania. Z jednej strony student uzyska wszechstronną wiedzę z zakresu zagadnień prawnych w cyberprzestrzeni (np. prawo telekomunikacyjne, prawo internetowe), a drugiej zaś umiejętności praktyczne z zakresu wykrywania przestępczości komputerowej, prowadzenia czynności dochodzeniowo-śledczych oraz operacyjno-rozpoznawczych, a także z zakresu informatyki śledczej. W ten sposób będzie przygotowany np. do podjęcia zatrudnienia w organach ścigania, jak również w sektorze prywatnym, na stanowiskach związanych z ochroną danych i bezpieczeństwem informacji[31].		
Studia podyplomowe (roczne)	**Rozpoznawanie, zapobieganie i zwalczanie cyberprzestępstw popełnianych na szkodę banków oraz ich klientów**		Wydział Bezpieczeństwa Wewnętrznego Wyższej Szkoły Policji w Szczytnie[32]
	Głównym celem kształcenia jest przygotowanie do skutecznego rozpoznawania i zwalczania współczesnych zagrożeń przestępczością kryminalną oraz im zapobiegania przez: doskonalenie umiejętności w zakresie najnowszych osiągnięć kryminalistyki; poszerzenie wiedzy o aktualnych zagrożeniach przestępczością; przedstawienie prawidłowych rozwiązań prawnych metod pracy operacyjnej; zapoznanie z nowoczesnymi technologiami w zakresie badania dowodów cyfrowych; kształcenie umiejętności wykorzystania źródeł i rezultatów biegłego wywiadu. Te sprofilowane studia zostały skierowane do wąskiej grupy odbiorców, tj. funkcjonariuszy Policji z jednostek przeznaczonych do walki z cyberprzestępczością oraz przestępczością gospodarczą; prokuratorów i sędziów prowadzących sprawy z zakresu cyberprzestępczości; pracowników sektora finansowego, w szczególności banków, zajmujących się przeciwdziałaniem oszustwom w bankowości internetowej mobilnej i kartowej oraz ich zwalczaniem, bezpieczeństwem transakcji internetowych, mobilnych i kartowych, a także bezpieczeństwem teleinformatycznym oraz dla pracowników zatrudnionych w Security Operations Center[33].		

[30] http://www.wspia.eu/dla-kandydata/kierunki-studiow/kierunek-prawo/prawo/cyberprzesteczosc [dostęp: 24.05.2018].

[31] Tamże.

[32] https://www.wspol.edu.pl/g/images/2017/dokumenty/oferta_studiow_podyplom_na_wbw_w_zakr_cyber.pdf [dostęp: 24.05.2018].

[33] Tamże.

	Specjalista ds. cyberprzestępczości	Krakowska Akademia im. Andrzeja Frycza Modrzewskiego koszt: 6900 zł[34]
	Celem studiów jest przygotowanie słuchaczy do pracy w komórkach IT w zakresie kreowania właściwej polityki bezpieczeństwa teleinformatycznego, tworzenia bezpiecznego środowiska gromadzenia i przesyłania danych, zgodnie z przyjętymi standardami oraz nabytymi umiejętnościami praktycznymi (Enterprise Device Management). Absolwenci zostaną przygotowani do samodzielnego prowadzenia zespołów odpowiedzialnych za reagowanie na incydenty sieciowe oraz kierowania nimi przez: uporządkowanie dotychczasowej wiedzy z zakresu cyberbezpieczeństwa; znajomość regulacji prawnokarnych; kształtowanie umiejętności doboru właściwych metod i narzędzi planowania oraz prowadzenia polityki w zakresie bezpieczeństwa teleinformatycznego; wdrożenie polityki bezpieczeństwa środowiska mobilnego; reagowania na incydenty bezpieczeństwa IT; pozyskanie wiedzy dotyczącej zasad i sposobów dokumentowania oraz zabezpieczania cyfrowego materiału dowodowego (informatyka śledcza, odzyskiwanie danych); przeprowadzanie procesu szacowania ryzyka dla bezpieczeństwa informacji[35].	
	Cyberprzestępczość	Wyższa Szkoła Bankowa w Gdańsku koszt: 4360 zł (z rabatem 3760 zł)[36]
	Celem studiów podyplomowych jest zaznajomienie słuchaczy z zagadnieniami związanymi ze zjawiskiem cybeprzestępczości i metodami jej zwalczania oraz zapobiegania. Absolwent studiów zyska teoretyczną oraz praktyczną wiedzę z zakresu bezpieczeństwa systemów informatycznych, analizy i informatyki śledczej, rodzajów zagrożeń i ataków oraz przeciwdziałania im, poszukiwania, gromadzenia i zabezpieczania materiału dowodowego oraz działań prewencyjnych. Słuchacz zapozna się z regulacjami prawnymi dotyczącymi zwalczania cybeprzestępczości obowiązującymi w Polsce i na świecie. Ponadto będzie potrafił przeprowadzić wstępną kwalifikację prawną zaistniałego incydentu oraz wskazać instytucję właściwą do podjęcia dalszych działań. Pozna zagadnienia prawne dotyczące ochrony danych osobowych i prywatności	

