W raporcie z wizytacji wskazano, że podstawową formą jest terapia indywidualna zamiast grupowej. Zwrócono także uwagę na fakt, iż osadzeni nie mają zaufania do terapeutów, skoro nie jest przestrzegana zasada poufności, a podawane przez nich w czasie terapii →informacje są później zamieszczane w aktach, dostępnych dla wielu osób.

Wątpliwości natury prawnej budzi sposób przedłużania pobytu w ośrodku. Obecnie nie jest wymagane wydanie w tym zakresie orzeczenia przez sąd ani też udział w posiedzeniu osadzonego czy jego obrońcy. Oznacza to, iż osadzony nie ma możliwości zaskarżenia decyzji sądu, albowiem środki odwoławcze przysługują wyłącznie w odniesieniu do orzeczeń. Standardy przyjęte w ustawie słabiej gwarantują ochronę praw i wolności osadzonych niż regulacje dotyczące pobytu niepoczytalnych sprawców przestępstw w szpitalach psychiatrycznych.

Od czasu utworzenia ośrodka na liczne mankamenty jego funkcjonowania oraz na konieczność uzupełniania i zmiany przepisów uwagę zwracał Rzecznik Praw Obywatelskich, do potrzebnych zmian jednak nie doszło.

Anna Pacholska

A. Depko, K. Eichstaedt, P. Gałecki, *Metodyka pracy biegłego psychiatry, psychologa oraz seksuologa w sprawach karnych, nieletnich oraz wykroczeń*, Wolters Kluwer Polska, Warszawa 2017; Raport przedstawicieli Krajowego Mechanizmu Prewencji Tortur z wizytacji Krajowego Ośrodka Zapobiegania Zachowaniom Dyssocjalnym w Gostyninie, RPO.gov.pl (dostęp 8.02.2020); Rozporządzenie Ministra Zdrowia z dnia 16 stycznia 2014 r. w sprawie Krajowego Ośrodka Zapobiegania Zachowaniom Dyssocjalnym, Dz. U. 2016.1480 t.j.; K. Żaczkiewicz-Zborska, *Bezterminowy pobyt w ośrodku dla groźnych przestępców zgodny z Konstytucją RP*, LEX/el. 2017; Ustawa z dnia 22 listopada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób, Dz. U. 2019.2203.

KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA – działa w Polsce od 28 sierpnia 2018 r. na mocy przepisów Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Próby wypracowania efektywnej polityki zapewnienia →bezpieczeństwa [t. 1] w →cyberprzestrzeni [t. 1] rozpoczęły się w Polsce w 2008 r. wraz z uchwaleniem

Rządowego programu ochrony cyberprzestrzeni RP na lata 2009–2011. Niewątpliwie asumptem do opracowania programu były ratyfikacja przez Polskę 16 maja 2005 r. konwencji Rady Europy o zapobieganiu → terroryzmowi [t. 4], a także ataki cybernetyczne wymierzone w Estonię w 2007 i Gruzję w 2008 r. Wówczas większość państw europejskich podjęła próbę wdrożenia → strategii [t. 4] i doktryn w zakresie → cyberbezpieczeństwa [t. 1]. Jednakże dopiero ustawa z 2018 r. nadała realny kształt systemowi i w pełni umożliwiła jego funkcjonowanie.

Zgodnie z art. 3 wspomnianego aktu prawnego polski system cyberbezpieczeństwa ma zapewnić bezpieczeństwo cyberprzestrzeni Rzeczypospolitej Polskiej. Generalnie chodzi głównie o zagwarantowanie ciągłości świadczenia usług kluczowych, a więc tych o szczególnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej. Usługi te zostały wskazane w załączniku do Rozporządzenia Rady Ministrów z 11 września 2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych (generowanie i dystrybucja energii elektrycznej, administrowanie infrastrukturą energetyczną, produkcja paliw ciekłych bądź utrzymywanie rezerw strategicznych i zapasów ropy naftowej, produktów naftowych oraz gazu ziemnego itp.). Ponadto system cyberbezpieczeństwa odpowiada również za utrzymanie ciągłości świadczenia usług cyfrowych świadczonych elektronicznie (np. internetowe platformy handlowe, usługi przetwarzania w chmurze, wyszukiwarki internetowe). Ustawodawcy chodziło o stworzenie spójnego i efektywnego systemu odpowiedzialnego za szeroko pojęte cyberbezpieczeństwo. Przepisy ustawy wyraźnie sformułowały zakres odpowiedzialności podmiotów i instytucji, których aktywność w tym zakresie ma zapewnić lepszą wykrywalność, zapobieganie oraz minimalizowanie skutków wszelkich incydentów sieciowych, zarówno awarii, jak i ataków sieciowych. Na mocy ustawy z 2018 r. implementowano zatem zharmonizowany mechanizm pozwalający wykrywać, powiadamiać oraz reagować w obliczu potencjalnych → cyberzagrożeń [t. 1].

