Paweł Olber
Instytut Służby Kryminalnej Wyższa Szkoła Policji w Szczytnie
ORCID: 0000-0002-4614-9527

Piotr Lewulis
Katedra Kryminalistyki Wydział Prawa i Administracji Uniwersytet Warszawski
ORCID: 0000-0002-8303-0971

MODUS OPERANDI SPRAWCÓW OSZUSTW Z WYKORZYSTANIEM INTERNETOWYCH PORTALI SPRZEDAŻOWYCH W KONTEKŚCIE WYKRYWCZYM I DOWODOWYM

Modus operandi of the perpetrators of frauds using internet sales portals in the context of detection and evidence

Wstęp

Postęp w zakresie rozwiązań telekomunikacyjnych w ciągu ostatnich lat przyspiesza rozwój gospodarczy, przeobrażając społeczną rzeczywistość[1]. Z roku na rok rośnie zaufanie do płatności online i chęć dokonywania zakupów drogą elektroniczną[2]. Co ciekawe, choć nie zaskakujące, trwające obecnie zawirowania społeczne związane z pandemią wirusa SARS-CoV-2 wydają się sprzyjać rozwojowi i zyskom szeroko rozumianej branży *e-commerce*[3]. Niestety, szerokie wykorzystanie zaawansowanych technologii informatycznych w dużej liczbie dziedzin życia społeczno-gospodarczego bezpośrednio wpływa na wzrost występowania związanej z tym przestępczości. Telefony komórkowe, smartfony, tablety czy komputery oraz sieć Internet – poprzez możliwości, jakie dają – odgrywają

---

1 Główny Urząd Statystyczny, *Jak korzystamy z Internetu? 2019*, GUS 2020, https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/5/10/1/jak_korzystamy_z_internetu_2019_.pdf (dostęp 19.10.2020).

2 Izba Gospodarki Elektronicznej, *E-commerce w Polsce 2019*, https://eizba.pl/wp-content/uploads/2019/07/raport_GEMIUS_2019-1.pdf (dostęp 19.10.2020), s. 70.

3 K. Janoś, *Koronawirus sprzyja e-commerce. Sprzedaż w sieci może być dwukrotnie większa niż przed rokiem*, online: https://www.money.pl/gospodarka/koronawirus-sprzyja-e-commerce-sprzedaz-w-sieci-moze-byc-dwukrotnie-wieksza-niz-przed-rokiem-6522842250507905a.html (dostęp 19.10.2020).

coraz większą rolę w nielegalnej działalności lub też w znaczny sposób ułatwiają jej prowadzenie. Powszechne jest w tym kontekście dokonywanie przestępstw motywowanych chęcią zysku.

Doprowadzenie do niekorzystnego rozporządzenia mieniem w drodze czy to wprowadzenia osoby w błąd, czy też wyzyskania jej błędu stanowi kluczowe znamię oszustwa – czynu zabronionego określonego w art. 286 k.k. Działania sprawców współczesnych oszustw w bardzo dużym stopniu oparte są na interakcjach w przestrzeni internetowej, w szczególności na wykorzystaniu internetowych portali sprzedażowych. Szczegółowy sposób działania sprawców jest zróżnicowany zależnie od funkcjonalności konkretnych platform sprzedażowych oraz docelowej grupy osób pokrzywdzonych. Istnieją jednak wspólne elementy *modus operandi* sprawców takich czynów, które mają bezpośredni wpływ na skuteczność procesów wykrywczych. Kryminalistyczna poprawność i celowość czynności wykrywczych podejmowanych w postępowaniu przygotowawczym oczywiście oddziałuje na przebieg późniejszego postępowania dowodowego, w rezultacie determinując skuteczność postępowania karnego. W przypadku tzw. oszustw internetowych popełnianych z wykorzystaniem internetowych portali sprzedażowych należy brać pod uwagę ich specyfikę już w pierwszych czynnościach postępowania, a błędy popełnione na tym etapie mogą być trudne do skorygowania. Organy ścigania muszą zaś podejmować wszelkie działania, które przyczynią się do zwiększenia skuteczności w walce z cyberprzestępczością.

W niniejszym opracowaniu zaprezentowany jest opis współczesnego *modus operandi* sprawcy typowych oszustw popełnianych za pośrednictwem internetowych portali sprzedażowych, ze wskazaniem potencjalnych problemów w pracy wykrywczej i dowodowej oraz z podaniem sposobów ich rozwiązywania. Opis ten uzupełniony jest aktualnymi danymi na temat skali tego rodzaju czynów, wynikającymi z analizy danych statystycznych (obejmujących dostępne dane za lata 2015–2020), a częściowo także z przeprowadzonych w 2019 r. badań aktowych.

Oszustwo „internetowe" a oszustwo „komputerowe"

Przed przedstawieniem opisu sposobu działania współczesnych oszustów internetowych warto zwrócić uwagę, że szeroko pojęte doprowadzenie do niekorzystnego rozporządzenia mieniem stanowi jedno z historycznie najstarszych zjawisk szkodliwych związanych z rozwojem technologii komputerowych[4].

[4] Oszustwa popełniane z pomocą technologii komputerowych opisywano już w latach 70. XX wieku, zob.: D.B. Parker, *Crime by Computer*, Scribner, New York 1976, por. A. Adamski, *Prawo karne komputerowe*, Wydawnictwo C.H. Beck, Warszawa 2000, s. XVI–XVII.

Oszustwo należy do kategorii czynów zabronionych tradycyjnie ujętych w ustawodawstwie karnym, a wykorzystanie nowych technologii do jego popełnienia nie powinno dziwić – przenoszenie się sprawców do „świata cyfrowego" stanowi naturalny efekt rozwoju handlu prowadzonego drogą elektroniczną.

Z karnomaterialnego punktu widzenia warto przy tym dokonać czytelnego rozróżnienia pomiędzy oszustwem „zwykłym" (z art. 286 k.k.) oraz „komputerowym" (z art. 287 k.k.). Co ciekawe, w początkowych okresach rozwoju przestępczości komputerowej (a więc w latach 70. i 80. XX wieku) rozróżnienie to nie istniało, a do ścigania wszystkich tych czynów z powodzeniem stosowano tradycyjne regulacje prawnokarne[5].

