

**MORSKIE CENTRUM  
CYBERBEZPIECZEŃSTWA**

**Cybersecurity  
& Cybercrime**

NUMER SPECJALNY 2025/2 (8)

**PRZESTĘPCZOŚĆ  
TELEINFORMATYCZNA  
2025**

**Redakcja:**

**Jerzy Kosiński**

**Jakub Syta**

**Alicja Żukowska**

**GDYNIA 2025**

**MORSKIE CENTRUM  
CYBERBEZPIECZENSTWA**

# **Cybersecurity & Cybercrime**

NUMER SPECJALNY 2025/2 (8)

**PRZESTĘPCZOŚĆ  
TELEINFORMATYCZNA**

**2024**

**Redakcja:**

**Jerzy Kosinski**

**Jakub Syta**

**Alicja Zukowska**

GDYNIA 2025

**Redaktor naczelny czasopisma:** dr inż. Jakub Syta

**Projekt okładki:** mgr inż. Łukasz Grzyb

**Recenzenci:**

prof. dr hab. Krzysztof FICOŃ

dr hab. Bartłomiej PAŃCZEK, prof. Akademii Marynarki Wojennej w Gdyni

dr hab. Jacek BIL

Wszystkie artykuły dostępne są w Otwartym Dostępie (Open Access) na licencji CC BY-NC-ND (Attribution – Non-Commercial – No Derivative Works). Poglądy wyrażone w artykułach nie zawsze są zgodne z poglądami redaktora naczelnego, rady naukowej i recenzentów.

**Wydawca: Morskie Centrum Cyberbezpieczeństwa  
Akademia Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni**

ISSN (druk) 2720-4251

ISSN (online) 2720-426X

**Współwydawca: Wydział Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej  
im. Bohaterów Westerplatte w Gdyni**

## SPIS TREŚCI

Jerzy KOSIŃSKI Jakub SYTA Alicja Żukowska SŁOWO WSTĘPNE	5
Krzysztof LIDERMAN, Artur KSIĘŻOPOLSKI CYBERBEZPIECZEŃSTWO ŁAŃCUCHA DOSTAW	9
Bartosz CIEŚLIK GENAI W CYBERBEZPIECZEŃSTWIE	28
Tomasz JANCZEWSKI WYKORZYSTANIE SZTUCZNEJ INTELIGENCJI DO ANALIZY LOGÓW SERWERA W CELU WYKRYWANIA ANOMALII	51
Jacek CHARATYNOWICZ MIEJSCE RYNKU KRYPTOAKTYWÓW W SYSTEMIE FINANSOWYM RP	63
Tomasz PAWLICKI ANALIZA BLOCKCHAIN – JAK ZROZUMIEĆ ELEKTRONICZNE PRZEPIŁY	76
Adam BEHAN, Wiktoria SZYBIAK MODEL ZABEZPIECZENIA KRYPTOWALUT W TOKU POSTĘPOWANIA KARNEGO W ŚWIELE WYTYCZNYCH PROKURATURY KRAJOWEJ – ANALIZA I PROPOZYCJE ZMIAN	106
Aleksandra SZYNCZEWSKA, Szymon JASIŃSKI OSZUSTWA Z WYKORZYSTANIEM TOKENÓW PODSZYWAJĄCYCH SIĘ POD POPULARNE KRYPTOAKTYWA	126
Zbigniew JAKUBOWSKI, Grzegorz MARCZAK RADIO FORENSICS - NETWORK ANALYSIS USING (IN)EXPENSIVE HARDWARE AND WIFI 6/6E/7 REVOLUTION	144
Jędrzej GRODZICKI AGENT ROZLICZENIOWY JAKO ELEMENT SYSTEMU BEZPIECZEŃSTWA INSTRUMENTÓW PŁATNICZYCH	159
Wojciech PILSZAK INFORMACJE PRZECHOWYWANE ELEKTRONICZNIE A OPINIA Z INFORMATYKI ŚLEDZCZEJ	167
Maciej SZMIT PRZESTĘPCZOŚĆ TELEINFORMATYCZNA - GARŚĆ STATYSTYK	180

Luiza PISKOREK OCHRONA INTERNETU PRZED NIELEGALNYMI TREŚCIAMI - PIRACTWO TREŚCI AUDIOWIZUALNYCH ONLINE	194
Krystian WOJCIECHOWSKI SAMOLOTY, OSINT I WIELKA POLITYKA	224
Kamil KOŁODZIEJCZYK WALKA Z ANALIZĄ – WYBRANE MECHANIZMY OCHRONNE MALWARE I SPOSOBY ICH NEUTRALIZACJI	263
Grzegorz TWOREK ZABEZPIECZANIE DANYCH ULOTNYCH W SYSTEMACH WINDOWS	277
Paulina TUREK, Piotr DELA OPRACOWANIE WPŁYWU KORZYSTANIA ZE SMARTFONÓW PRZEZ UCZNIÓW PAŃSTWOWYCH SZKÓŁ PODSTAWOWYCH NA TERENIE GMINY MIASTA KRAKÓW.	281
Agnieszka CENZARTOWICZ JAK UGOTOWAĆ ŻABĘ I UPOŁOWAĆ JEDNOROŻCA?	296
Łukasz WARCHAŁ DOPUSZCZALNOŚĆ ZASTOSOWANIA ART. 40 USTAWY O SŁUŻBIE KONTRWYWIADU WOJSKOWEGO I SŁUŻBIE WYWIADU WOJSKOWEGO W RAMACH OSŁONY KONTRWYWIADOWCZEJ WŁASNYCH STRUKTUR	304

