Zeszyty Naukowe Gdańskiej Szkoły Wyższej
ISSN 2300-9055 2018, Nr 3(20), s. 133–146
Kwartalnik DOI 10.24426/zngsw.v20i3.143

Jerzy Kosiński
Akademia Marynarki Wojennej w Gdyni

Próba prognozy cyberprzestępczości w Polsce w roku 2018

Streszczenie
W artykule podjęto próbę prognozy cybearprzestępczości w Polsce w 2018 roku. Opisano pojęcie cyberprzestępczości i jej interpretację w Kodeksie karnym. Do prognozowania wykorzystano trend liniowy i metodę Holta.

Słowa kluczowe: cyberprzestępczość, prognozowanie, trend liniowy, metoda Holta.

Jednym z większych wyzwań związanych z bezpieczeństwem, nie tylko wewnętrznym, jest zagrożenie cyberprzestępczością. W najbliższej perspektywie czasowej można przewidywać dalszą eskalację cyberprzestępczości oraz wykorzystania cyberprzestrzeni przez przestępców.

Pojęcie cyberprzestępczości można interpretować wielorako, np. opierając się na Konwencji Rady Europy z dnia 23 listopada 2001 r. o cyberprzestępczości (pobrane z: http://www.uncjin.org/Documents/congr10/10e.pdf). Konwencja zawiera definicje czterech rodzajów przestępstw komputerowych:

1) przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych oraz systemów,
2) przestępstwa fałszerstwa i oszustwa komputerowego,
3) przestępstwa związane z pornografią dziecięcą,
4) przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych.

Uzupełnieniem konwencji jest Protokół Dodatkowy do Konwencji dotyczący czynów przestępczych o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych (pobrane z: http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=8&DF=&CL=ENG).

Warto w tym momencie zwrócić uwagę na niejednoznaczność, niespójność i niezrozumiałość (więcej w: Kosiński, 2015, s. 31–45; Liderman, 2011, s. 401–409) pojęć zaczynających się od przedrostka „cyber-". Z punktu widzenia nauk społecznych i prawnych wystarczające będzie jednakowe interpretowanie tych pojęć bez ich jednoznacznego opisania. Jednak i tutaj niezbędne jest spójne podejście do kwestii znamion cyberprzestępstwa pozwalające na reakcję, a także na lepszą współpracę i koordynację zwalczania. Pojęcie cyberprzestępczości jest pojęciem wieloznacznym. Powstało z połączenia przedrostka „cyber-" i słowa „przestępczość". Zatem należy je rozumieć

jako działania przestępcze związane z czymś, co określa przedrostek „cyber-". Jest to idealny medialny prefiks — większość czytelników i słuchaczy nie ma pojęcia, co znaczy, ale może poprzedzać dowolne słowo, aby całość wydawała się nowa, atrakcyjna i jednocześnie dziwna, straszna lub, co najgorsze, naukowa. Przedrostek „cyber-" jest nadużywany i zwykle powoduje duży kłopot ze zdefiniowaniem określanych pojęć. Według Słownika języka polskiego „cyber-" to „pierwszy człon wyrazów złożonych wskazujący na ich związek z informatyką, a zwłaszcza z Internetem" (pobrane z: http://sjp.pwn.pl/slownik/2553911/cyber-; identycznie słowniki: Merriam-Webster, Oxford Dictionaries, Cambridge Dictionary). Używany w mediach, przez tłumaczy i polityków przedrostek „cyber-" często wywodzi się od słowa „cybernetyka". Wydaje się jednak, że takie proste powiązanie znaczeń nie jest uprawnione. Według Słownika języka polskiego (pobrane z: https://sjp.pwn.pl/sjp/;2553914) „cybernetyka" to nauka o procesach sterowania oraz przekazywania i przekształcania informacji w systemach takich jak, np. maszyna, organizm żywy, społeczeństwo[1]. Tym samym określenie „przestępstwa cybernetyczne", często używane przez polityków, w tłumaczeniach i literaturze wojskowej, wydaje się kompletnie niewłaściwe.

Czytając w mediach i na portalach informacje:

- „Wtorkowy atak cybernetyczny był podobny do tego sprzed miesiąca" (*Szef MON: atak cybernetyczny groźny ze względu na cel*, 2017),
- „System zapewniania bezpieczeństwa cybernetycznego w Polsce działa" (*Po globalnym cyberataku premier zwołała nadzwyczajne spotkanie. Znamy decyzję ws. stopnia alarmowego*, 2017),
- „Bezpieczeństwo cybernetyczne: jest porozumienie z Parlamentem" (pobrane z: http://www2.consilium.europa.eu/pl/press/press-releases/2015/12/08/improve-cybersecurity/),
- „Premier Beata Szydło po ostatnich atakach cybernetycznych: Nie podwyższamy stopnia alarmowego" (2017),

trudno skojarzyć je z oszustem, który za pomocą poczty elektronicznej przysłał nam fałszywą informację lub próbował uniemożliwić nam dostęp do danych zapisanych w komputerze. Skojarzenie idzie w stronę mniej lub więcej człekokształtnych żołnierzy albo robotów wojskowych (Ficoń, 2013, s. 377–386 i 422–426).

Zasadą powinna być, nie tylko „brzytwa Okhama"[2], mówiąca, że nie należy wprowadzać nowych pojęć, kategorii czy bytów, jeśli nie jest to uzasadnione, ale także nienadawanie nowych znaczeń już zdefiniowanym pojęciom. Zatem nie używajmy w tym kontekście przymiotnika cybernetyczny. Znacznie lepiej, chociaż również nie zawsze zrozumiale, jest dodawać wyłącznie przedrostek „cyber-" w jego słownikowym znaczeniu. Oczywiście podejście cybernetyczne do cyberprzestępczości warto stosować i korzystać ze znamiennego dla cybernetyki stosowania metody analogii, polegającej na dopatrywaniu się wspólnych cech w różnych tworach, a w szczególno-

[1] Wiele innych definicji i określeń cybernetyki można znaleźć na stronach Amerykańskiego Towarzystwa Cybernetycznego, http://www.asc-cybernetics.org/foundations/definitions.htm.