Z czasem wskazano, także w kontekście polskiego ustawodawstwa, na nieadekwatność stosowania ogólnego przepisu penalizującego oszustwo wobec tzw. oszustw komputerowych. Nie bez racji uznano bowiem, że znamię „doprowadzenia innej osoby do niekorzystnego rozporządzenia mieniem" nie może być spełnione, gdy decyzja o rozporządzeniu mieniem podejmowana jest *de facto* nie przez człowieka, lecz automatycznie przez system komputerowy „wprowadzony w błąd" przez sprawcę wprowadzającego dane lub polecenia[6]. Chodzi zatem o stany faktyczne, w których niekorzystne rozporządzenie mieniem następuje niejako automatycznie, wskutek dyspozycji systemu informatycznego wprowadzonego w błąd przez sprawcę (czy to dzięki wykorzystaniu złośliwego oprogramowania, innych technik hackerskich, czy też po prostu przez wprowadzenie nieprawdziwych danych).

Rozróżnienie to wydaje się w pełni zrozumiałe w drodze porównania ustawowych znamion czynów zabronionych z art. 286 i art. 287 k.k. Należy uznać je za uzasadnione, biorąc pod uwagę ogólne zasady prawa karnego obejmujące m.in. zakaz stosowania analogii i usuwanie istniejących w przepisach karnych luk w drodze interpretacji rozszerzającej. Zaistnienie czynu z art. 286 k.k. wymaga zatem działania człowieka zarówno po stronie sprawcy, jak i po stronie pokrzywdzonego – który w wyniku błędu dokonuje niekorzystnego rozporządzenia mieniem. Taka właśnie sytuacja ma zaś miejsce w większości przypadków oszustw internetowych popełnianych z wykorzystaniem portali sprzedażowych. W rezultacie dla przedstawienia realnego, popartego danymi empirycznymi opisu tego rodzaju zachowań z punktu widzenia nauk penalnych najwłaściwsza jest

---

5 H.M. Jarrett, M.W. Bailie, E. Hagen, S. Eltringham, *Prosecuting Computer Crimes*, US Department of Justice 2008, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (dostęp 19.10.2020), s. 1.

6 A. Chmiel, *Przestępstwa związane z wykorzystaniem komputera – charakterystyka zagadnienia*, „Palestra" 1991, nr 10.

analiza danych dotyczących przestępstw ściganych z art. 286 k.k. O powyższych rozróżnieniach należy pamiętać, mówiąc o „oszustwach popełnianych z wykorzystaniem internetowych platform sprzedażowych" czy po prostu o „oszustwach internetowych". W ramach niniejszego opracowania przez te pojęcia będą rozumiane czyny z art. 286 k.k.

Nadmienić warto, że spełnienie celów sprawców możliwe jest przy zastosowaniu różnych technik. Niektóre z nich (np. te bazujące na bezprawnym uzyskaniu dostępu do bankowości elektronicznej pokrzywdzonej osoby) mogą otwierać ich na odpowiedzialność także z innych przepisów – np. w związku z uzyskaniem bezprawnego dostępu do informacji przez przełamanie czy ominięcie zabezpieczeń informatycznych, o którym mowa w art. 267 k.k. Do wyczerpania znamion czynu opisanych w tym przepisie nie zawsze jednak dochodzi, a dla istoty podniesionych tu problemów kryminalistycznych bardziej reprezentatywne jest ich omówienie w kontekście przestępstwa oszustwa. Pozostaje to zgodne także z utrzymującą się praktyką w zakresie kwalifikacji prawnych nadawanych opisanym w niniejszym artykule rodzajom zdarzeń.

Oszustwo internetowe w świetle aktualnych danych empirycznych

O realnym związku *modus operandi* sprawców oszustw z technologią teleinformatyczną świadczą dostępne dane statystyczne. Należy pamiętać, że oszustwo stanowi jedno z najczęściej stwierdzanych w Polsce przestępstw. Jego szkodliwość społeczna jest przy tym bardzo duża – przynosi ono szkodę po stronie osób fizycznych, niszczy zaufanie społeczne w obrocie gospodarczym, skutkując niekiedy dotkliwym na gruncie osobistym uszczerbkiem finansowym. Warto zatem zilustrować, jak dużą część wszystkich czynów z art. 286 k.k. stanowią te związane z technologią komputerową.

Dane przedstawione poniżej (ryc. 1) pochodzą z Krajowego Systemu Informacyjnego Policji (KSIP)[7], uzupełnionego o informacje na temat postępowań prowadzonych na terenie wszystkich jednostek w Polsce. Sposób kodowania danych o zdarzeniach w KSIP pozwala na uzupełnianie podstawowej informacji o *modus operandi* sprawcy (przez nadanie mu etykiety w postaci jednej ze skatalogowanych w systemie predefiniowanych wartości – w tym przez określenie, że czyn miał charakter cyberprzestępstwa). Zestawienie i porównanie ogólnej liczby stwierdzonych przez Policję oszustw z liczbą oszustw mających związek

[7] Dane uzyskane od Komendanta Głównego Policji w trybie wniosku o dostęp do informacji publicznej (Wnioski nr Gip-3492/18, Gip-3859/18 oraz Gip-4275/18, Gip-872/19 oraz Kwo-1040/20/RP).

z wykorzystaniem technologii komputerowej pozwala zilustrować skalę omawianego zjawiska.

Należy wymienić dwa najistotniejsze ograniczenia tej formy prezentacji danych. Po pierwsze, wskazane dane dotyczą czynów stwierdzonych, ale niekoniecznie wykrytych przez Policję. W statystykach Policji pojęcie „przestępstwa stwierdzonego" dotyczy zdarzeń objętych zakończonym postępowaniem przygotowawczym, w wyniku którego potwierdzono zaistnienie czynu zabronionego (niezależnie od wykrycia sprawcy)[8]. Dostępne dane statystyczne w oczywisty sposób nie uwzględniają więc czynów niezgłoszonych ani faktycznego rezultatu prowadzonego postępowania. Po drugie, rejestracja w KSIP zdarzeń z uwzględnieniem wartości *modus operandi* nie jest obligatoryjna i zależy od decyzji rejestrującego sprawę funkcjonariusza. Liczba przestępstw stwierdzonych z uwzględnieniem jakichkolwiek wartości *modus operandi* obrazuje potencjalnie tylko część rzeczywistej wielkości opisywanych zjawisk. Niestety nie ma możliwości precyzyjnego ustalenia, jaka jest skala tych nieścisłości. Na marginesie tych rozważań warto zauważyć, że należy zachęcać funkcjonariuszy Policji do uzupełniania wartości *modus operandi* w systemie rejestracyjnym, co pozwoli na opracowanie w przyszłości lepszych rozwiązań na rzecz zapobiegania przestępczości na podstawie rzeczywistych danych kryminologicznych.