## SŁOWO WSTĘPNE

Szanowni Państwo,

Tradycyjnie, przez trzy dni poprzedzające Boże Ciało, czyli w dniach 27–29 maja 2024 roku, na terenie Akademii Marynarki Wojennej im. Bohaterów Westerplatte odbyła się konferencja „Przestępczość Teleinformatyczna”. Partnerami organizacyjnymi konferencji byli:

- Allegro Sp. z o.o.
- zondacrypto
- Bankowe Centrum Cyberbezpieczeństwa ZBP
- VS Data
- LexisNexis Risk Solutions

w partnerstwie merytorycznym z:

- Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni
- Centralne Biuro Zwalczania Cyberprzestępczości
- Departament do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej
- Stowarzyszenie Sygnał
- Fundacja Przeciwdziałania Cyberprzestępczości
- Polska Platforma Bezpieczeństwa Wewnętrznego
- Polska Sekcja IEEE.

Wydarzenie – również tradycyjnie – zgromadziło ponad 400 ekspertów z kraju i zagranicy: przedstawicieli służb publicznych, podmiotów świadczących usługi elektroniczne, administracji publicznej, sektora bankowego, firm technologicznych oraz środowiska naukowego. Program konferencji obejmował wykłady i dyskusje podzielone na 14 sesji tematycznych oraz cztery różne warsztaty, w tym ćwiczenia typu „cyber-polygon”.

Pierwszy dzień konferencji rozpoczął się uroczystym otwarciem, podczas którego głos zabrali m.in.: kontradmirał prof. dr hab. Tomasz Szubrycht (Rektor-Komendant Akademii Marynarki Wojennej), Dominik Rozdziałowski (Departament Cyberbezpieczeństwa MON), nadinsp. Adam Cieślak (Komendant Centralnego Biura Zwalczania Cyberprzestępczości) oraz Bogna Niklasiewicz (Dyrektor Działu Trust and Safety w Allegro.pl). W swoich wystąpieniach podkreślali rosnące znaczenie walki z cyberprzestępczością.

Następnie Mariusz Tokarski (Allegro) podzielił się praktycznymi doświadczeniami z zakresu przeciwdziałania oszustwom na platformach e-commerce, a Sean Cooper (Team Cymru) omówił najnowsze taktyki obfuskacji, czyli ukrywania złośliwych działań w sieci, oraz metody ich wykrywania. Prezentacja ukazała, jak cyberprzestępcy wykorzystują coraz bardziej zaawansowane techniki, by utrudnić identyfikację i neutralizację zagrożeń. Pierwszy blok zakończyło wystąpienie Krzysztofa Lidermana i Artura Książepolskiego (NASK), którzy zwrócili uwagę na problematykę bezpieczeństwa łańcuchów dostaw.

W dalszej części odbyły się sesje równoległe. W sesji anglojęzycznej Jindrich Karasek (Trend Micro) przedstawił koncepcję „Web of Cognitive Warfare”, czyli wojny

kognitywnej prowadzonej w cyberprzestrzeni, gdzie celem ataków jest manipulacja percepcją i zachowaniami użytkowników. Robert Kośla (Microsoft) omówił relacje pomiędzy sztuczną inteligencją a cyberodpornością, rozważając, czy jest to prawdziwa sprzeczność, czy raczej symbioza.

Równolegle, w ramach sesji bankowej, Agnieszka Gryszczyńska (Prokuratura Krajowa) analizowała wpływ nowych regulacji dotyczących zwalczania nadużyć w komunikacji elektronicznej na sektor bankowy, a Piotr Marek Balcerzak (ZBP) oraz Łukasz Wołoncej (DataWalk S.A.) zaprezentowali zastosowanie analizy grafowej w walce z cyberprzestępczością finansową. Na koniec sesji przedstawiciel mBank przedstawił prezentację pt. „Mechanizmy obronne i wektory ataków na klientów bankowości elektronicznej”.

Po południu, podczas sesji ogólnej, Wojciech Pliszak podzielił się swoimi – niekoniernie pozytywnymi – doświadczeniami praktycznymi z zakresu przeciwdziałania cyberprzestępczości. Kolejne prezentacje dotyczyły m.in. scamów z wykorzystaniem transakcji autoryzowanych – APP (Maciej Jamiołkowski, LexisNexis), aktualnych przypadków oszustw internetowych („Nie klikaj, nie otwieraj, nie patrz – katastrofa internetu”, Bartosz Kwitkowski, Prebytes) oraz przerażającej wizji końca prywatności związanej ze wspieranym komputerowo profilowaniem psychologicznym, przedstawionej przez Michała Kosińskiego (Stanford University).