[2] Łac. *Non sunt multiplicanda entia sine necessitate* — bytów nie mnożyć, fikcyj nie tworzyć, tłumaczyć fakty jak najprościej.

ści metody modelowania, w której chodzi o wspólne cechy tworu naturalnego i jego modelu (Mazur, 1966, s. 13).

Można dyskutować, czy należy tworzyć nowe kategorie przestępstw w zależności od narzędzi, sprzętu lub mechanizmu, za pomocą których zostały one popełnione. Przecież nie tworzy się kategorii przestępstw samochodowych, nożowych lub pistoletowych. Jednakże, ze względu na charakter i różnorodność metod, technik i narzędzi popełniania cyberprzestępstw, które odróżniają je od klasycznych przestępstw oraz ich dużą liczbę, należy taką kategorię wprowadzić.

Cyberprzestępczość może być rozumiana w wąskim znaczeniu (przestępczość komputerowa) obejmującym każde nielegalne zachowania realizowane za pomocą działań elektronicznych nakierowanych na bezpieczeństwo systemów komputerowych i danych w nich przetwarzanych. Można także cyberprzestępczość rozumieć w szerokim znaczeniu (przestępczość związana z komputerami) — jako wszelkie nielegalne zachowania popełnione za pomocą lub względem systemu komputerowego czy sieci, w tym takie przestępstwa jak nielegalne posiadanie, oferowanie lub rozpowszechnianie informacji za pomocą systemu komputerowego lub sieci (*Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Crimes related to computer networks*, 2000). Tak rozumiana cyberprzestępczość mieści się w obszarze od przestępstw gospodarczych, takich jak: oszustwa, fałszerstwa, szpiegostwo przemysłowe, sabotaż i wymuszenia, poprzez piractwo komputerowe i inne przestępstwa przeciwko własności intelektualnej oraz przypadki naruszenia prywatności, propagację nielegalnych i szkodliwych treści, ułatwianie prostytucji i inne przestępstwa przeciwko moralności, aż do przestępczości zorganizowanej. Tę drugą granicę wyznacza także cyberterroryzm obejmujący ataki na bezpieczeństwo publiczne, życie i walkę elektroniczną skierowaną przeciwko infrastrukturze krytycznej. W pojęciu cyberterroryzmu, tak jak w cyberprzestępczości, przedrostek „cyber" odnosi się do popełnienia przestępstwa związanego z nowymi technologiami informacyjnymi lub wykorzystania cyberprzestrzeni do tradycyjnych działań (np. planowania, komunikacji, prowadzenia wywiadu, działań logistycznych i finansowych).

Zwykle przyjęło się mówić, że cyberprzestępczość jest jednym z cyberzagrożeń, które obejmują nieuprawnione zachowania skierowane na uzyskanie dostępu, pozyskanie, manipulowanie lub utratę integralności, poufności i dostępności danych, aplikacji czy systemu komputerowego. W obszarze cyberzagrożeń znajdują się ponadto m.in.: cyberterroryzm, cyberszpiegostwo i wojna elektroniczna. Cyberzagrożenia rozpatrywane są w kontekście cyberbezpieczeństwa rozumianego jako bezpieczeństwo połączonych globalnie systemów informacyjnych (np. infrastruktura internetu), sieci telekomunikacyjnych, systemów komputerowych i systemów sterowania przemysłowego. Naruszenie cyberbezpieczeństwa jest wykorzystywane do wielu działań przestępczych, które powodują znaczące straty materialne i niematerialne organizacji, firm i osób prywatnych. Nie można nie zauważać, że jest to istotny problem także w kontekście bezpieczeństwa wewnętrznego, a tym samym również bezpieczeństwa państwa.

Innym źródłem interpretacji pojęcia cyberprzestępczości może być Komunikat Komisji (KE) do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z dnia 22 maja 2007 r. zatytułowany „W kierunku ogólnej strategii zwalczania cyberprzestęp-

czości", w którym Komisja zwróciła uwagę na brak uzgodnionej definicji cyberprzestępczości i zaproponowała, żeby za cyberprzestępstwa uznać „czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takich sieciom i systemom".

W podręczniku Interpolu z 2007 r. zwraca się szczególną uwagę na cztery obszary, na których koncentruje się aktualnie cyberprzestępczość: hacking, oprogramowanie złośliwe (włącznie z botnetami), piractwo intelektualne, nielegalna zawartość cyfrowych nośników danych.

Specyfika cyberprzestępczości została bardzo trafnie ujęta w raporcie Europolu za 2007 r. (*Europol, High Tech Crimes within EU. Threat Assessment 2007*, 2007). Cyberprzestępstwa są w nim ukazane w dwóch ujęciach — wertykalnym i horyzontalnym. Ujęcie wertykalne dotyczy przestępstw, które są specyficzne dla cyberprzestrzeni i poza nią nie mogą być dokonywane. Wśród nich wyróżniono: hacking (ataki DDoS, botnety, *zombies* itp.), *crimeware* (wirusy, robaki, konie trojańskie itp.), spamming. W ujęciu horyzontalnym znalazły się przestępstwa, których dokonanie zostało znacznie ułatwione przez wykorzystanie technik komputerowych i informatycznych. Za powodujące największe zagrożenia uznano: pornografię dziecięcą, nieuprawnione wykorzystanie kart płatniczych, kradzież tożsamości (phishing), piractwo intelektualne, pranie brudnych pieniędzy za pośrednictwem Internetu (cyberlaundering), cyberterroryzm.