Analiza przedstawionych danych umożliwia jednak ostrożne wyrażenie hipotezy, że istotna część stwierdzanych w Polsce oszustw popełniana jest z wykorzystaniem technologii teleinformatycznych. W 2019 r. było to ponad 44,5% wszystkich czynów z art. 286 k.k. Jak wskazują dane z kilku ostatnich lat, skala udziału takich czynów w ogóle oszustw rośnie. W momencie przygotowania niniejszego opracowania dane za cały rok 2020 nie są jeszcze dostępne – w świetle jednak informacji prasowych[9] można oczekiwać dalszego (dynamicznego) wzrostu występowania oszustw internetowych, co ma związek także z bieżącą sytuacją epidemiologiczną.

Powyższe dane statystyczne można dodatkowo zilustrować danymi empirycznymi, pochodzącymi z badania przeprowadzonego metodą analizy akt prawomocnie zakończonych w latach 2016–2018 spraw karnych z Sądu Okręgowego w Warszawie[10].

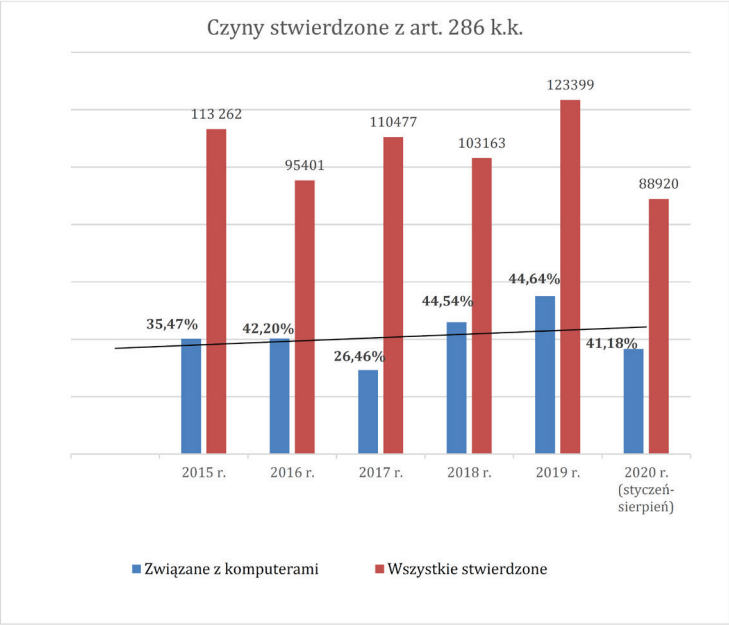
---

8 Komenda Główna Policji, *Uwagi* i definicje – statystyka, http://statystyka.policja.pl/download/20/ 232288/Uwagiidefinicje.docx (dostęp: 19.10.2020).

9 D. Kaczyńska, *Pandemia internetowych oszustów. Oto ciemna strona boomu na e-sklepy*, https://www.forbes.pl/biznes/falszywe-sklepy-internetowe-oszusci-wykorzystuja-pandemie-koronawirusa/f3y2pcz (dostęp 19.10.2020).

10 Szerzej na temat metodologii i wyników badań zob.: P. Lewulis, *Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 2021.

Ryc. 1. Dane Policji o stwierdzonych (w latach 2015–2019 oraz w części roku 2020) przestępstwach oszustwa w typie podstawowym z art. 286 § 1 z uwzględnieniem ogólnej ich liczby oraz liczby przestępstw, w których *modus operandi* sprawcy miał związek z technologiami komputerowymi. Wykres uzupełniono o przedstawienie linii trendu (liniowego) w liczbie zdarzeń związanych z komputerami



Źródło: opracowanie własne na podstawie danych KGP.

Badanie zrealizowane zostało w pierwszym półroczu 2019 r., a spośród N = 3343 spełniających wskazane kryteria spraw z art. 286 k.k. analizą objęto n = 218 losowych postępowań. Pamiętając o ograniczonej reprezentatywności tak zbudowanej próby[11], należy wskazać, że 68 (28,8%) spośród 218 postępowań prowadzonych w sprawach oszustw dotyczyło czynów mających związek z wykorzystaniem Internetu. W szczególności zaś łącznie 47 postępowań (21,6%) dotyczyło oszustw dokonywanych za pośrednictwem internetowych platform sprzedażowych różnego typu (m.in. na portalach aukcyjnych lub ogłoszeniowych).

Niezależnie od istniejących ograniczeń metod gromadzenia zaprezentowanych tu danych pewne jest, że zjawisko oszustw internetowych występuje w rzeczywistości, a jego skala, jak się wydaje, rośnie wraz z upływem czasu. Ponieważ zaś *modus operandi* sprawców w tego rodzaju czynach jest znany i relatywnie

[11] Przedstawione tu dane obejmują wszak wycinek badania prowadzonego w innym kontekście.

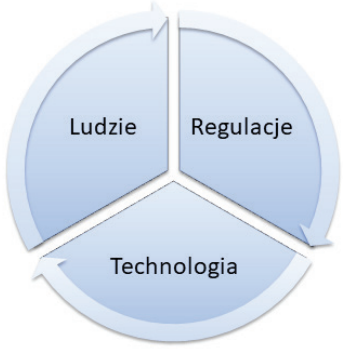
jednolity, nakłada to na organy ścigania obowiązek szczególnej dbałości o sprawny przebieg procesów wykrywczych.

Modus operandi sprawców przestępstw

W literaturze przedmiotu funkcjonuje wiele definicji pojęcia *modus operandi.* Według A. Solarza jest to „zespół charakterystycznych czynności taktycznych i technicznych w stadium przygotowania, wykonania i stadium końcowym przestępstwa”[12]. Z kolei T. Hanausek definiuje *modus operandi* jako „powtarzający się sposób działania sprawcy, polegający na atakowaniu takich samych przedmiotów (dóbr), używaniu tych samych lub takich samych technicznych sposobów działania przestępczego, działaniu w podobnym czasie, miejscu czy okolicznościach”[13].