W trakcie sesji bankowej Roman Kielich (Euronet) przedyskutował zagadnienia dotyczące bezpieczeństwa logicznego bankomatów, a Robert Pogorzelski (PKO BP) przedstawił prezentację pt. „Publiczna infrastruktura oczami napastnika – narzędzia i źródła danych”.

Drugiego dnia rano odbywały się równolegle cztery sesje. W pierwszej, prowadzonej przez przedstawicieli Stowarzyszenia Sygnał, dyskutowano takie tematy jak: „Web blocking/dynamic blocking/live blocking – o kierunkach zmian regulacyjnych i systemowych w Europie w zakresie natychmiastowego blokowania dostępu do nielegalnych treści” (Teresa Wierzbowska), „Blokowanie stron pirackich – aspekty prawne i doświadczenia innych krajów europejskich” (Luiza Piskorek) oraz „Przegląd najciekawszych realizacji w zakresie streamingu i sharingu w minionym roku” (Piotr Wójtów).

Druga sesja obejmowała prezentacje: Piotra Olewniczaka (Enigma Systemy Ochrony Informacji) – „Najlepszą formą obrony przed cyberzagrożeniami jest atak”, Michała Jarskiego (Forcepoint) – „Gdzie się podziały moje dane, czyli do czego służy DSPM?”, Wojciecha Ryżowskiego (Ministerstwo Finansów) – „Rola informacji o transakcjach ponadprogowych w zwalczaniu przestępczości” oraz Tomasza Boronia i Pawła Brządkiewicza (CBZC Bydgoszcz) – „Discord – analiza struktury bazy danych”.

Równocześnie odbywały się cztery warsztaty. Tomasz Janczewski (Akademia Marynarki Wojennej) podzielił się doświadczeniami z zakresu „Bezpiecznego kodowania aplikacji webowych”. Przedstawiciele ZBP, CDeX oraz Akademii Marynarki Wojennej przygotowali cyberćwiczenia dla sektora bankowego – CyberFIGHT Bank.01-2024. Grzegorz Tworek (Standard Chartered Bank) poprowadził warsztaty dotyczące „Zabezpieczania danych ulotnych w systemach Windows”. Ostatni warsztat prowadził Piotr Olewniczak (Enigma) – „Najlepszą formą obrony przed cyberzagrożeniami jest atak... z użyciem platformy Fidelis Elevate. Najlepsze praktyki przewidywania, mitygacji, analizy i odpowiedzi”.

Południowy blok techniczny zawierał prezentacje: „Zabezpieczanie danych ulotnych w systemach Windows” (Grzegorz Tworek, Standard Chartered Bank), „Dekodowanie informacji w ruchu sieciowym” (Aleksander Goszczycki, Matie) oraz „Zdalne zabezpieczanie dowodów cyfrowych” (Kacper Kulczycki, HSDR&C Kacper Kulczycki).

W bloku dotyczącym kryptowalut usłyszeliśmy prezentacje: „Oszustwo z wykorzystaniem fałszywych tokenów kryptowalutowych” (Aleksandra Szynczewska, Szymon Jasiński – zondacrypto), „The Landscape of Current Cryptocurrency Crimes and Trends” (Nina Waldman, Marco Basile – Chainalysis), „Wpływ rozwoju rynku kryptoaktywów na sektor finansowy” (Jacek Charatynowicz – Centralne Biuro Śledcze Policji) oraz „Procesowe i praktyczne aspekty zabezpieczania walut wirtualnych” (Sławomir Sol – Prokuratura Okręgowa w Gliwicach).

Wieczorny blok dotyczył analizy powłamaniowej. Tomasz Janczewski (Akademia Marynarki Wojennej) przedstawił prezentację „Securing Web Applications in the Face of Evolving Cybercrime”, Krzysztof Bińkowski (NetKomputer, Akademia Marynarki Wojennej) wygłosił wykład „Paluszek i główka to... – czyli NIE/BEZPIECZNA biometryka w urządzeniach mobilnych z perspektywy użytkownika i informatyki śledczej”, Witold Sobolewski (VS DATA) podzielił się najnowszymi doświadczeniami podczas prezentacji „Ransom mnie strzela”, Bartosz Trybus (CERT Polska) przedstawił narzędzie do analizy powłamaniowej, a Łukasz Wołoncej i Wojciech Wesołowski (DataWalk) zaprezentowali case study dotyczące „Analizy danych niestrukturalnych OSINT w śledztwach dotyczących zbrodni wojennych”.

Trzeci, ostatni dzień konferencji, również obfitował w wartościowe i merytoryczne wystąpienia. Jack McCurley (Recorded Future) przedstawił krajobraz chińskich cyberzagrożeń. Mateusz Chrobok (Mangopay) wraz z Michałem Barbasiem omówili zjawisko „Fraud as a Service w rosyjskim darkniecie”. Następnie Betina Tynka (Mediarecovery) opowiedziała o możliwościach zastosowania generatywnej sztucznej inteligencji w OSINT, Krzysztof Wosiński zaprezentował „Geolokalizację – OSINT-owe techniki wyszukiwania miejsca wykonania zdjęcia/filmu”, a Krystian Wojciechowski (CTB AGH Kraków) pokazał, co źródła otwarte mówią o ruchu samolotów i statków.