Wskazany powyżej zakres wydawać się może dość wąski, niemniej jednak można do tych czterech kategorii dopasować konkretne artykuły Kodeksu Karnego (KK). Do kategorii przestępstw przeciwko poufności, integralności i dostępności danych informatycznych i systemów będą należały czyny penalizowane z:
- art. 165 — sprowadzenie stanów powszechnie niebezpiecznych dla życia lub zdrowia,
- art. 267 — bezprawne uzyskanie informacji (*hacking*, podsłuch komp.),
- art. 268a — utrudnianie zapoznania się z informacją, niszczenie danych,
- art. 269 — niszczenie, uszkadzanie, usuwanie, zmiana, zakłócanie gromadzenia, przetwarzania danych informatycznych o szczególnym znaczeniu lub ich nośników,
- art. 269a — zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej,
- art. 269b — wytwarzanie, sprzedaż, oferowanie „narzędzi hackerskich".

Do kategorii przestępstw komputerowych należą czyny penalizowane z:
- art. 270 — fałszerstwo komputerowe,
- art. 285 § 1 — oszustwo telekomunikacyjne (ang. *phreaking*),
- art. 287 — oszustwo komputerowe,
- art. 310 — podrabianie lub przerabianie pieniądza, innego środka płatniczego albo dokumentu uprawniającego do otrzymania sumy pieniężnej; wprowadzanie do obrotu, przechowywanie takich środków.

Do kategorii przestępstw związanych z pornografią dziecięcą należą czyny z:
- art. 191a — naruszenie intymności seksualnej; utrwalanie wizerunku nagiej osoby,
- art. 198–204 — seksualne wykorzystanie,
- art. 200a — uwodzenie małoletniego.

Do kategorii przestępstw związanych z naruszeniem praw autorskich i praw pokrewnych należą czyny penalizowane w dwóch artykułach KK:
- art. 278 § 2 — nielegalne uzyskanie programu komputerowego,

– art. 293 — paserstwo programu komputerowego.

Warto zdawać sobie sprawę, że w polskich statystykach policyjnych wyżej wymienionych artykułów nie zawsze można wyróżnić tylko te czyny, które związane są z systemem komputerowym lub siecią teleinformatyczną.

Do prognozowania w niniejszym artykule wykorzystano powszechnie stosowane model: trendu liniowego i liniowy model Holta.

Model trendu liniowego wyrażony jest równaniem:

$$\hat{y}_t = a \cdot t + b$$

gdzie:

$$a = \frac{\sum_{i=1}^{n} (t_i - \overline{t}) \cdot y_{t_i}}{\sum_{i=1}^{n} (t_i - \overline{t})^2}, \; b = \overline{y} - a \cdot \overline{t}$$

Liniowy model Holta wygładzania wykładniczego służy do wygładzania szeregu czasowego, w którym występują tendencja rozwojowa i wahania przypadkowe.

Prognozę na chwilę t wyznacza się następująco:

$$y_t^* (\alpha, \beta) = F_t (\alpha, \beta) + (t - T) \cdot S_T (\alpha, \beta)$$

gdzie:

T — liczba momentów czasu szeregu czasowego branych pod uwagę do budowy prognozy, najczęściej T = t–1,

α i β — dwa parametry wygładzające.

Model Holta opisuje się za pomocą następujących równań:

$$F_{t-1}(\alpha,\beta) = \alpha \cdot y_{t-1} + (1-\alpha) \cdot (F_{t-2}(\alpha,\beta) + S_{t-2}(\alpha,\beta))$$
$$S_{t-1}(\alpha,\beta) = \beta \cdot (F_{t-1}(\alpha,\beta) - F_{t-2}(\alpha,\beta)) + (1-\beta) \cdot S_{t-2}(\alpha,\beta)$$

w których: F_{t-1} odpowiada wygładzonej wartości z prostego modelu wygładzania wykładniczego (ocena wartości średniej na okres t–1), a S_{t-1} to wygładzony przyrost trendu na okres t–1.

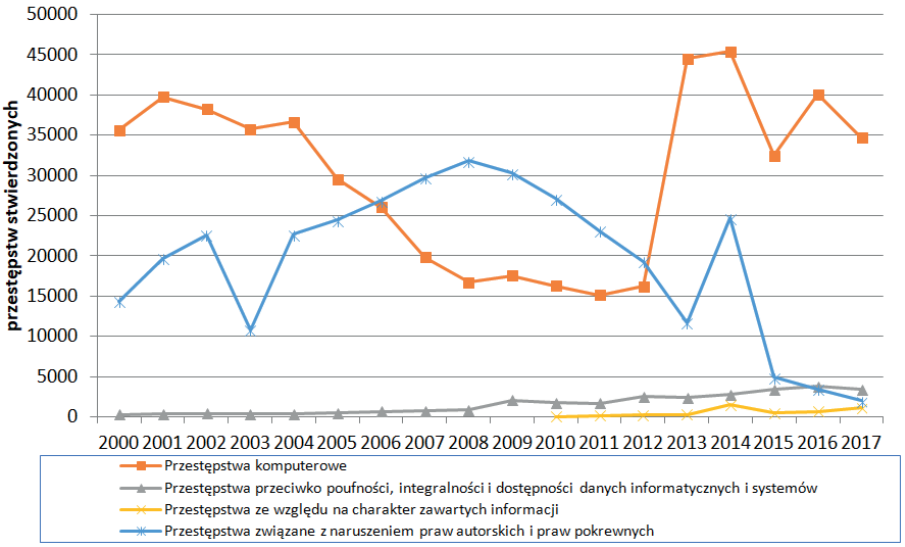
Do budowy modelu Holta potrzebne jest przyjęcie początkowych wartości F_1 i S_1. W niniejszym badaniu przyjmowano dwie ze standardowych propozycji: (1) na podstawie wartości rzeczywistych $F_1 = y_1$, $S_1 = y_2 - y_1$ oraz (2) na podstawie współczynników regresji $F_1 = a$, $S_1 = b$ (nie miało to znaczenia w wartości prognoz, ale (1) prowadziło do mniejszych błędów). Problem znalezienia takiej pary (α*,β*), dla której:

$$s(\alpha^*, \beta) = \min_{\alpha \in [0,1], \beta \in [0,1]} s(\alpha, \beta)$$

gdzie:

$$s(\alpha, \beta) = \sqrt{\frac{1}{n} \sum_{t=1}^{n} \left(y_t - y_t^* (\alpha, \beta) \right)^2}$$

można rozwiązać jedną ze standardowych metod optymalizacji nieliniowej. Stałe wygładzania w badaniu były ustalane kierując się minimalnym błędem średnim prognoz wygasłych.



Rys. 1. Ilość cyberprzestępstw stwierdzonych w latach 2000–2017

Źródło: opracowanie własne na podstawie danych KGP.

Prognoza cyberprzestępczości stwierdzonej na rok 2018 w oparciu o dane z lat 2000–2017 zdominowana jest bardzo nieliniowymi ilościami przestępstw komputerowych i przestępstw związanych z naruszeniami praw autorskich i prac pokrewnych.

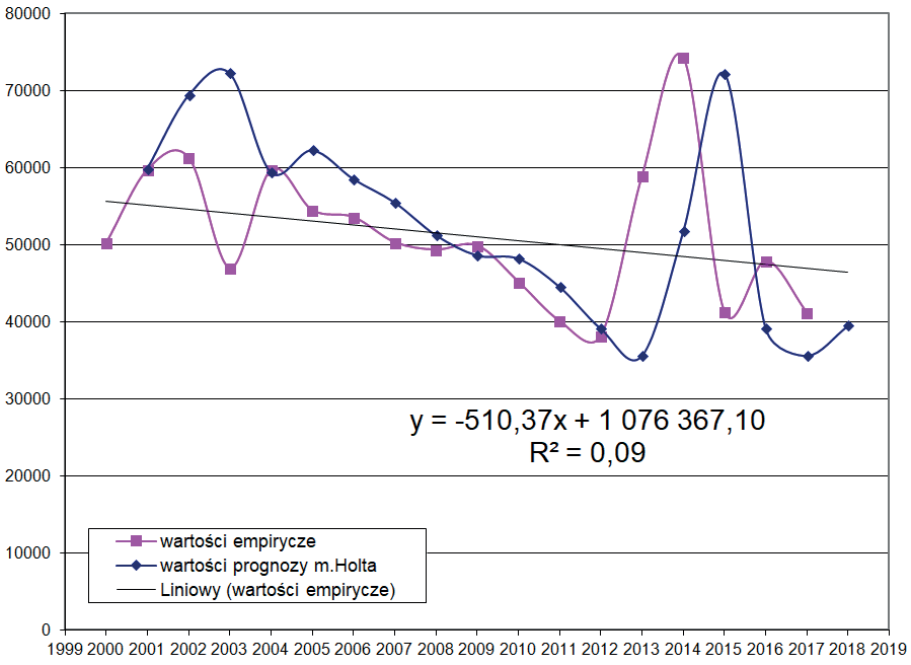
Tabela 1. Prognoza cyberprzestępczości stwierdzonej na rok 2018

Okresy	Wartości rzeczywiste	Wygładzona wartość zmiennej prognozowanej	Wygładzona wartość przyrostu trendu	Prognozy wygasłe	Błąd bezwzględny	Błąd do kwadratu	Błąd względny
Rok	Y_t	F_t	S_t	y_t^*	$(y_t-y_t^*)$	$(y_t-y_t^*)^2$	$(y_t-y_t^*)/y_t$
2000	50289	56132,3725	-510,3725				
2001	59815	59815,0000	9526,0000	59815	0,0000	0,0000	0,00%
2002	61294	64436,3535	7844,6872	69341	8047,0000	64754209,0000	13,13%
2003	46981	56860,6659	2558,5827	72281	25300,0407	640092058,3995	53,85%
2004	59761	59627,5461	2629,9871	59419	341,7514	116794,0291	0,57%
2005	54489	57522,6122	1006,8562	62258	7768,5332	60350107,3272	14,26%
2006	53595	55521,9099	-24,1349	58529	4934,4684	24348978,1029	9,21%
2007	50328	52346,7971	-1104,2901	55498	5169,7750	26726573,8584	10,27%
2008	49373	50103,0425	-1494,8985	51243	1869,5071	3495056,6571	3,79%
2009	49917	49405,8917	-1221,4306	48608	1308,8560	1713104,1019	2,62%
2010	45207	46369,6986	-1843,5312	48184	2977,4611	8865274,6829	6,59%
2011	40128	41845,4844	-2762,4693	44526	4398,1674	19343876,0883	10,96%
2012	38165	38523,4849	-2954,2763	39083	918,0150	842751,5579	2,41%

Okresy	Wartości rzeczywiste	Wygładzona wartość zmiennej prognozowanej	Wygładzona wartość przyrostu trendu	Prognozy wygasłe	Błąd bezwzględny	Błąd do kwadratu	Błąd względny
2013	58907	49793,5925	1921,8425	35569	23337,7914	544652508,1920	39,62%
2014	74357	65515,4689	6652,4941	51715	22641,5650	512640467,2628	30,45%
2015	41329	53371,6150	209,1061	72168	30838,9630	951041637,8823	74,62%
2016	47927	44473,4239	-914,6372	39083	8843,9850	78216070,5095	18,45%
2017	41247	39029,8225	-1767,9778	35569	5677,7914	32237315,3673	13,77%
2018			**Prognoza**	**39479**	**α = 0,6095 β = 0,3428**		

Źródło: opracowanie własne na podstawie danych KGP.