[34] https://www.ka.edu.pl/csp-oferta/specjalista-ds-cyberprzestepczosci/ [dostęp: 15.03.2018].
[35] Tamże.
[36] https://www.wsb.pl/gdansk/studenci/studia-podyplomowe/kierunki/cyberprzestepczosc [dostęp: 24.05.2018].

	w cyfrowym świecie, jak również przykłady działań socjotechnicznych stosowanych przez przestępców – będzie umiał je zidentyfikować, ustalić ich cel i zabezpieczyć organizację lub zminimalizować skutki takich działań. Nauczy się samodzielnie przygotować działania ćwiczebne sprawdzające skuteczność zabezpieczeń organizacji. Przygotuje strategię polityki bezpieczeństwa informatycznego organizacji oraz zarządzania obiegiem informacji wewnątrz niej i na zewnątrz. Pozna zasady tworzenia audytów bezpieczeństwa. Uczestnik studiów zdobędzie szczegółową wiedzę na temat aktualnych typów zagrożeń pochodzących z Internetu. Nauczy się je rozpoznać i im przeciwdziałać. Otrzyma zaawansowaną wiedzę z zakresu informatyki śledczej, dzięki czemu będzie potrafił samodzielnie zabezpieczyć część śladów cyfrowych i podjąć decyzję o właściwym użyciu instytucji specjalistycznych. Pozna zasady prawidłowego dokumentowania przebiegu incydentów informatycznych oraz czynności podjętych w celu przeciwdziałania. Uzyska także szczegółową wiedzę na temat technik i metod wywiadu otwartoźródłowego oraz kompetencje do zaawansowanego wyszukiwania danych i informacji w Internecie. Pozna podstawy analizy kryminalnej i będzie potrafił wykorzystać je do wnioskowania o przebiegu, przyczynach i sprawcach incydentów informatycznych[37].	
	Agent ds. cyberprzestępczości	Grupa Uczelni Vistula koszt: 7000 zł[38]
	Celem studiów jest jak najlepsze przygotowanie do pracy w działach IT i/lub w komórkach bezpieczeństwa teleinformatycznego. W ciągu dwóch semestrów słuchacz pozna zasady kreowania właściwej polityki bezpieczeństwa cyberprzestrzeni, tworzenia bezpiecznego środowiska, gromadzenia, przetwarzania i przesyłania danych zgodnie z przyjętymi standardami. Dzięki uporządkowaniu dotychczasowej wiedzy z zakresu cyberbezpieczeństwa, zdobyciu teoretycznej wiedzy i praktycznych umiejętności słuchacz zostanie przygotowany do samodzielnego prowadzenia zespołów odpowiedzialnych za reagowanie na incydenty sieciowe oraz kierowania nimi. Zyska kompetencje do: planowania i prowadzenia polityki w zakresie bezpieczeństwa teleinformatycznego; wdrażania polityki bezpieczeństwa środowiska mobilnego; umiejętnego dokumentowania oraz zabezpieczania cyfrowego materiału dowodowego (informatyka śledcza, odzyskiwanie danych); przeprowadzania procesu szacowania ryzyka dla bezpieczeństwa informacji.	

[37] Tamże.

[38] http://www.vistula.edu.pl/kierunki-studiow/kontynuacja-edukacji/studia-podyplomowe/informatyka/agent-ds-cyberprzestepczosci/ [dostęp: 30.03.2018].