Podczas drugiego bloku uczestnicy mogli wysłuchać prezentacji „Podsumowanie warsztatów bankowych” prowadzonej przez organizatorów – przedstawicieli Związku Banków Polskich oraz Akademii Marynarki Wojennej. Piotr Weroicy przedstawił case study „Atak Ransomware (LockBit) na małą firmę IT”. Następnie Agnieszka Cenzarowicz oraz Piotr Warsicki (SWC Group) zaprezentowali prezentację pt. „Jak „odpalić” start-up i ująć z tym na sucho – przewodnik”, a Dariusz Podufalski i Michał Mikulski (Prokuratura Okręgowa w Bydgoszczy) przedstawił case study „Serwujemy DDoS, atak jako usługa – modus operandi i zabezpieczanie danych”. Na koniec Jakub Syta (Akademia Marynarki Wojennej) przedstawił wnioski dotyczące cyberwojny, bazując na doświadczeniach z wojny na Ukrainie.

Ostatni wspólny blok konferencji tradycyjnie związany był z uczelniami i projektami badawczymi. Jacek Czech (CTB AGH Kraków) przedstawił aktywności AGH w obszarze bezpieczeństwa, Adam Czubak (Uniwersytet Opolski) zaprezentował projekt CyberEva, a Marek Wierzbicki oraz Klaudia Kaczmarek (Polska Platforma Bezpieczeństwa Wewnętrznego) przedstawił prezentację „Project CYCLOPS. Stowarzyszenie EACTDA – project Tools4LEAs”.

Wszystkie wystąpienia prezentowały wysoką wartość merytoryczną. Szereg referatów znajduje się w niniejszej publikacji. Ostatecznie udało się zgromadzić 18 tekstów dotyczących różnych zagadnień związanych z przeciwdziałaniem cyberprzestępczości oraz zapewnianiem cyberbezpieczeństwa. Poruszane tematy są bardzo szerokie – od bezpieczeństwa łańcucha dostaw i osłony kontrwywiadowczej, przez kryptografię, aż po zabezpieczanie danych ulotnych czy generatywną AI. Wierzymy, że każdy czytelnik znajdzie coś wartościowego dla siebie.

dr hab. inż. Jerzy Kosiński, prof. AMW  
dr inż. Jakub SYTA  
dr Alicja Żukowska

Morskie Centrum Cyberbezpieczeństwa  
Akademia Marynarki Wojennej w Gdyni

# CYBERBEZPIECZEŃSTWO ŁAŃCUCHÓW DOSTAW

## SUPPLY CHAIN CYBERSECURITY

Krzysztof LIDERMAN<sup>1</sup>, Artur KSIĘŻOPOLSKI<sup>2</sup>

### Streszczenie:

W artykule odniesiono się do zawartości podstawowych aktów prawnych unijnych z zapisami dotyczącymi łańcuchów dostaw, które od października 2024 roku powinny być zaimplementowane w przepisach prawa krajowego. Wskazano także istotne standardy i normy zawierające zalecenia dotyczące łańcuchów dostaw. Przedstawiono operacyjne (użyteczne z technicznego punktu widzenia) definicje cyberprzestrzeni i cyberbezpieczeństwa, niezbędne do zdefiniowania cyfrowych łańcuchów dostaw oraz zaproponowano sposób ich formalnego opisu. W części wstępnej zamieszczono krótki rys historyczny rozwoju interpretacji pojęcia „dostawa”.

**Słowa kluczowe:** łańcuch dostaw, cyfrowy łańcuch dostaw, klasyfikacja łańcuchów dostaw, modelowanie łańcuchów dostaw, cyberbezpieczeństwo.

### Summary:

The article refers to the content of basic EU legal acts with provisions on supply chains, which should be implemented in national law from October 2024. It also identifies relevant standards and norms with recommendations for supply chains. Operational (technically useful) definitions of cyberspace and cybersecurity, necessary to define digital supply chains, are presented and a way of formally describing them is proposed. The introductory part provides a brief historical outline of the development of the interpretation of the term "supply".

**Keywords:** supply chain, digital supply chain, supply chain classification, supply chain modeling, cybersecurity.

### WSTĘP

Impulsem do podjęcia prezentowanej w artykule tematyki są zapisy w dokumentach unijnych dotyczące łańcuchów dostaw, które to dokumenty do października 2024 roku powinny być zaimplementowane do systemów prawnych krajów unijnych. W kolejnych rozdziałach niniejszego artykułu autorzy starali się dać odpowiedź na następujące pytania:

1. Jakie są uznane definicje łańcucha dostaw?
2. Jak można poklasyfikować łańcuchy dostaw?
3. Jakie są podstawowe elementy łańcucha dostaw?
4. Jak można formalnie opisać łańcuch dostaw?

---

<sup>1</sup> PIB-NASK, krzysztof.liderman@nask.pl, ORCID: 0000-0002-0004-5095.

<sup>2</sup> PIB-NASK, artur.ksiezopolski@nask.pl.

## 5. Co to jest „cyberbezpieczeństwo łańcucha dostaw”?

Poza tym, w rozdziale II zamieszczono krótki rys historyczny rozwoju interpretacji pojęcia „dostawa”, a w rozdziale III wskazano publikacje unijne, normy międzynarodowe i standardy (np. organizacji ISO oraz NIST) z których warto korzystać przy zajmowaniu się tematyką łańcuchów dostaw.