Przedstawiona w tabeli 1 prognoza liczby cyberprzestępstw stwierdzonych obarczona jest dużym procentowym błędem średniokwadratowym (MSE) — 17,91%, co sprawia, że prognoza 39 479 stwierdzonych cyberprzestępstw jest niedopuszczalna. Podobnie jest z prognozą uzyskaną w wyniku obliczenia funkcji trendu, pomimo jej podobnej wartości (46 440) — współczynnik determinacji $R^2 = 0,09$ oznacza, że dopasowanie linii trendu jest niezadawalające. Wizualnie obie prognozy przedstawione są na rysunku 2. Przedstawiony na rysunku 2 malejący trend liczby cyberprzestępstw kłóci się z powszechnym odczuciem i analizami (World Economic Forum, 2018; Europol, 2017).



Rys. 2. Wartości empiryczne oraz prognozy cyberprzestępczości stwierdzonej

Źródło: opracowanie własne na podstawie danych KGP.

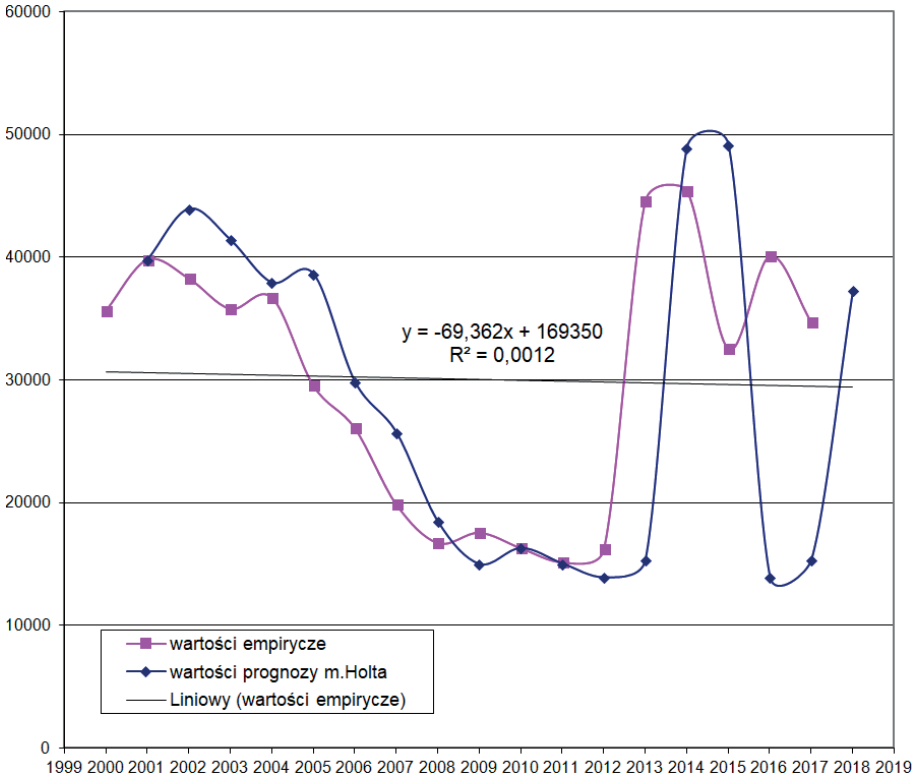
Prognozy oparte o dane z krótszych okresów, ostatnich 10 lub 5 lat obaczone są jeszcze większym błędem. Jak na początku artykułu wspomniano, cyberprzestępczość można podzielić na cztery kategorie, wobec czego warto zweryfikować prognozy dla każdej z kategorii osobno.

Tabela 2. Prognoza przestępczości komputerowej stwierdzonej na rok 2018

Okresy	Wartości rzeczywiste	Wygładzona wartość zmiennej prognozowanej	Wygładzona wartość przyrostu trendu	Prognozy wygasłe	Błąd bezwzględny	Błąd do kwadratu	Błąd względny
Rok	Y_t	F_t	S_t	y_t^*	$(y_t-y_t^*)$	$(y_t-y_t^*)^2$	$(y_t-y_t^*)/y_t$
2000	35611	30695,39	-69,3622				
2001	39772	39772,00	4161,0000	39772	0,0000	0,0000	0,00%
2002	38253	38253,00	3148,2560	43933	5680,0000	32262400,0000	14,85%
2003	35774	35774,00	2144,9163	41401	5627,2560	31666010,0895	15,73%
2004	36705	36705,00	1928,4750	37919	1213,9163	1473592,6746	3,31%
2005	29534	29534,00	306,0386	38633	9099,4750	82800445,0372	30,81%
2006	26061	26061,00	-367,7640	29840	3779,0386	14281132,7156	14,50%
2007	19849	19849,00	-1409,7913	25693	5844,2360	34155094,5983	29,44%
2008	16703	16703,00	-1719,3573	18439	1736,2087	3014420,7662	10,39%
2009	17549	17549,00	-1261,9541	14984	2565,3573	6581057,9931	14,62%
2010	16285	16285,00	-1262,3189	16287	2,0459	4,1858	0,01%
2011	15150	15150,00	-1239,6179	15023	127,3189	16210,0940	0,84%
2012	16183	16183,00	-834,4101	13910	2272,6179	5164792,1806	14,04%
2013	44562	44562,00	4374,3409	15349	29213,4101	853423331,9785	65,56%
2014	45403	45403,00	3744,3462	48936	3533,3409	12484497,8335	7,78%
2015	32514	32514,00	778,6206	49147	16633,3462	276668206,0745	51,16%
2016	40064	40064,00	3423,5722	13910	26153,6179	684011729,9637	65,28%
2017	34684	34684,00	2613,0935	15349	19335,4101	373858085,2626	55,75%
2018			**Prognoza**	**37297**	**α = 1,0000 β = 0,1783**		

Źródło: opracowanie własne na podstawie danych KGP.