	Cyberprzestępczość	Uczelnia Łazarskiego w Warszawie[39] koszt studiów nie został podany
	Celem studiów jest zapoznanie studentów z problematyką cyberprzestępczości ze szczególnym uwzględnieniem zagrożeń związanych z wykorzystaniem sieci teleinformatycznych. Studia uruchomiono w związku z potrzebą reakcji na rosnące znaczenie technologii informatycznych w naszym życiu, tj.: wzrost liczby dokumentów przekazywanych drogą elektroniczną; rosnącą liczbę przestępstw, w których wykorzystywane są technologie informatyczne; pojawiające się nowe formy przestępczości, takie jak cyberprzestępczość, cyberterroryzm; niedobór specjalistów w zakresie zwalczania nowych form przestępczości z wykorzystaniem Internetu w Policji i innych służbach; podniesienie efektywności i skuteczności ścigania karnego; zastosowanie nowych metod zapobiegania cyberprzestępczości. Studia skierowane są do osób zainteresowanych zwalczaniem nowych form przestępczości, a przede wszystkim do pracowników administracji państwowej, pracowników organów ścigania i wymiaru sprawiedliwości, pracowników banków. Program studiów realizowany jest w partnerstwie z Komendą Główną Policji. Prowadzący zajęcia to uznani wykładowcy i eksperci z doświadczeniem w zakresie cyberprzestępczości i informatyki śledczej, a absolwent studiów uzyskuje nowe kwalifikacje w zakresie zwalczania i zapobiegania przestępczości ze szczególnym uwzględnieniem przestępczości internetowej. Ukończenie studiów umożliwia awans zawodowy, a nowe umiejętności zawodowe mogą zostać wykorzystane także poza służbą w Policji[40].	
	Cyberprzestępczość	Wyższa Szkoła Handlowa w Radomiu koszt: 3000 zł[41]
	Studia podyplomowe adresowane są do kadry kierowniczej wszystkich szczebli oraz specjalistów z jednostek administracji publicznej, organów ścigania, wymiaru sprawiedliwości, instytucji bankowych i finansowych odpowiedzialnych za bezpieczeństwo w danej jednostce. Celem studiów jest pogłębienie wiedzy teoretycznej w zakresie problematyki bezpieczeństwa teleinformatycznego oraz nabycie przez słuchaczy praktycznych umiejętności w zakresie zwalczania nowych form przestępczości oraz reagowania na incydenty sieciowe[42].	

Źródło: opracowanie własne.

[39] http://www.uczelnie.info.pl/PL-H10/aktualnosc/5693/studia-podyplomowe-w-warszawie-cyberprzestepczosc-na-uczelni-lazarskiego.html [dostęp: 12.04.2018].

[40] Tamże.

[41] http://podyplomowe.wsh.pl/wp-content/uploads/2017/05/cyberprzestepczosc.pdf - [dostęp: 28.04.2018].

[42] Tamże.

Po przeprowadzonej analizie powyższych ofert kształcenia specjalistów ds. cyberprzestępczości należy stwierdzić, że uczelnie nie są jeszcze wystarczająco przygotowane, aby rozpocząć kształcenie w tym zakresie. Propozycję kształcenia na rok akademicki 2018/2019 w zakresie cyberprzestępczości przygotowały tylko nieliczne uczelnie[43] (jedna oferta na studiach pierwszego stopnia, jedna na studiach drugiego stopnia i jedna na studiach jednolitych magisterskich). Również opłaty za studia są bardzo zróżnicowane w zależności od kategorii specjalistów pozyskanych jako wykładowcy, nawiązanej przez uczelnie współpracy międzysektorowej w celu zdobycia doświadczeń praktycznych czy też dodatkowej certyfikacji modułów kształcenia. Więcej ofert (sześć) można odnaleźć w propozycjach rocznych studiów podyplomowych.

Należy zwrócić uwagę na ofertę studiów podyplomowych wdrożoną od roku akademickiego 2017/2018 przez Wyższą Szkołę Policji w Szczytnie w zakresie „Rozpoznawania, zapobiegania i zwalczania cyberprzestępstw popełnianych na szkodę banków oraz ich klientów". Jest ona skierowana do funkcjonariuszy Policji z jednostek przeznaczonych do walki z cyberprzestępczością oraz przestępczością gospodarczą; prokuratorów i sędziów prowadzących sprawy z zakresu cyberprzestępczości; pracowników sektora finansowego, w szczególności banków, zajmujących się przeciwdziałaniem oszustwom w bankowości internetowej mobilnej i kartowej oraz ich zwalczaniem. Oferta ta stała się podstawą dokształcania kadr nowo utworzonych komórek do walki z cyberprzestępczością w strukturach organizacyjnych polskiej Policji i prokuratury.

Inaczej przedstawiają się oferty uczelni w aspekcie kształcenia specjalistów ds. cyberbezpieczeństwa, które najczęściej pojawiają się na kierunkach studiów: bezpieczeństwo narodowe i bezpieczeństwo wewnętrzne. Uwidacznia się zatem tendencja wdrażania przez większość uczelni programu kształcenia czy to specjalnościowego, czy podyplomowego w zakresie cyberbezpieczeństwa, a nie cyberprzestępczości. Za tą obserwacją przemawia fakt, że ofertę kształcenia w zakresie cyberbezpieczeństwa traktować można w szerszym zakresie i kierować ją do większej grupy odbiorców.