W tym artykule będzie używane ogólne określenie „wrogi podmiot”. Może nim być podmiot indywidualny (jakaś osoba) lub grupowy (grupa przestępcza, służby obcego państwa, itp.) który celowo wykonuje działania przynoszące szkody podmiotowi, przeciwko któremu są skierowane. To określenie porządkuje dyskurs, ponieważ znaczeniowo obejmuje wszystkie popularne określenia takie jak adwersarz, intruz, haker, atakujący, cyberprzestępca itp. eliminując różnorodność nazw i jednocześnie nie blokując, w razie potrzeby, przypisania określonej roli wrogiemu podmiotowi.

## ŁAŃCUCH DOSTAW – HISTORIA

Modne dzisiaj pojęcie łańcucha dostaw ma długą historię. Można ją poznać śledząc np. zapiski historyczne lub współcześnie, zmiany w interpretacji słowa „dostawa” używanego w różnych normach i standardach. Przykładu historycznego dostarczają np. dzieje Imperium Rzymskiego. Za czasów Imperium Rzymskiego strategicznym towarem gwarantującym władzom spokój w Rzymie było zboże, sprzedawane mieszkańcom stolicy po niskich cenach lub rozdawane za darmo. Zboże było sprowadzane statkami głównie z Egiptu, zatem spokój w stolicy imperium zależał od regularności i wolumenu dostaw.

Jednak znacznie ważniejsze ze strategicznego punktu widzenia były nie dostawy żywności „dla ludu” ale przede wszystkim żywności, uzbrojenia, żołdu i rekrutów dla armii. Tutaj pojawia się nowe określenie, rozszerzające pojęcie dostawy – logistyka<sup>3</sup>. Już w starożytności zauważono, że zaopatrzenie armii (to inne słowo używane w kontekście „dostawa dóbr różnych niezbędnych do prowadzenia działań bojowych”) może decydować o wygranej. Historia logistyki jest ściśle związana z historią wojska, bo to właśnie wojsko potrzebowało i nadal potrzebuje ciągłego zaopatrzenia. W X w. bizantyjski cesarz Leon VI w swoim dziele pt.: *„Summaryczne wyłożenie sztuki wojennej”* wyróżnił obok strategii i taktyki, trzecią naukę wojenną – logistykę. Pisał, że jest rzeczą logistyki *„żeby żołd był wypłacany, wojsko odpowiednio uzbrojone i uszeregowane, wyposażone w sprzęt wojenny; żeby potrzeby wojska były dostatecznie i w odpowiednim czasie zaspokojone, a każda wyprawa wojenna odpowiednio przygotowana, tzn. przestrzeń i czas odpowiednio obliczone, obszar oszacowany z uwzględnieniem ruchu wojsk, a także siły oporu przeciwnika, i zgodnie z tymi funkcjami należy regulować i porządkować ruchy i podział własnych sił zbrojnych [7].*

---

<sup>3</sup> Źródło terminu „logistyka” można się doszukiwać w języku grackim i łacińskim: gr. *logistikós* (logistikos) – człowiek myślący według reguł logicznych; łac. *logisticus* – rozumiały, racjonalny, zdolny do logicznego myślenia.

Współczesne rozumienie logistyki związane jest z wydaną w 1837 roku przez A. H. Jominiego książką pt.: „Zarys sztuki wojennej” [6]. Opisał on logistykę jako praktyczną sztukę przemieszczania armii, obejmującą także ciągłe jej zaopatrywanie, prace inżynierskie i sztabowe. Szczęólnego znaczenia logistyka nabrała dla wojska w XX wieku, gdzie obie wojny światowe były prowadzone w skali globalnej, a zaopatrzenie armii odbywało się na olbrzymich przestrzeniach. Znaczenie ciągłości dostaw dla „być albo nie być” całych narodów dobitnie pokazuje bitwa o Atlantyk i niemieckie próby przerwania oceanicznych dostaw z USA do Wielkiej Brytanii, oraz przygotowanie lądowania aliantów w Normandii. To były m.in. powody, dla których podczas II wojny światowej Departament Obrony USA powołał specjalne zespoły, których zadaniem był rozwój matematycznych modeli planowania oraz ich zastosowanie w rozwiązywaniu problemów zaopatrzeniowych armii amerykańskiej. Były to też początki nauki znanej dziś pod nazwą badań operacyjnych, jak też ekonomicznej dyscypliny naukowej – logistyki.

Obszar cywilny logistiką zainteresował się dopiero na początku lat 50-tych XX wieku, gdy zaczęto łączyć produkcję z dystrybucją fizyczną wyprodukowanych dóbr w celu wypracowania większych zysków. Lata 60-te XX wieku w USA (w Europie lata 70-te) to próby usystematyzowania problemu planowania, produkcji, magazynowania i dystrybucji dóbr i współczesnego zdefiniowania procesu obejmującego te wszystkie działania [28].