Przedstawiona w tabeli 2 prognoza metodą Holta (37 297 przestępstw) obarczona jest dużym procentowym błędem średniokwadratowym (MSE) — 23,18%, co ponownie sprawia, że prognoza jest niedopuszczalna. Równie niezadawalająca jest prognoza trendu liniowego (29 377 przestępstw), gdyż współczynnik determinacji R^2 wynosi 0,0012. Ilustracja tych prognoz znajduje się na rysunku 3.



Rys. 3. Wartości empiryczne oraz prognozy stwierdzonej przestępczości komputerowej

Źródło: opracowanie własne na podstawie danych KGP.

Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych

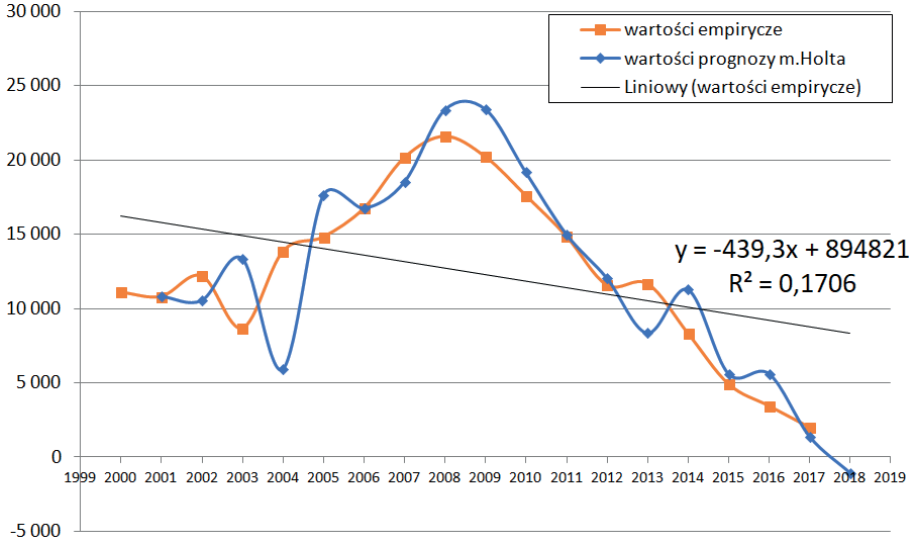
Tabela 3. Prognoza stwierdzonej przestępczości związanej z naruszeniem praw autorskich i praw pokrewnych na rok 2018

Okresy	Wartości rzeczywiste	Wygładzona wartość zmiennej prognozowanej	Wygładzona wartość przyrostu trendu	Prognozy wygasłe	Błąd bezwzględny	Błąd do kwadratu	Błąd względny
Rok	Y_t	F_t	S_t	y_t^*	$(y_t-y_t^*)$	$(y_t-y_t^*)^2$	$(y_t-y_t^*)/y_t$
2000	11 116	11 116,00	-284,00				
2001	10 832	10 832,00	-284,00	10 832	—	—	0,00%
2002	12 216	12 100,57	1 267,18	10 548	1 668,00	2 782 224,00	13,65%
2003	8 685	9 009,05	-3 087,61	13 368	-4 682,75	21928161,45	-53,92%
2004	13 868	13 318,10	4 302,39	5 921	7 946,56	63147796,13	57,30%
2005	14 843	15 035,20	1 719,43	17 620	-2 777,49	7714466,66	-18,71%
2006	16 774	16 772,66	1 737,44	16 755	19,37	375,06	0,12%
2007	20 195	20 078,40	3 304,33	18 510	1 684,90	2838884,76	8,34%
2008	21 626	21 747,57	1 670,63	23 383	-1 756,74	3086130,69	-8,12%

Okresy	Wartości rzeczywiste	Wygładzona wartość zmiennej prognozowanej	Wygładzona wartość przyrostu trendu	Prognozy wygasłe	Błąd bezwzględny	Błąd do kwadratu	Błąd względny
2009	20 240	20 459,93	-1 284,97	23 418	-3 178,20	10100950,78	-15,70%
2010	17 624	17 731,33	-2 727,31	19 175	-1 550,96	2405473,54	-8,80%
2011	14 883	14 891,37	-2 839,85	15 004	-121,02	14645,98	-0,81%
2012	11 589	11 621,01	-3 269,98	12 052	-462,52	213928,70	-3,99%
2013	11 684	11 453,36	-170,44	8 351	3 332,97	11108714,35	28,53%
2014	8 329	8 533,41	-2 917,47	11 283	-2 953,92	8725629,47	-35,47%
2015	4 918	4 966,30	-3 566,53	5 616	-697,94	487118,21	-14,19%
2016	3 439	3 589,64	-4 941,94	5 616	-2 176,94	4739061,43	-63,30%
2017	1 998	1 956,60	-3 010,20	1 400	598,23	357881,20	29,94%
2018			**Prognoza**	**-1 054**	**α = 0,9308 β = 0,9991**		

Źródło: opracowanie własne na podstawie danych KGP.

Prognozy cyberprzestępstw związanych z naruszeniem praw autorskich i praw pokrewnych w oparciu o dane z ostatnich 17 lat wskazują, że trend tych liczb jest malejący. Niestety te prognozy są statystycznie niedopuszczalne (procentowy błąd średniokwadratowy (MSE) — 8,46%, lecz ujemna wartość prognozy, a współczynnik determinacji $R^2 = 0{,}1706$).



Rys. 4. Wartości empiryczne oraz prognozy stwierdzonej przestępczości związanej z naruszeniem praw autorskich i praw pokrewnych na rok 2018

Źródło: opracowanie własne na podstawie danych KGP.