Bezpieczeństwo w cyberprzestrzeni jest pojmowane w kategoriach bezpieczeństwa przesyłu oraz wymiany danych i → informacji (rozumianych jako treści cyfrowe). Z cyberbezpieczeństwem wiąże się również bezpieczne świadczenie usług na odległość za pośrednictwem systemów

informatycznych. Wspomniane usługi są realizowane przez operatorów usług kluczowych o istotnym znaczeniu dla bezpieczeństwa państwa i jego obywateli oraz usług świadczonych na indywidualne żądanie użytkowników internetu przez dostawców usług cyfrowych.

W myśl przepisów ustawy z 2018 r. utrzymanie cyberbezpieczeństwa na poziomie krajowym mają zapewnić właściwie funkcjonujące systemy informacyjne, świadcząc usługi kluczowe i cyfrowe oraz zapewniające obsługę incydentów. Tak skonstruowany krajowy system cyberbezpieczeństwa pozwolił wygenerować swoistą przestrzeń, dzięki której jest możliwa skuteczna i skoordynowana współpraca pomiędzy podmiotami świadczącymi usługi cyfrowe a organami i instytucjami państwowymi właściwymi w zakresie cyberbezpieczeństwa. W ustawie w sposób enumeratywny wyszczególniono kilkanaście kategorii podmiotów krajowego systemu cyberbezpieczeństwa, do których zaliczono:

- operatorów usług kluczowych;
- dostawców usług cyfrowych;
- zespoły reagowania na incydenty bezpieczeństwa komputerowego (ang. Computer Security Incident Response Team, CSIRT), działające na poziomie krajowym, powołane w: Ministerstwie Obrony Narodowej (CSIRT MON), Naukowej i Akademickiej Sieci Komputerowej Państwowym Instytucie Badawczym (CSIRT NASK) oraz w →Agencji Bezpieczeństwa Wewnętrznego [t. 1] (CSIRT GOV);
- sektorowe zespoły cyberbezpieczeństwa (np. utworzone przez →organy właściwe do spraw cyberbezpieczeństwa [t. 3]);
- podmioty publiczne, w tym jednostki sektora finansów publicznych (organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały; jednostki samorządu terytorialnego oraz ich związki; związki metropolitalne; jednostki budżetowe; samorządowe zakłady budżetowe; agencje wykonawcze; instytucje gospodarki budżetowej; Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasę Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez prezesa Kasy Rolniczego Ubezpieczenia Społecznego; Narodowy Fundusz Zdrowia; uczelnie

publiczne; Polską Akademię Nauk i tworzone przez nią jednostki organizacyjne, instytuty badawcze, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polską Agencję Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, spółki prawa handlowego realizujące zadania użyteczności publicznej na rzecz bieżącego i permanentnego zaspokajania zbiorowych potrzeb ludności w drodze świadczenia usług dostępnych na zasadzie powszechności;

- podmioty świadczące usługi z zakresu cyberbezpieczeństwa;
- organy właściwe do spraw cyberbezpieczeństwa;
- Pojedynczy Punkt Kontaktowy ds. cyberbezpieczeństwa;
- Pełnomocnika Rządu ds. Cyberbezpieczeństwa;
- Kolegium do Spraw Cyberbezpieczeństwa.

Za operatorów usług kluczowych uznano firmy działające w określonych sektorach:

- finansowym (banki krajowe i zagraniczne wraz z oddziałami, spółdzielcze kasy oszczędnościowo-kredytowe);
- energetycznym (przedsiębiorstwa z koncesją na wykonywanie działalności gospodarczej w zakresie wytwarzania paliw ciekłych, przesyłania ropy naftowej, wytwarzania paliw syntetycznych, przetwarzania albo magazynowania energii elektrycznej, wydobywania gazu ziemnego);
- transportowym (firmy specjalizujące się w transporcie lotniczym i kolejowym oraz podmioty z zakresu transportu drogowego);
- →ochrony zdrowia [t. 3] (podmioty lecznicze, wytwórcy produktów leczniczych, przedsiębiorcy prowadzący apteki lub hurtownie farmaceutyczne);
- zaopatrzenia w wodę pitną (przedsiębiorstwa wodno-kanalizacyjne).