Pod koniec tego okresu zaczęto dostrzegać, że na problem można spojrzeć z szerszej perspektywy – łańcucha dostaw. Najprostsza definicja łańcucha dostaw jest taka, że jest to zbiór procesów dostawy danego produktu. Procesy te dotyczą współpracy między producentami, dostawcami, dystrybutorami, partnerami handlowymi i konsumentami. Logistyka z kolei obejmuje pewien zespół operacji należących do łańcucha dostaw (czyli jest częścią łańcucha dostaw), zwykle magazynowanie, transport i zarządzanie zapasami [29].

Jak zatem można zauważyć, pojęcie „dostawy”, biorąc pod uwagę technikę komputerową, ewoluowało od dostawy **fizycznych** elementów na teren organizacji lub bezpośredniej dostawy elementów **programowych** do konkretnego odbiorcy, poprzez dostawę **usług** w ramach outsourcingu po współczesne pojęcie **łańcucha dostaw**, w ramach którego przepływa sprzęt, oprogramowanie i usługi.

## **PRZEGLĄD WYTYCZNYCH UNII EUROPEJSKIEJ ORAZ WYBRANYCH NORM I STANDARDÓW DOTYCZĄCYCH CYBERBEZPIECZEŃSTWA ŁAŃCUCHÓW DOSTAW**

Jak już wspomniano, impulsem do podjęcia prezentowanej w artykule tematyki są zapisy w dokumentach unijnych. W NIS2 [10] w art.21 (*Środki zarządzania ryzykiem w cyberbezpieczeństwie*) zapisano:

(...) 2. Środki, o których mowa w ust. 1, bazują na podejściu uwzględniającym wszystkie zagrożenia i mającym na celu ochronę sieci i systemów

informatycznych oraz środowiska fizycznego tych systemów przed incydentami, i obejmują co najmniej następujące elementy: (...)

d) **bezpieczeństwo łańcucha dostaw**, w tym aspekty związane z bezpieczeństwem dotyczące stosunków między każdym podmiotem a jego bezpośrednimi dostawcami lub usługodawcami;

W [24], powielającym w dużej części zapisy NIS2, w art.8 zapisano dodatkowo: (...)  
ust.3. Podmioty Unii stosują co najmniej następujące szczegółowe środki zarządzania ryzykiem w cyberprzestrzeni:

(...) g) **zabezpieczenie łańcucha dostaw oprogramowania** poprzez kryteria regulujące opracowywanie i ocenę bezpiecznego oprogramowania;

a w art.11: W ramach swoich obowiązków IICB w szczególności:

(...) s) przyjmuje zalecenia **w odniesieniu do bezpieczeństwa łańcucha dostaw**, o którym mowa w art. 8 ust. 2 akapit pierwszy lit. m), z uwzględnieniem wyników skoordynowanego na poziomie Unii **szacowania ryzyka krytycznych łańcuchów dostaw**, o którym mowa w art. 22 dyrektywy (UE) 2022/2555, w celu wsparcia podmiotów Unii w przyjmowaniu skutecznych i proporcjonalnych środków zarządzania ryzykiem w cyberprzestrzeni.

W CER [11] w art. 13 (*Środki w zakresie odporności wprowadzane przez podmioty krytyczne*) w ust.1 zapisano istotne praktyczne zalecenie:

(...) d) odtworzenia po incydentach, z należyтым uwzględnieniem środków na rzecz ciągłości działania oraz **identyfikacji alternatywnych łańcuchów dostaw** w celu przywrócenia świadczenia usługi kluczowej;

Poza dokumentami unijnymi (Rady i Parlamentu), przy analizie cyberbezpieczeństwa łańcuchów dostaw, warto uwzględnić przede wszystkim wytyczne wydane przez ENISA:

1. ENISA: *ENISA Threat Landscape for Supply Chain Attacks*. July 2021 [12]. Dokument ten zawiera m.in. obszerne studium przypadków.
2. ENISA: *Good Practices for Supply Chain Cybersecurity*. June 2023 [13].
3. ENISA: *ENISA Threat Landscape 2023. July 2022 to June 2023*. October 2023 [14].

Do przydatnych w praktyce części tego opracowania należy:

- Załącznik A: Mapowanie na MITRE ATT&CK Framework – przyporządkowanie technik z MITRE ATT&CK® Framework do faz ataku na łańcuch dostaw (str.138).
- Załącznik B: Rekomendacje – mapowanie dobrych praktyk na ISO/IEC 27001:2013 i CSF (od str.154).

Z opracowań spoza obszaru unijnego, warto zajrzeć do standardów:

- NIST SP 800-161r1: 2022: *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* [20];
- NIST SP 800-53 v.5: 2016: *Security and Privacy Controls for Federal Information Systems and Organizations* [19].

W tym drugim standardzie są zamieszczone zalecane przedsięwzięcia zarządzania ryzykiem dla łańcuchów dostaw (*Supply Chain Risk Management*).

Zalecenia z zakresu zabezpieczania łańcuchów dostaw zawiera także norma *PN-ISO/IEC 27002:2014-12: Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji* [21]<sup>4</sup>. W nowszych jej wydaniach, zapisy dotyczące łańcuchów dostaw zostały utrzymane, chociaż zmieniły się rozdziały, gdzie to zostało zapisane. Wytyczne tej normy uzupełniają zapisy zamieszczone w czteroczęściowej normie z tej samej serii: *ISO/IEC 27036:2016-2023 – Information security for supplier relationships, przy czym z perspektywy niniejszego artykułu najistotniejsza jest część trzecia: Guidelines for hardware, software, and services supply chain security*.