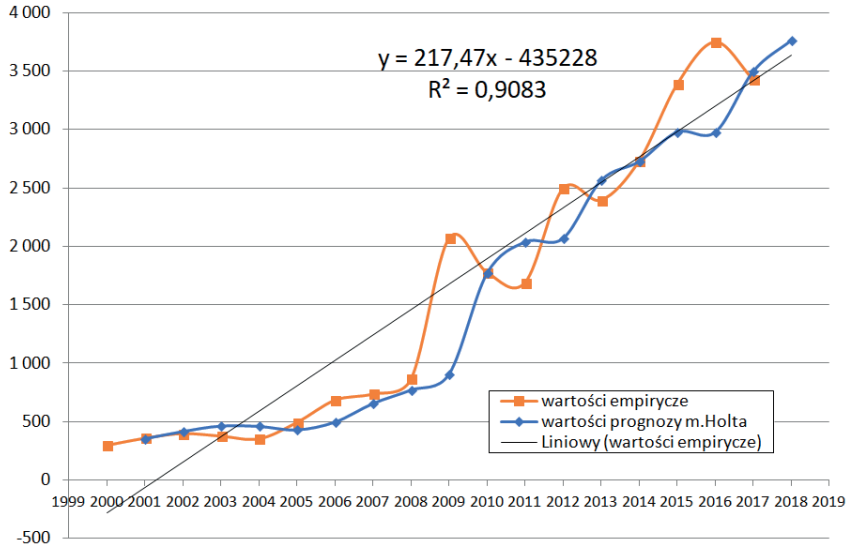
Przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów

Ilość odnotowanych przestępstw przeciwko poufności, integralności i dostępności danych informatycznych i systemów jest znacznie mniejsza niż w każdej z dwóch wcześniejszych kategorii. Są to jednak w większości klasyczne cyberprzestępstwa. Prognozy wskazują wzrost ilości tego typu przestępstw, przy jednoczesnym dobrym dopasowaniu (procentowy błąd średniokwadratowy (MSE) metody Holta — 4,26% oznacza prognozę dokładną, a współczynnik determinacji $R^2 = 0{,}9083$ trendu liniowego dopasowanie bardzo dobre).

Tabela 4. Prognoza stwierdzonej przestępczości przeciwko poufności, integralności i dostępności danych informatycznych i systemów na 2018 rok

Okres	Wartości rzeczywiste	Wygładzona wartość części stałej	Wygładzona wartość przyrostu	Prognoza wygasła	Błąd średni	Błąd kwadratowy	Procentowy błąd średni
Rok	Y_t	F_t	S_t	y_t^*	$(y_t - y_t^*)$	$(y_t - y_t^*)^2$	$(y_t - y_t^*)/y_t$
2000	293	293,00	62,00				
2001	355	355,00	62,00	355	—	—	0,00%
2002	394	405,15	58,50	417	-23,00	529,00	-5,84%
2003	372	416,41	44,54	464	-91,64	8 398,42	-24,64%
2004	349	403,25	27,49	461	-111,95	12 532,79	-32,08%
2005	490	461,28	36,51	431	59,26	3 511,66	12,09%
2006	680	591,70	64,26	498	182,20	33 197,59	26,79%
2007	733	695,67	76,00	656	77,03	5 933,72	10,51%
2008	862	818,22	89,75	772	90,33	8 160,00	10,48%
2009	2 067	1 505,34	266,27	908	1 159,02	1 343 330,13	56,07%
2010	1 773	1 772,33	266,49	1 772	1,39	1,93	0,08%
2011	1 687	1 857,49	212,90	2 039	-351,81	123 772,10	-20,85%
2012	2 494	2 288,72	277,42	2 070	423,61	179 443,53	16,99%
2013	2 393	2 476,90	251,05	2 566	-173,14	29 977,22	-7,24%
2014	2 728	2 727,98	251,06	2 728	0,05	0,00	0,00%
2015	3 383	3 187,24	312,58	2 979	403,97	163 187,73	11,94%
2016	3 747	3 374,84	368,02	2 979	767,97	589 770,26	20,50%
2016	3 428	3 462,80	301,64	3 500	-71,82	5 158,13	-2,10%
2017			**Prognoza**	**3 764**	**α = 0,5154 β = 0,2955**		

Źródło: opracowanie własne na podstawie danych KGP.



Rys. 5. Wartości empiryczne oraz prognozy stwierdzonej przestępczości przeciwko poufności, integralności i dostępności danych informatycznych i systemów na 2018 rok

Źródło: opracowanie własne na podstawie danych KGP.

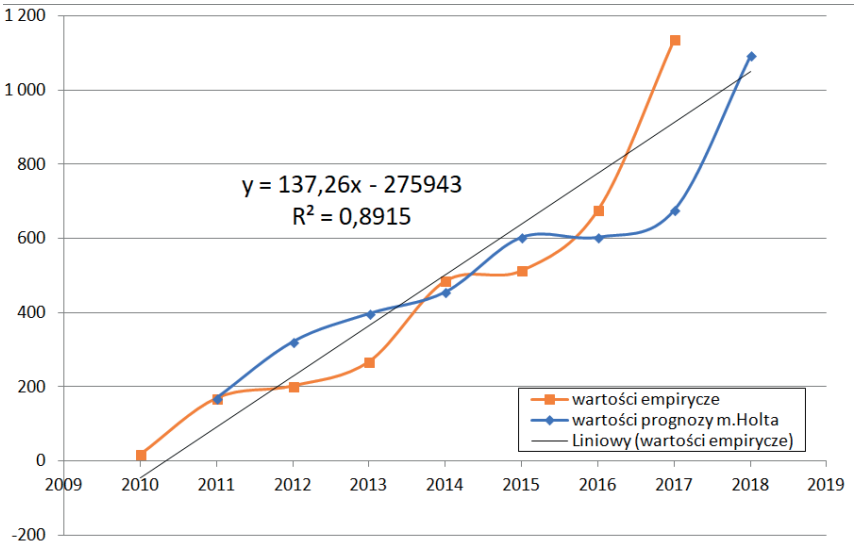
Przestępstwa ze względu na charakter zawartych informacji

W przypadku przestępstw ze względu na charakter zawartych informacji statystyki prowadzone są od 2010 roku. Prognozy mają bardzo podobną wartość, ale liczona metodą Holta ma błąd niedopuszczalny (procentowy błąd średniokwadratowy (MSE) — 11,26%), natomiast druga liczona trendem liniowym ma dopasowanie dobre (współczynnik determinacji $R^2 = 0,8915$).