Aby krajowy system cyberbezpieczeństwa stanowił efektywny mechanizm zabezpieczający przed cyberzagrożeniami, powołano tzw. system zarządzania cyberbezpieczeństwem, który w Polsce obejmuje poziom roboczy, za który odpowiada Zespół ds. Obsługi Incydentów Krytycznych,

oraz poziom instytucjonalny, reprezentowany przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa i Kolegium ds. Cyberbezpieczeństwa.

Zespół ds. Obsługi Incydentów Krytycznych pełni funkcję pomocniczą w sprawach obsługi incydentów zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV. Jest również organem koordynującym działania podejmowane przez CSIRT MON, CSIRT NASK, CSIRT GOV i → Rządowe Centrum Bezpieczeństwa [t. 3]. W gremium tym zasiadają przedstawiciele CSIRT MON, CSIRT NASK, szefa Agencji Bezpieczeństwa Wewnętrznego (ABW) realizującego zadania w ramach CSIRT GOV oraz Rządowego Centrum Bezpieczeństwa (RCB). Prace Zespołu są obsługiwane przez RCB, którego dyrektor przewodniczy tymże pracom.

Pełnomocnik Rządu ds. Cyberbezpieczeństwa koordynuje działania i realizuje politykę rządu w zakresie cyberbezpieczeństwa. Analizuje zatem i prowadzi ocenę funkcjonowania krajowego systemu cyberbezpieczeństwa. Sprawuje również nadzór nad procesem zarządzania ryzykiem systemu cyberbezpieczeństwa RP, opiniuje dokumenty rządowe, upowszechnia innowacyjne rozwiązania służące zapewnieniu cyberbezpieczeństwa, inicjuje krajowe ćwiczenia z zakresu cyberbezpieczeństwa oraz na wniosek CSIRT rekomenduje stosowanie określonych urządzeń informatycznych lub oprogramowania. Ponadto pełnomocnik współpracuje w zakresie cyberbezpieczeństwa z innymi państwami, instytucjami czy też organizacjami międzynarodowymi, wspiera badania naukowe z obszaru bezpieczeństwa w sieci oraz angażuje się w prace zmierzające do podniesienia poziomu świadomości społeczeństwa, zwłaszcza w zakresie bezpiecznego korzystania z internetu oraz ryzykownych działań z tym związanych.

Natomiast Kolegium ds. Cyberbezpieczeństwa jest organem opiniodawczo-doradczym w sprawach cyberbezpieczeństwa oraz aktywności CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa, a także organów właściwych do spraw cyberbezpieczeństwa. Kolegium składa się z: Prezesa Rady Ministrów (przewodniczącego Kolegium), Pełnomocnika Rządu ds. Cyberbezpieczeństwa, ministra ds. wewnętrznych, ministra ds. informatyzacji, ministra obrony narodowej, ministra ds. zagranicznych, szefa Kancelarii Prezesa Rady Ministrów, szefa → Biura Bezpieczeństwa Narodowego [t. 1], ministra odpowiedzialnego za koordynację → służb specjalnych [t. 4] lub

osoby przez niego upoważnionej (jeśli nie został wyznaczony odpowiedni minister, to jego miejsce zajmuje szef ABW). W obradach Kolegium uczestniczą również osoby bezpośrednio lub pośrednio odpowiedzialne za zapewnienie bezpieczeństwa państwa, m.in. dyrektor RCB, szef ABW (bądź jego zastępca), szef → Służby Kontrwywiadu Wojskowego [t. 4] (bądź jego zastępca), a także dyrektor NASK.