Tylko należycie wykształcone kadry w zakresie cybeprzestępczości czy też cyberbezpieczeństwa przyczynią się do zwiększenia efektywności podejmowanych czynności procesowych i operacyjnych oraz poszerzenia współpracy organów ścigania z innymi podmiotami, które mają już wiedzę w zakresie istoty cyberprzestępstwa lub mogą przyczynić się do ustalenia jego sprawcy.

[43] Badania przeprowadzono od 1 marca do 30 maja, tj. w okresie wdrażania nowych programów w profilach kształcenia na nowy rok akademicki, w czasie przyjmowania programów przez rady podstawowych jednostek organizacyjnych uczelni.

Dotyczy to głównie współpracy z wykwalifikowanymi w zakresie cyberprzestępczości czy też cyberbezpieczeństwa krajowymi oraz międzynarodowymi podmiotami prywatnymi, szczególnie z sektora telekomunikacyjnego, bankowego oraz ubezpieczeniowego, ale także odpowiednich działań edukacyjnych społeczeństwa w ramach profilaktyki cyberprzestępczości.

Streszczenie

Niedobór specjalistów ds. zwalczania cyberprzestępczości oraz cyberbezpieczeństwa jest obecnie poważnym utrudnieniem z uwagi na bardzo szybko rozwijającą się branżę IT i zasobów Internetu oraz wzrastającą skalę cyberprzestępstw. Firma Cisco Networking Academy, zajmująca się od 20 lat edukacją przyszłych specjalistów IT, szacuje, że obecnie w Polsce brakuje ich ok. 50 tys.[44] Dynamiczny rozwój trendów technologicznych, takich jak IoT, *big data*, cyberbezpieczeństwo, automatyka, a co za tym idzie – cyberprzestępczości, sprawia, że wzrasta zapotrzebowanie na nowy rodzaj ekspertów znających nowe dziedziny, takie jak: technologie chmurowe, automatyka, architektura sieci, analityka, rozpoznawanie, wykrywanie, ujawnianie i zwalczanie cyberprzestępstw, techniki analizy Internetu, w tym Darknetu; informatyka śledcza i dowody w postaci elektronicznej, bezpieczeństwo sieci i systemów informatycznych i szereg innych. Z uwagi na specyfikę i ważność tematyki niniejszy artykuł poświęcony został problematyce kształcenia specjalistów w dziedzinie zwalczania cyberprzestępczości. W opracowaniu zwrócono uwagę na zdiagnozowanie aktualnej problematyki cyberprzestępczości; prawnokarną klasyfikację terminu cyberprzestępczość; tworzenie w Polsce nowych działów i biur do walki z cyberprzestępczością w ramach organów ścigania i wymiaru sprawiedliwości; diagnozę potrzeb kształcenia specjalistów ds. zwalczania cyberprzestępczości w *Polityce Cyberbezpieczeństwa RP na lata 2017–2022*. W celu zweryfikowania obecnego stanu i przygotowania polskiego rynku edukacyjnego na potrzeby kształcenia ekspertów ds. cyberprzestępczości przeprowadzono analizę oferty kształcenia polskich uczelni.

Słowa kluczowe: cyberprzestępczość, edukacja i profilaktyka w zapobieganiu cyberprzestępczości, prawo karne, kryminalistyka, biuro ds. walki z cyberprzestępczością, branża IT, trendy technologiczne, zasoby Internetu

Summary

The shortage of specialists in the fight against cybercrime and cybersecurity is currently a serious obstacle due to the rapidly growing IT industry and Internet resources as well as the growing scale of cybercrime. Cisco Networking Academy, which has been educating future IT specialists for 20 years, estimates that there are currently

[44] DLP Expert, „Data Leak Prevention" 2017, nr 4 (23), styczeń 2018, s. 9.

about 50,000 missing in Poland. Dynamic development of technological trends, such as IoT (Internet of Things), big data, cyber security, automation and even cybercrime, make demand for a new type of experts familiar with new areas, such as: cloud automation technologies, network architecture, analytics, recognition, detection, disclosure and fight against cybercrime, Internet analysis techniques including Darknet; forensics and evidence in electronic form, security of networks and information systems, and many others. Due to the specificity and importance of the subject, this article is devoted to the training of specialists in combating cybercrime. In the study, the Author drew attention to: diagnosing the current issue of cybercrime; legal and criminal classification of the term cybercrime; creating new departments and offices in Poland to fight cybercrime of law enforcement and justice authorities; diagnosis of the training needs of specialists in combating cybercrime in the Cybersecurity Policy of the Republic of Poland for 2017–2022. The Author, in order to verify the current state and prepare the educational market for the needs of educating cybercrime experts, has analyzed the offer of education at Polish universities.