Niezależnie jednak od ujęcia definicyjnego *modus operandi* oraz istniejących różnic w tym zakresie sprowadzają się one do ustalenia „sposobu popełnienia” danego przestępstwa. Udzielenie odpowiedzi na pytanie, „w jaki sposób popełniono przestępstwo”, wymaga szczegółowej analizy każdego przypadku. Ogólnikowo rejestrowany *modus operandi* ma bowiem znikomą wartość identyfikacyjną[14]. Analizowanie popularnie występujących sposobów popełniania przestępstw ma jednak wartość badawczą, umożliwiającą dostosowywanie rozwiązań stosowanych przez organy ścigania do faktycznej rzeczywistości.

Ryc. 2. Spektrum działalności przestępczej: ludzie, technologia, regulacje



Źródło: opracowanie własne.

[12] A. Solarz, *Zagadnienie przestępczości zawodowej w Polsce*, Państwowe Wydawnictwo Naukowe, Warszawa 1967, s. 167.

[13] T. Hanausek, *Modus operandi i alibi*, „Studia Kryminologiczne, Kryminalistyczne i Penitencjarne” 1978, nr 8.

[14] M. Sąsiada, *Modus operandi jako środek identyfikacji sprawcy przestępstwa*, „Wrocławskie Studia Erazmiańskie. Zeszyty Studenckie” 2008, z. 1, s. 206.

W celu zrozumienia *modus operandi* sprawców oszustw popełnianych w cyberprzestrzeni istotne jest poznanie ogólnego mechanizmu działalności przestępczej z wykorzystaniem nowych technologii, do której to kategorii oszustwa popełniane w Internecie z pewnością należą. Sama technologia nie przesądza jednak o wszystkim, gdyż jest bezużyteczna bez jej użytkowników oraz dodatkowych procedur i regulacji. Wyłącznie połączenie tych trzech elementów tworzy całościowe spektrum działalności przestępczej w cyberprzestrzeni, obejmując wszystkie metody i sposoby popełniania przestępstw.

Przestępcy wykorzystują zarówno słabości samej technologii, jak i luki w procedurach i przepisach prawnych, a także podstęp i słabości ludzkie. W przypadku oszustw z wykorzystaniem internetowych portali sprzedażowych najbardziej istotnym celem działalności przestępczej jest człowiek. Przestępcy stosują różne techniki manipulacji, wykorzystując w szczególności istniejące możliwości świata wirtualnego[15]. Jedną z takich możliwości jest zakup rozmaitych dóbr i usług, nierzadko po okazyjnych cenach. Sprawcy czynów zabronionych mają świadomość tych możliwości i oczekiwań konsumenckich, wobec czego tworzą fałszywe sklepy internetowe lub popełniają oszustwa z wykorzystaniem gotowej infrastruktury portali aukcyjnych w Internecie[16]. Te właśnie warianty oszustw internetowych są na tyle charakterystyczne w zakresie *modus operandi* sprawcy, że uzasadnione jest bardziej szczegółowe ich omówienie poniżej.

Fałszywe sklepy internetowe

Przygotowanie do popełniania przestępstw z wykorzystaniem fałszywych sklepów internetowych obejmuje następujące po sobie czynności:

- rejestrację domeny,
- konfigurację oprogramowania sklepu wraz z odpowiednią szatą graficzną,
- zdefiniowanie metody płatności,
- przygotowanie bazy atrakcyjnych produktów,
- przeprowadzenie kampanii promującej.

Tworzony jest zatem fałszywy „sklep internetowy", a oszustwo dokonuje się z chwilą realizacji płatności za zakupiony produkt – czynność ta jest zatem

[15] B.K. Rajput, *Understanding modus operandi of the cyber economic crime from people- process-technology framework's perspective*, „Journal of Emerging Technologies and Innovative Research" 2018, t. 5(3), s. 1093.

[16] J. Lizut, *Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych*, Wydawnictwo Wyższej Szkoły Pedagogicznej im. Janusza Korczaka, Warszawa 2014, s. 245.

kluczowym elementem w przebiegu tych zdarzeń, od którego zależy skuteczność działania sprawcy. Płatność może przebiegać według kilku schematów.

Po pierwsze, gdy bezpośrednio po dokonaniu zakupów system wyświetla użytkownikowi informację o rachunku bankowym (obsługiwanym przez sprawcę przestępstwa), na który kupujący wpłaca pieniądze. Ze strony klienta transakcja jest jak najbardziej wiarygodna, jednakże kupujący nigdy nie otrzymuje zakupionego produktu[17].

Po drugie, sprawca może wykorzystać fałszywą bramkę płatności („podstawioną" przez sprawcę witrynę przypominającą rzeczywisty system płatności) w celu kradzieży danych logowania do bankowości elektronicznej oraz wyłudzania kodów uwierzytelniających przelewy.

Po trzecie, sprawcy wykorzystują prawdziwe mechanizmy płatności internetowych. Sposób działania polega wówczas na wykonaniu przez sprawcę, równolegle z pokrzywdzonym korzystającym z fałszywego sklepu internetowego, zakupów na identyczną kwotę w innym, realnym sklepie. Po dokonaniu zakupów przestępca wybiera płatność online PayU, a następnie przekazuje ofierze link do płatności za pośrednictwem systemu zintegrowanego z fałszywym sklepem internetowym. Ofiara nieświadomie opłaca zamówienie dokonane przez przestępcę w prawdziwym sklepie internetowym[18]. Opisywany mechanizm przedstawiono na poniższej rycinie.

Ryc. 3. Schemat oszustwa z wykorzystaniem prawdziwej płatności w fałszywym sklepie internetowym

Źródło: opracowanie własne.

[17] Raport roczny 2019 z działalności CERT Polska, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf (dostęp 19.10.2020), s. 49–50.

[18] Ibidem.