Struktura krajowego systemu cyberbezpieczeństwa wydaje się logiczna i uzasadniona, bowiem za efektywność systemu odpowiadają zespoły reagowania na incydenty bezpieczeństwa komputerowego funkcjonujące na poziomie krajowym, a zatem CSIRT MON, CSIRT NASK oraz CSIRT GOV. Każdy z tych zespołów realizuje swoje ustawowe obowiązki w konkretnym obszarze: CSIRT MON w obszarze wojskowym, a CSIRT NASK cywilnym. CSIRT GOV działa na poziomie administracji publicznej. Daje się jednak zauważyć deficyt zespołów reagowania na incydenty w obszarach bezpośrednio związanych z → infrastrukturą krytyczną, stanami nadzwyczajnymi oraz atakami terrorystycznymi. Wątpliwa jest także reakcja poszczególnych sektorów na potencjalne incydenty, zwłaszcza chodzi o sektor ochrony zdrowia, transportu czy też zaopatrzenia w wodę pitną.

Utworzenie krajowego systemu cyberbezpieczeństwa w Polsce było podyktowane koniecznością wdrożenia do polskiego porządku prawnego postanowień Dyrektywy 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 (Network and Information Systems Directive, dyrektywa NIS). Jednak dyrektywa NIS nie ograniczała państw członkowskich UE konkretnymi rozwiązaniami w zakresie cyberbezpieczeństwa, pozwalając tym samym na dowolność w kwestii wyboru właściwego modelu organizacji systemu odpowiedzialnego za zapewnienie bezpieczeństwa w cyberprzestrzeni.

Powołane przepisami ustawy z 2018 r. zespoły ds. bezpieczeństwa komputerowego i reagowania na incydenty wywodzą się od zespołów uruchomionych pod koniec lat 80. XX w. W 1988 r. miała miejsce jedna z poważniejszych w skutkach epidemia tzw. robaka Morrisa (Morris Worm), który zainfekował globalne systemy informatyczne. W odpowiedzi na atak podjęto prace nad skonstruowaniem systemu właściwego

reagowania na incydenty w obszarze bezpieczeństwa informatycznego. Agencja Zaawansowanych Projektów Badawczych w Obszarze Obronności (ang. Defence Advanced Research Projects Agency, DARPA) powołała w Uniwersytecie Carnegiego i Mellonów w Pittsburgu pierwszy specjalistyczny zespół CSIRT – Centrum Koordynacji CERT (Computer Emergency Response Team). Zespoły zaczęły również powstawać w Europie. Pierwszy z nich – SURFnet-CERT – został powołany w 1992 r. z inicjatywy holenderskiego dostawcy usług internetowych. Zespół funkcjonował w ramach ośrodków akademickich. Nowo powstające CERT coraz szybciej uzyskały miano prężnie działających jednostek specjalizujących się nie tylko w skutecznym reagowaniu na pojawiające się incydenty, ale również świadczące usługi prewencyjne i szkoleniowe. Ewolucja zespołów CERT i coraz wyższy poziom ich specjalizacji przyczyniły się do wprowadzenia nowego terminu – CSIRT.

Julia Anna Gawęcka

J. Gawęcka, *Krajowy system cyberbezpieczeństwa*, [w:] *Vademecum bezpieczeństwa informacyjnego*, t. 1: *A–M*, O. Wasiuta, R. Klepka (red.), AT Wydawnictwo, Wydawnictwo Libron, Kraków 2019; *Krajowy system cyberbezpieczeństwa*, gov.pl (dostęp 25.03.2019); *Krajowy system cyberbezpieczeństwa*, KSOIN.pl (dostęp 26.03.2019); M. Maj, *Pięć kluczowych wyzwań przy wdrożeniu Ustawy o krajowym systemie cyberbezpieczeństwa*, 13.07.2018, CyberSecurity.org (dostęp 23.03.2019); *The Morris Worm. 30 Years Since First Major Attack on the Internet*, 2.10.2018, FBI.gov (dostęp 25.03.2019); Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018, poz. 1560.

KRYMINALISTYKA – nauka, która przy zastosowaniu taktyki i techniki śledczej stawia sobie za cel optymalne wypracowanie metod ustalenia faktu popełnienia przestępstwa, sposobów działania sprawcy bądź sprawców, ich identyfikacji, zabezpieczenia i zebrania dowodów potwierdzających ich winę i określających stopień przyczynienia się do zaistnienia przestępstwa oraz zapobiegania czynom przestępczym i → patologiom społecznym [t. 3].

Przy tak szerokim spektrum zainteresowań badawczych w kryminalistyce można wyodrębnić kilka działów. Jednym z nich jest taktyka