Keywords: cybercrime, education and prevention of cybercrime, criminal law, criminalistics, office for combating cybercrime, IT, technological trends, internet resources

Bibliografia

Literatura

DLP Expert, „Data Leak Prevention" (kwartalnik) 2017, nr 4 (23), styczeń 2018.

Gwoździewicz S., *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej oraz Strategia na rzecz lepszego internetu dla dzieci w działaniach prawnych Unii Europejskiej na lata 2014–2020 (The European Union Cybersecurity Strategy and better Internet for children in European Union Legal Action for 2014–2020)*, w: *Принципи і тенденції застосування приватного права ЄС і постадянських країн* (*Zasady i tendencje stosowania prawa prywatnego UE w krajach postradzieckich*), Taras Shevchenko National University of Kyiv, Faculty of Law, Department of Civil Law, Kyiv 2018.

Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Wolters Kluwer, Warszawa 2016.

Raport roczny z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego Internetu 2016, NASK/CERT Polska, Warszawa 2016.

Sawicki M., *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013.

Wasilewski J., *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15 (8).

Źródła

Konwencja Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r.

Komunikat Wspólny Komisji Europejskiej, Wysokiego Przedstawiciela UE do spraw Zagranicznych i Polityki Bezpieczeństwa do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 07.02.2013 r., *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*, Bruksela 2013.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. 1997 Nr 133, poz. 883).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 1994 Nr 24, poz. 83).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz.U.2017.0.2067 t.j.).

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022: poszanowanie praw i wolności w cyberprzestrzeni, kompleksowe podejście do cyberbezpieczeństwa istotnym elementem polityki państwa, Ministerstwo Cyfryzacji, Warszawa 2017.

Rozporządzenie Ministra Sprawiedliwości z dnia 7 kwietnia 2016 r. – Regulamin wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury (Dz.U. 2016, poz. 508).

Zarządzenie nr 17 Komendanta Głównego Policji z dnia 18 listopada 2016 r. zmieniające zarządzenie w sprawie regulaminu Komendy Głównej Policji (Dz.Urz. KGP z 2016 r., poz. 69).

Uchwała nr 23/000/2018 Senatu AJP z dnia 24 kwietnia 2018 r. w sprawie utworzenia studiów pierwszego stopnia na kierunku kryminologia stosowana – profil praktyczny, http://bip.ajp.edu.pl/ [dostęp: 24.05.2018].

Zarządzenie nr 1/0101/2018 Rektora AJP z dnia 16 stycznia 2018 r. w sprawie powołania Zespołu ds. przygotowania wniosku o nadanie uprawnień do prowadzenia studiów pierwszego stopnia na kierunku kryminologia stosowana – profil praktyczny, http://bip.ajp.edu.pl/ [dostęp: 20.03.2018].

Internet

https://www.computerworld.pl [dostęp: 26.05.2018].

https://wsaib.pl/kandydaci/studia-ii-stopnia/bezpieczenstwo-wewnetrzne/cyberprzestepczosc [dostęp: 24.05.2018].

http://www.wspia.eu/dla-kandydata/kierunki-studiow/kierunek-prawo/prawo/cyberprzesteczosc [dostęp: 24.05.2018].

https://www.wspol.edu.pl/g/images/2017/dokumenty/oferta_studiow_podyplom_na_wbw_w_zakr_cyber.pdf [dostęp: 24.05.2018].

https://www.ka.edu.pl/csp-oferta/specjalista-ds-cyberprzestepczosci/ [pobrane w dniu 15.03.2018 r.]

https://www.wsb.pl/gdansk/studenci/studia-podyplomowe/kierunki/cyberprzestepczosc [dostęp: 24.05.2018].

http://www.vistula.edu.pl/kierunki-studiow/kontynuacja-edukacji/studia-podyplomowe/informatyka/agent-ds-cyberprzestepczosci/ [dostęp: 30.03.2018].

http://www.uczelnie.info.pl/PL-H10/aktualnosc/5693/studia-podyplomowe-w-warszawie-cyberprzestepczosc-na-uczelni-lazarskiego.html [dostęp: 12.04.2018 r.]
http://podyplomowe.wsh.pl/wp-content/uploads/2017/05/cyberprzestepczosc.pdf [dostęp: 28.04.2018].