Legalne aukcje internetowe

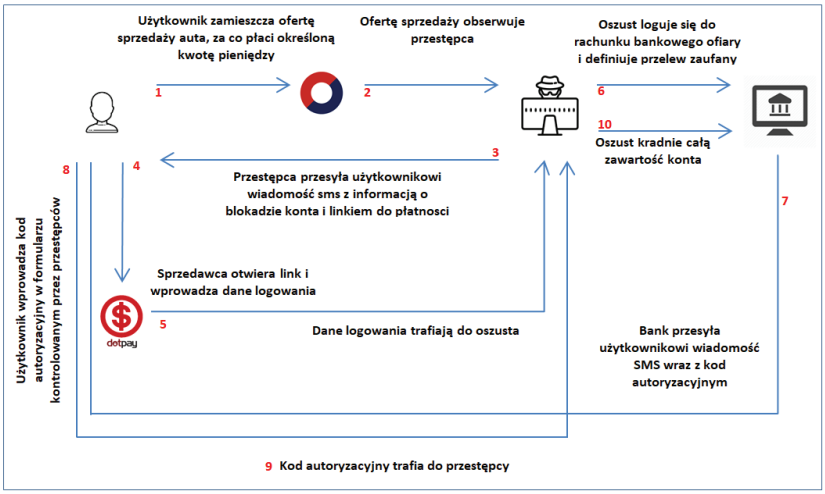
Liczba oszustw związanych z popularnymi portalami aukcyjnymi nie maleje. Nadal powszechne są tzw. aukcje oszukańcze, w których sprawcy nie wysyłają wylicytowanych przedmiotów, ewentualnie przesyłają kupującemu inny bezwartościowy przedmiot, o podobnych gabarytach i zbliżonej wadze[19].

Poza tymi najprostszymi oszustwami w handlu elektronicznym przestępcy prowadzą działania wymierzone w kradzież całej zawartości rachunków bankowych ofiar. Scenariusz takiego działania można opisać na przykładzie ataku na klientów serwisu Otomoto.pl. Wykorzystywany mechanizm przestępczy składa się z następujących etapów:

- użytkownik publikuje ofertę sprzedaży samochodu, płacąc za to kilkadziesiąt złotych;
- po pewnym czasie użytkownik otrzymuje wiadomość SMS o treści sugerującej zablokowanie konta z powodu istniejących zaległości w płatnościach. Wiadomość zawiera link do systemu płatności wraz z informacją o konieczności zapłaty symbolicznej kwoty za odblokowanie konta;
- użytkownik otwiera wskazany w wiadomości link, który prowadzi go do fałszywego panelu płatności dotpay;
- użytkownik inicjuje metodę płatności, nie zauważając, że korzysta z szablonu logowania (przygotowanego przez przestępców), który łudząco przypomina system płatności prawdziwego banku;
- użytkownik loguje się do systemu, wprowadzając dane uwierzytelniające, które przechwytywane są przez przestępców;
- ofiara otrzymuje (przygotowany przez przestępców) ekran płatności łudząco przypominający ekran płatności prawdziwego banku;
- przestępcy logują się na konto ofiary, gdzie definiują przelew zaufany;
- ofiara otrzymuje wiadomość tekstową SMS wraz z jednorazowym kodem autoryzacyjnym, będąc przekonana, że jest to autoryzacja zaległej płatności;
- ofiara zostaje poproszona o podanie jednorazowego kodu autoryzacyjnego. Pierwsza próba wpisania kodu kończy się wyświetleniem informacji o błędzie. W tym czasie przestępcy przechwytują kod i dokonują autoryzacji przelewu zaufanego;
- ofiara ponownie wpisuje jednorazowy kod, który tym razem okazuje się prawidłowy;
- przestępcy, wykorzystując przelew zaufany, wyprowadzają wszystkie środki zgromadzone na koncie ofiary.

[19] T. Pączkowski, *Słownik cyberbezpieczeństw*a, Szkoła Policji, Katowice 2017, s. 41.

Ryc. 4. Schemat kradzieży środków finansowych z rachunku bankowego



Źródło: opracowanie własne.

Przedstawione powyżej mechanizmy potwierdzają, że istnieje wiele wariantów oszustw internetowych wykorzystujących platformy handlu elektronicznego, które różnią się pomiędzy sobą mechanizmem działań przestępczych. Nie sposób przedstawić wszystkie znane i przewidywane mechanizmy. Z pewnością jednak działania sprawców oszustw z wykorzystaniem internetowych portali sprzedażowych mają wiele cech wspólnych. Wprowadzenie pokrzywdzonych w błąd polega na ogół na mylnych lub z gruntu fałszywych informacjach na temat jakości, rodzaju czy cech oferowanych produktów lub w ogóle co do intencji wysyłki towaru po otrzymaniu zapłaty.

Wcześniej proponowana w literaturze polskiej typologia *modus operandi* sprawcy oszustwa internetowego oparta była przede wszystkim na sposobie wykorzystania konta użytkownika w internetowym portalu sprzedaży oraz rolę odgrywaną przez sprawcę w procesie dokonywania transakcji[20]. Podział ten przedstawia się następująco:

- Ze względu na sposób wykorzystania konta użytkownika:
  - Wykorzystanie konta sprzedającego: sprawca dokonuje nielegalnego przejęcia konta użytkownika portalu sprzedaży internetowej. Przejęte konto użytkownika (po zmianie hasła dostępowego) wykorzystywane jest w dalszej działalności przestępczej w celu dokonywania oszustw internetowych.

[20] J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015, s. 172–173.

  - Stworzenie nowego konta: sprawca tworzy konto użytkownika w portalu sprzedaży internetowej, posługując się prawdziwymi danymi osoby fizycznej lub prawdziwymi danymi firmy w celu uwiarygodnienia uczciwych intencji[21]. Utworzone konto użytkownika wykorzystywane jest jednak w dalszej działalności przestępczej.
- Ze względu na rolę sprawcy w trakcie fałszywej transakcji:
  - Wejście w rolę sprzedającego: sprawca podszywając się pod sprzedającego, wysyła wiadomość e-mail z gratulacjami wygranej do osoby biorącej udział w aukcji internetowej (bezpośrednio po jej zakończeniu). W przesłanej wiadomości podaje jednocześnie swój numer rachunku bankowego w celu dokonania wpłaty za zakupiony przedmiot.
  - Wejście w rolę kupującego: sprawca bezpośrednio po zakończeniu aukcji internetowej kontaktuje się (podając się za osobę, która wygrała licytację) ze sprzedającym. W przesłanej do sprzedającego wiadomości e-mail sprawca podaje adres wysyłki zakupionego produktu.