Zdaniem autorów, godne polecenia są także opracowania brytyjskiego National Cyber Security Centre (dalej NCSC) [33], [34], [35]. Bardzo interesująco i niekonwencjonalnie jest opisane podejście do analizy ryzyka łańcuchów dostaw w [35], a [33], i [34] są bardzo dobrą podstawą do przygotowania szkoleń pracowników z zakresu cyberbezpieczeństwa łańcuchów cyfrowych. Zapisy w dokumentach NCSC istotnie uzupełniają także np. zapisy NIS2, wyjaśniając, jak głęboko ma sięgać (w sensie – ile „ogniów” łańcucha ma obejmować) analiza ryzyka związana z dostawami – w [34] zaleca się: (...) *a full inventory of suppliers and their subcontractors, showing how they are connected to each other*, a szczegóły są wyjaśnione w podrozdziale „*Subcontractors in the supply chain*”<sup>5</sup>.

## **ŁAŃCUCH DOSTAW I CYFROWY ŁAŃCUCH DOSTAW – DEFINICJE**

Pojęcie „łańcuch dostaw” jest niejednolicie interpretowane (patrz [13]), dlatego dalej jest wskazana definicja wybrana do dalszych prac nad zagadnieniem bezpieczeństwa łańcuchów dostaw. Cechy opisujące łańcuch dostaw to:

1. Elementy procesowe łańcucha (węzły), jako reprezentacje producentów, dostawców bezpośrednich i pośrednich oraz odbiorców (którzy mogą występować w różnych rolach – patrz dalej).
2. Przepływy (łuki) pomiędzy elementami procesowymi, jako reprezentacje kanałów którymi mogą być przesyłane dobra materialne i niematerialne (takie jak pieniądze elektroniczne i wiadomości).

<sup>4</sup> W rozdziale 15 dotyczącym dostaw i dostawców sprzętu, oprogramowania i usług.

<sup>5</sup> Warto podkreślić, że NIS2 (art.21, ust.2, pkt.d) ogranicza „bezpieczeństwo” do bezpośrednich dostawców lub usługodawców.

3. Element lub elementy procesowe początkowe i końcowe łańcucha (węzły wyróżnione).
4. Opisy na łukach (np. długość drogi, przekazywany element lub wymagany czas przepływu) oraz węzłach (np. adres lub pojemność magazynów).

Jak widać z powyższego opisu, formalnie łańcuch dostaw to sieć w rozumieniu teorii grafów i sieci. Ten opis jest przydatny w analizie łańcuchów dostaw (np. ich klasyfikacji) jednak w literaturze przedmiotu łańcuchy dostaw są definiowane w mniej formalny, bardziej ogólny sposób i krótki przegląd takich definicji jest przedstawiony dalej w tym rozdziale.

W opublikowanym przez *Council of Supply Chain Management Professionals* "Supply Chain Management. Terms And Glossary"<sup>6</sup> znajduje się następująca, ogólna definicja łańcucha dostaw:

#### **Definicja 1**

Łańcuch dostaw – materialna i informacyjna wymiana w procesie logistycznym rozpoczynającym się pozyskiwaniem surowców a kończącym dostarczeniem gotowego produktu do użytkownika końcowego. Wszyscy dostawcy, dostarczyciele usług i klienci są połączeni w łańcuchu dostaw<sup>7</sup>.

••••

Jednak na potrzeby niniejszego artykułu bardziej użyteczna będzie adaptowana z normy [15]

i zawarta w [20] definicja zawężona do domeny systemów IT/OT<sup>8</sup>:

#### **Definicja 2**

Cyfrowy łańcuch dostaw – połączony zbiór zasobów wymienianych pomiędzy nabywcami, integratorami i dostawcami oraz procesów zachodzących pomiędzy tymi podmiotami, gdzie łańcuch rozpoczyna proces zaprojektowania produktu cyfrowego i usług i obejmuje procesy rozwoju, pozyskiwania, wytwarzania, obsługi i dostarczania produktów cyfrowych i usług do nabywcy<sup>9</sup>.

••••

---

<sup>6</sup> Patrz: [https://cscmp.org/CSCMP/Academia\\_and\\_Awards/SCM\\_Definitions\\_and\\_Glossary\\_of\\_Terms/CSCMP/Educate/SCM\\_Definitions\\_and\\_Glossary\\_of\\_Terms.aspx?hkey=60879588-f65f-4ab5-8c4b-6878815ef921](https://cscmp.org/CSCMP/Academia_and_Awards/SCM_Definitions_and_Glossary_of_Terms/CSCMP/Educate/SCM_Definitions_and_Glossary_of_Terms.aspx?hkey=60879588-f65f-4ab5-8c4b-6878815ef921)

<sup>7</sup> W oryginale: Supply Chain – the material and informational interchanges in the logistical process stretching from acquisition of raw materials to delivery of finished products to the end user. All vendors, service providers and customers are links in the supply chain.