Tabela 5. Prognoza stwierdzonej przestępczości ze względu na charakter zawartych informacji — 8 lat

Okres	Wartości rzeczywiste	Wygładzona wartość części stałej	Wygładzona wartość przyrostu	Prognoza wygasła	Błąd średni	Błąd kwadratowy	Procentowy błąd średni
Rok	Y_t	F_t	S_t	y_t^*	$(y_t - y_t^*)$	$(y_t - y_t^*)^2$	$(y_t - y_t^*)/y_t$
2010	17	17,00	152,00				
2011	169	169,00	152,00	169	—	—	0,00%
2012	202	256,03	140,89	321	-119,00	14 161,00	-58,91%
2013	268	326,53	128,85	397	-128,92	16 619,19	-48,10%
2014	485	471,55	131,62	455	29,62	877,30	6,11%
2015	513	553,94	123,20	603	-90,17	8 130,88	-17,58%
2016	677	643,48	138,51	603	73,83	5 450,66	10,91%
2017	1 137	928,22	166,14	677	459,86	211 473,58	40,45%
2018			Prognoza	1 094	$\alpha = 0,5460$ $\beta = 0,1710$		

Źródło: opracowanie własne na podstawie danych KGP.



Rys. 6. Wartości empiryczne oraz prognozy stwierdzonej przestępczości ze względu na charakter zawartych informacji

Źródło: opracowanie własne na podstawie danych KGP.

Podsumowanie

Z wykonanych analiz wynika, że prognozowanie cyberprzestępczości w wymiarze globalnym jest bardzo niedokładne. To samo stwierdzenie dotyczy cyberprzestępstw z kategorii: przestępstwa fałszerstwa i oszustwa komputerowego (przestępstwa komputerowe) oraz przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych. Nieznacznie dokładniejsze mogą być prognozy cyberprzestępstw ze względu na charakter zawartych informacji.

Pomimo statystycznie dobrego prognozowania przestępstw przeciwko poufności, integralności i dostępności danych informatycznych i systemów należy się liczyć z dużym błędem wynikającym z warunków egzogenicznych (liczby przestępstw są w dużej mierze wynikiem czynników przypadkowych).

Bibliografia

Europol, High Tech Crimes within EU. Threat Assessment 2007. (2007). Hague.

Europol. (2017). *Internet Organised Crime Threat Assessment* (IOCTA 2017). Pobrane z: https://www.europol.europa.eu/sites/default/files/documents/iocta2017.pdf.

Ficoń, K. (2013). *Sztuczna inteligencja nie tylko dla humanistów.* Warszawa.

Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów z dnia 22 maja 2007 r. W kierunku ogólnej strategii zwalczania cyberprzestępczości, KOM(2007) 267 wersja ostateczna. Pobrane z: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:pl:PDF.

Kosiński, J. (2015). *Paradygmaty cyberprzestępczości.* Difin.

Liderman, K. (2011). O zagrożeniach dla skutecznej ochrony informacji, przetwarzanej w sieciach i systemach teleinformatycznych, powodowanych nowomową. *Studia Bezpieczeństwa Narodowego, IOiZ, 2*, 401–409.

Mazur, M. (1966). *Cybernetyczna teoria układów samodzielnych*. PWN.

Po globalnym cyberataku premier zwołała nadzwyczajne spotkanie. Znamy decyzję ws. stopnia alarmowego. (2017). Pobrane z: https://www.wprost.pl/kraj/10062533/po-globalnym-cyberataku-premier-zwolala-nadzwyczajne-spotkanie-znamy-decyzje-ws-stopnia-alarmowego.html.

Premier Beata Szydło po ostatnich atakach cybernetycznych: Nie podwyższamy stopnia alarmowego. (2017). Pobrane z: https://www.premier.gov.pl/mobile/wydarzenia/aktualnosci/premier-beata-szydlo-po-ostatnich-atakach-cybernetycznych-nie-podwyzszamy.html.

Szef MON: atak cybernetyczny groźny ze względu na cel. (2017). Pobrane z: http://wiadomosci.onet.pl/kraj/szef-mon-atak-cybernetyczny-grozny-ze-wzgledu-na-cel/hwqmys6.

Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Crimes related to computer networks. (2000). UN, Vienna. Pobrane z: http://www.uncjin.org/Documents/congr10/10e.pdf.

World Economic Forum. (2018). *The Global Risks Report 2018* (13th Edition). Pobrane z: http://wef.ch/risks2018.

An attempt to predict cybercrime in Poland in 2018

Abstract

The article attempts to forecast cybercrime in Poland in 2018. The concept of cybercrime and its interpretation in the Polish Penal Code have been described. Linear trend and the Holt's method were used for forecasting.

Keywords: cybercrime, forecasting, linear trend, Holt's method.

Artykuł stanowi element prac w ramach projektu pt. „Stworzenie systemu prognozowania rozwoju przestępczości jako elementu budowania strategii bezpieczeństwa i porządku publicznego", Nr DOB-BIO7/05/02/2015.