Autorzy niniejszego artykułu proponują, aby podział ten uzupełnić o dodatkowy – ze względu na sposób przekazania środków finansowych przez pokrzywdzonego za pomocą:

- legalnego przelewu: w wyniku podstępnego działania przestępców ofiara dokonuje samodzielnie wpłaty określonej kwoty pieniędzy na rachunek bankowy, który jest kontrolowany przez oszustów, lub dokonuje płatności za produkt zakupiony (w tym samym czasie) przez przestępców w prawdziwym sklepie internetowym. Dokonujący płatności jest przekonany, że realizuje przelew za przedmioty, które zostały przezeń zakupione;
- kradzieży pieniędzy: przestępcy wykorzystując fałszywe bramki płatności, dokonują kradzieży danych logowania do systemów bankowości internetowej. Po zalogowaniu się dodają kontrolowany przez siebie rachunek do listy odbiorców zaufanych i następnie dokonują kradzieży wszystkich środków finansowych, zgromadzonych na rachunku ofiary.

Przeprowadzona analiza *modus operandi* sprawców przestępstw dokonywanych za pośrednictwem internetowych portali sprzedażowych pozwala identyfikować różne mechanizmy przestępcze. Należy zaznaczyć, że przedstawiony powyżej ogólny podział *modus operandi* nie obejmuje całego katalogu możliwych sposobów dokonywania przestępstw. Sposoby działania sprawców przestępstw

[21] Istnieje wiele sposobów na pozyskanie danych osobowych. Zagadnienie to wykracza jednak poza zakres przedmiotowego opracowania.

internetowych ulegają i będą ulegać ciągłym modyfikacjom, są i będą zależne od pomysłowości i wiedzy przestępców, a przede wszystkim od rozwoju nowych usług i narzędzi internetowych.

Należy jednak podkreślić, że elementem niezmiennym w opisywanych sposobach działania jest wykorzystywanie cudzych danych osobowych, m.in. do zakładania rachunków bankowych czy też kont na internetowych portalach sprzedaży. Taki sposób postępowania pozwala oszustom na zachowanie pełnej anonimowości i utrudnia realizację czynności wykrywczych i dowodowych.

Czynności wykrywczo-dowodowe

Oszustwa popełniane w Internecie uznawane są za trudne do ścigania. Zarówno proces wykrywczy, jak i dowodowy wymagają stałego współdziałania pokrzywdzonego z organami ścigania i wymiarem sprawiedliwości[22]. Z punktu widzenia możliwości szybkiego wykrycia sprawcy i wyjaśnienia niezbędnych okoliczności sprawy istotne znaczenie mają informacje oraz źródła dowodowe uzyskiwane w pierwszej fazie postępowania przygotowawczego, w szczególności dzięki właściwemu przyjęciu zawiadomienia o przestępstwie.

Szybkość reakcji na przestępstwa internetowe jest sprawą kluczową z uwagi na zmiany i ulotność danych cyfrowych, które należy zabezpieczyć w celu zgromadzenia niezbędnego materiału dowodowego. W tym kontekście istotna jest znajomość *modus operandi* sprawcy, jak również samych przestępstw i ich znamion ustawowych, aby wiedzieć, w jaki sposób przyjąć zawiadomienie o popełnieniu przestępstwa oraz zaplanować dalsze czynności wykrywczo-dowodowe.

W świetle dotychczasowej wiedzy autorów, a także informacji zgromadzonych na podstawie analizy literatury przedmiotu, skuteczne czynności wykrywczo-dowodowe w zakresie ścigania oszustw z wykorzystaniem internetowych portali sprzedażowych (z zasady) mogą i powinny obejmować następujące po sobie działania[23]:

- przyjęcie zawiadomienia o przestępstwie;
- nawiązanie kontaktu z portalem internetowym w celu uzyskania wszelkich informacji dotyczących konta użytkownika, za którego pośrednictwem dokonano przestępstwa;
- próba nawiązania kontaktu z osobą, której dane zostały zamieszczone w ofercie sprzedaży;

---

22 K. Witek, *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka" 2018, nr 2(24), s. 44.

23 D. Taberski, *Postępowania w sprawach o oszustwa popełnione za pośrednictwem Internetu*, „Prokuratura i Prawo" 2018, nr 6, s. 65–68.

- po uzyskaniu danych dotyczących konta użytkownika, w szczególności adresu IP, wydanie postanowienia o wszczęciu dochodzenia;
- przesłanie akt sprawy do prokuratury w celu wydania postanowienia o zwolnieniu z tajemnicy telekomunikacyjnej i żądaniu wydania danych informatycznych;
- wystąpienie do właściwego miejscowo sądu okręgowego w celu wydania postanowienia o uchyleniu tajemnicy bankowej;
- wydanie kolejnych postanowień w celu uzyskania od dostawcy usług internetowych informacji w zakresie numerów IP przypisanych do sprzętu wykorzystywanego przez sprawcę w trakcie logowań do bankowego serwisu transakcyjnego;
- analiza akt postępowania pod kątem możliwości przekazania sprawy prokuraturze właściwej miejscowo ze względu na miejsce działania sprawcy;
- w razie potrzeby wydanie kolejnych postanowień o zwolnieniu z tajemnicy telekomunikacyjnej, np. w celu ustalenia numerów kart SIM abonentów, z którymi łączył się sprawca;
- przeprowadzenie czynności procesowych z właścicielem rachunku bankowego, właścicielem przejętego konta na portalu aukcyjnym lub osobą, której tożsamość została wykorzystana dla celów działalności przestępczej, w szczególności przeszukanie miejsca jej zamieszkania i zabezpieczenie urządzeń, które mogły być wykorzystane do popełnienia przestępstwa;
- ustalenie miejsca zamieszkania (pobytu) osoby/osób, których dane zostały wykorzystane przez przestępcę w celu rejestracji karty lub kart SIM;
- przesłuchanie abonentów telefonów, którzy (według historii połączeń) kontaktowali się z numerem telefonu sprawcy;
- podjęcie próby ustalenia, czy inne jednostki prowadzą postępowania w sprawie przestępstw popełnionych przez tego samego sprawcę;
- podjęcie decyzji o ewentualnym przedstawieniu zarzutów;
- realizacja czynności z podejrzanym, gromadzenie danych osobopoznawczych oraz wykonywanie czynności kończących postępowanie.

Proces wykrywczo-dowodowy w sprawach dotyczących przestępstw internetowych wymaga realizacji wielu czasochłonnych czynności. Nie dziwi więc fakt, że najwięcej postępowań przygotowawczych w sprawach o przestępstwa internetowe, zakończonych skierowaniem aktu oskarżenia i prawomocnym skaza-

niem, trwało około roku[24]. Istniejąca sytuacja z pewnością nie wpływa korzystnie na szeroko rozumianą efektywność i skuteczność postępowań karnych. Sprawna realizacja czynności wykrywczych i dowodowych zwiększa szansę wykrycia i zatrzymania przestępcy. Analizując przedstawiony w artykule proces wykrywczo-dowodowy, wśród przyczyn przewlekłości omawianych czynności można w szczególności wymienić:

- nieprawidłowości w trakcie przyjmowania zawiadomienia o przestępstwie, co przejawia się brakiem w sporządzanej dokumentacji istotnych informacji na temat popełnionego oszustwa,
- realizację czynności w zakresie ustalenia, czy inne podmioty prowadzą postępowania w sprawie przestępstw popełnionych przez tego samego sprawcę. Czynności te wiążą się z opracowaniem i przesłaniem zapytań do innych jednostek organizacyjnych Policji oraz
- powielanie czynności procesowych w związku z prowadzeniem wielu równoległych postępowań przez różne jednostki prokuratury i Policji.

Podsumowanie

Analiza bieżących tendencji wskazuje szybki wzrost przestępczości z wykorzystaniem zaawansowanych technologii informatycznych obejmujących coraz więcej dziedzin życia społecznego i gospodarczego. Internet – dzięki możliwościom, jakie oferuje użytkownikom – odgrywa coraz większą rolę w nielegalnej działalności lub w znaczny sposób ułatwia jej prowadzenie. Handel przedmiotami uzyskanymi w wyniku przestępstwa, oszustwa internetowe czy też przestępczość z wykorzystaniem elektronicznych instrumentów płatniczych to tylko niektóre z czynów, jakie można popełnić, nie wychodząc z domu i nie narażając się na bezpośredni kontakt ze swoją ofiarą, przypadkowym świadkiem czy przedstawicielami organów ścigania. Przewiduje się dalszy wzrost przestępczości związanej z wykorzystaniem zaawansowanych technologii informatycznych. W szczególności, z uwagi na aktualne trendy wynikające z ustalonych danych statystycznych, rósł będzie stopień wykorzystania technologii komputerowej do popełniania „tradycyjnych" przestępstw. Ze względu na mało skomplikowany i prosty do zrealizowania przebieg tych czynów należy spodziewać się wzrostu liczby oszustw dokonywanych z wykorzystaniem platform handlowych i portali aukcyjnych. W najbliższych latach, jak można przypuszczać, wzrośnie obrót na aukcjach internetowych i serwisach darmowych ogłoszeń, gdyż coraz więcej osób poszukuje tzw. zakupowych okazji, z kolei inni będą sprzedawać przedmio-

[24] Ibidem, s. 70.

ty codziennego użytku, które są im zbędne, lub w celu poprawy stanu budżetu domowego, co bezpośrednio może się przełożyć na wzrost liczby przestępstw internetowych. W uzupełnieniu zatem zaprezentowanych rozważań teoretycznych możliwe jest przedstawienie kilku rekomendacji w celu zwiększenia skuteczności organów ścigania w kontekście oszustw internetowych.

Organy ścigania powinny stale przygotowywać się do reakcji na przyszłe działania przestępcze. Tylko funkcjonariusze mający właściwe przygotowanie merytoryczne będą mogli nawiązać właściwą współpracę z informatykami, administratorami baz danych, portali i sieci komputerowych, co umożliwi im skuteczne ściganie tego typu czynów. W tym kontekście należy podkreślić potrzebę szkolenia i nieustającego podnoszenia poziomu wiedzy funkcjonariuszy Policji.

Biorąc pod uwagę różnorodne możliwości sprawców w zakresie *modus operandi*, należy zauważyć, że nie sposób przedstawić pełny ich katalog. Niezależnie jednak od tego, w jaki sposób doszło do wprowadzenia pokrzywdzonego w błąd w konkretnej sprawie, wspólnym elementem wszystkich oszustw jest doprowadzenie do niekorzystnego rozporządzenia mieniem. W przypadku oszustw popełnianych za pośrednictwem sieci wiąże się to z koniecznością zdalnego przekazania środków pieniężnych na któryś z dostępnych sposobów. Te zaś są znacznie mniej różnorodne, co umożliwia ich wnikliwe badanie w celu optymalizacji działań wykrywczych.

Niezależnie od tego niezbędna jest także szeroko rozumiana edukacja społeczna. Najlepszym rozwiązaniem w zakresie zwalczania przestępczości internetowej jest wiedza i świadomość użytkowników Internetu na temat potencjalnych zagrożeń[25], która umożliwi skuteczną prewencję na poziomie indywidualnym. Konieczne jest zatem edukowanie społeczeństwa w celu minimalizowania liczby oszustw oraz zwiększenia wiedzy i świadomości w zakresie czyhających niebezpieczeństw. Użytkownicy Internetu powinni mieć świadomość istniejącego ryzyka, a także znać algorytm postępowania w przypadku, gdyby stali się ofiarą oszustwa.

Problemem nie są więc wyłącznie regulacje prawne, ale czynniki ludzkie, a także szybkość i skuteczność reakcji organów ścigania i wymiaru sprawiedliwości, w szczególności umiejętne przyjęcie zawiadomienia o przestępstwie oraz prawidłowe postawienie zarzutów związanych ze zrozumieniem materii oszustwa. Nie ulega jednak wątpliwości, że dobre, precyzyjne regulacje pomogłyby skutecznie karać przestępców i chronić ofiary, ale jak wynika z przedstawionych przykładów, najbardziej zawodnym czynnikiem jest człowiek[26].

---

[25] A. Prokopowicz, *Charakterystyka cyberprzestępczości – zagadnienia wybrane*, w: M. Maciąg, K. Maciąg (red.), *Kryminalistyka i kryminologia – najnowsze doniesienia*, Wydawnictwo Naukowe Tygiel, Lublin 2019, s. 165.

[26] K. Siwicki, *Prawo karne wobec oszustw i innych związanych z nimi przestępstw w handlu,*

Streszczenie

Działania wielu sprawców współczesnych oszustw oparte są na wykorzystaniu internetowych portali sprzedażowych. Szczegółowy sposób działania sprawców jest zróżnicowany w zależności od funkcjonalności konkretnych platform oraz docelowej grupy osób pokrzywdzonych. Wspólne elementy *modus operandi* sprawców takich czynów mają bezpośredni wpływ na skuteczność procesów wykrywczych. W niniejszym opracowaniu zaprezentowany został opis współczesnego *modus operandi* sprawców typowych oszustw popełnianych za pośrednictwem internetowych portali sprzedażowych, ze wskazaniem potencjalnych problemów w pracy wykrywczej i dowodowej oraz z podaniem sposobów ich rozwiązywania. Opis ten uzupełniony jest aktualnymi danymi na temat skali występowania tego rodzaju czynów pochodzącymi z analizy danych statystycznych oraz przeprowadzonych badań aktowych.

Słowa kluczowe: cyberprzestępczość, oszustwo komputerowe, oszustwo internetowe, *modus operandi*

Summary

Online sales portals are commonly used to commit fraud. Specific methods of perpetrator's operations vary, depending on the available functionalities of a given sales platform and specific features of targeted victims. However, there are several common elements of modus operandi shared by most online fraud perpetrators. These elements have a direct impact on the potential effectiveness of the investigative process. This presents the typical elements of modus operandi of a perpetrator of a fraud committed online via sales portals. The description is supplemented by a specific list of the existing investigative problems and potential methods of solving them. Presented practical information is illustrated with up-to-date data on the scale of the occurrence of such acts based on statistical data analysis and an analysis of criminal cases files.

Keywords: cybercrime, computer fraud, internet fraud, modus operandi

Bibliografia

Literatura

Adamski A., *Prawo karne komputerowe*, Wydawnictwo C.H. Beck, Warszawa 2000.

Chmiel A., *Przestępstwa związane z wykorzystaniem komputera – charakterystyka zagadnienia*, „Palestra" 1991, nr 10.Hanausek T., *Modus operandi i alibi*, „Studia Kryminologioczne, Kryminalistyczne i Penitencjarne" 1978, nr 8.

Kosiński J., *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015.

Lewulis P., *Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 2021.

Lizut J., *Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecz-*

w: M. Zieliński (red.), Przegląd Nauk Stosowanych nr 10, Wydział Ekonomii i Zarządzania, Opole 2016, s. 119.

nych, Wydawnictwo Wyższej Szkoły Pedagogicznej im. Janusza Korczaka, Warszawa 2014.

Parker D.B., *Crime by Computer*, Scribner, New York 1976.

Pączkowski T., *Słownik cyberbezpieczeństwa*, Szkoła Policji, Katowice 2017.

Prokopowicz A., *Charakterystyka cyberprzestępczości – zagadnienia wybrane*, w: M. Maciąg, K. Maciąg (red.), *Kryminalistyka i kryminologia – najnowsze doniesienia*, Wydawnictwo Naukowe Tygiel, Lublin 2019.

Rajput B.K., *Understanding modus operandi of the cyber economic crime from people- process-technology framework's perspective*, „Journal of Emerging Technologies and Innovative Research" 2018, t. 5(3).

Sąsiada M., *Modus operandi jako środek identyfikacji sprawcy przestępstwa*, „Wrocławskie Studia Erazmiańskie. Zeszyty Studenckie" 2008, z. 1.

Siwicki K., *Prawo karne wobec oszustw i innych związanych z nimi przestępstw w handlu*, w: M. Zieliński (red.), Przegląd Nauk Stosowanych nr 10, Wydział Ekonomii i Zarządzania, Opole 2016.

Solarz A., *Zagadnienie przestępczości zawodowej w Polsce*, Państwowe Wydawnictwo Naukowe, Warszawa 1967.

Taberski D., *Postępowania w sprawach o oszustwa popełnione za pośrednictwem Internetu*, „Prokuratura i Prawo" 2018, nr 6.

Witek K., *Przestępczość komputerowa – aspekty prawne*, „Edukacja – Technika – Informatyka" 2018, nr 2(24).

Źródła internetowe

Główny Urząd Statystyczny, *Jak korzystamy z Internetu? 2019*, GUS 2020, https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/5/10/1/jak_korzystamy_z_internetu_2019_.pdf (dostęp 19.10.2020).

Izba Gospodarki Elektronicznej, *E-commerce w Polsce 2019*, https://eizba.pl/wp-content/uploads/2019/07/raport_GEMIUS_2019-1.pdf (dostęp 19.10.2020).

Janoś K., *Koronawirus sprzyja e-commerce. Sprzedaż w sieci może być dwukrotnie większa niż przed rokiem*, https://www.money.pl/gospodarka/koronawirus-sprzyja-e-commerce-sprzedaz-w-sieci-moze-byc-dwukrotnie-wieksza-niz-przed-rokiem-6522842250507905a.html (dostęp 19.10.2020).

Jarrett H.M., Bailie M.W., Hagen E., Eltringham S., *Prosecuting Computer Crimes*, US Department of Justice 2008, https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (dostęp 19.10.2020).

Kaczyńska D., *Pandemia internetowych oszustów. Oto ciemna strona boomu na e-sklepy*, https://www.forbes.pl/biznes/falszywe-sklepy-internetowe-oszusci-wykorzystuja-pandemie-koronawirusa/f3y2pcz (dostęp 19.10.2020).

Komenda Główna Policji, *Uwagi* i definicje – statystyka, http://statystyka.policja.pl/download/20/232288/Uwagiidefinicje.docx (dostęp 19.10.2020).

Raport roczny 2019 z działalności CERT Polska, https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf (dostęp 19.10.2020).

Wkład poszczególnych autorów

dr Piotr Lewulis, Katedra Kryminalistyki Wydział Prawa i Administracji Uniwersytet Warszawski: autor korespondencyjny, konceptualizacja, gromadzenie danych, analiza ilościowa, wizualizacja, przygotowanie tekstu,

dr Paweł Olber, Instytut Służby Kryminalnej Wyższa Szkoła Policji w Szczytnie: konceptualizacja, gromadzenie danych analiza jakościowa, wizualizacja, przygotowanie tekstu.

Konflikt interesów

Brak

Źródło finansowania

Brak