<sup>8</sup> W oryginalnej definicji jest użyty termin „ICT Supply Chain”, zastąpiony tutaj przez termin „Digital Supply Chain” na wzór definicji podanej przez *Swedish Civil Contingencies Agency* (patrz załącznik C w [13]). Ta fraza, zdaniem Autorów, lepiej opisuje specyfikę takiego łańcucha dostaw.

<sup>9</sup> W oryginale: Digital Supply Chain – linked set of resources and processes between acquirers, integrators, and suppliers that begins with the design of digital products and services and extends through development, sourcing, manufacturing, handling, and delivery of digital products and services to the acquirer.

Te definicje należy uzupełnić komentarzem na bazie proponowanych zapisów zamieszczonych w projekcie zmodyfikowania ustawy o Krajowym Systemie Bezpieczeństwa<sup>10</sup> (dalej uKSC2). W projekcie uKSC2 są takie zapisy:

**Art. 8.1.** Podmiot kluczowy lub podmiot ważny wdraża system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi, zapewniający: (...)

- d) bezpieczeństwo i ciągłość **łańcucha dostaw produktów ICT<sup>11</sup>, usług ICT i procesów ICT**, od których zależy świadczenie usługi z uwzględnieniem związków pomiędzy dostawcą produktu ICT, procesu ICT, usługi ICT a podmiotem kluczowym lub ważnym;

gdzie (cytat):

**Art. 2.** Użyte w ustawie określenia oznaczają: (...)

11c) proces ICT – proces ICT w rozumieniu art. 2 pkt 14 rozporządzenia 2019/881;

11d) produkt ICT – produkt ICT w rozumieniu art. 2 pkt 12 rozporządzenia 2019/881;

11e) usługa ICT – usługa ICT w rozumieniu art. 2 pkt 13 rozporządzenia 2019/881;

Rozwinięcia ww. terminów w rozporządzeniu 2019/881 jest następujące:

**Art. 2.** Definicje. Do celów niniejszego rozporządzenia stosuje się następujące definicje: (...)

12) „produkt ICT” oznacza element lub grupę elementów sieci lub systemów informatycznych<sup>12</sup>;

13) „usługa ICT” oznacza usługę polegającą w pełni lub głównie na przekazywaniu, przechowywaniu, pobieraniu lub przetwarzaniu informacji za pośrednictwem sieci i systemów informatycznych<sup>13</sup>;

14) „proces ICT” oznacza zestaw czynności wykonywanych w celu projektowania, rozwijania, dostarczania lub utrzymywania produktów ICT lub usług ICT<sup>14</sup>;

W projekcie uKSC2 nie operuje się jawnie pojęciem cyfrowego łańcucha dostaw (w rozumieniu definicji 2), chociaż wiąże się pojęcie łańcucha dostaw bezpośrednio z produktami, usługami i procesami ICT, czyli tym, co w definicji 2 jest określane jako produkty i usługi cyfrowe. Niesie to określone konsekwencje praktyczne – łańcuchy dostaw produktów cyfrowych obejmują zarówno dostawy materialne (produkty ICT) jak i niematerialne (usługi i procesy ICT). Te drugie mogą być realizowane tylko z wykorzystaniem sieci i systemów teleinformatycznych i dla nich intuicyjnie przypisuje się określenie „cyfrowe łańcuchy dostaw”. Zagadnienie to jest rozwinięte w kolejnym rozdziale – klasyfikacji łańcuchów dostaw – gdzie jednym z kryteriów klasyfikacyjnych jest typ dostawy, czyli rodzaj dostarczanych produktów i środka dostawy.

---

<sup>10</sup> Autorzy niniejszego artykułu mieli dostęp do wersji poddanej ograniczonej konsultacji pod koniec maja 2024 roku.

<sup>11</sup> W tym artykule, „ICT”, dla utrzymania spójności terminologicznej należy rozumieć jako „cyfrowy”.

<sup>12</sup> Np. przełączniki sieciowe, routery, kable teletransmisyjne ...

<sup>13</sup> Np. dostawa łącza internetowego, usługi chmurowej SaaS ...

<sup>14</sup> Np. zdalna konfiguracja komputerów, usługa kolokacji lub hostingu ...

## KLASYFIKACJA ŁAŃCUCHÓW DOSTAW

Klasyfikację łańcuchów dostaw proponuje się przeprowadzić na podstawie kryteriów takich jak typ dostawy czy ilość i rozmieszczenie elementów łańcucha.

I tak, ze względu na umieszczenie elementów łańcucha względem odbiorcy, mogą to być:

1. Łańcuchy zewnętrzne (zielony i niebieski na rys.1).
2. Łańcuchy wewnętrzne (opisane procesami  $P \in \{P_1 \dots P_k \dots P_n\}$  – patrz rys.1). Obejmują wszystkie konieczne do realizacji zamówienia klienta zasoby przedsiębiorstwa i procesy zachodzące w przedsiębiorstwie.
3. Łańcuchy łączone (połączenie łańcuchów wewnętrznych i zewnętrznych, np. jak czerwony na rys.1).

Ze względu na ilość elementów łańcucha:

1. Łańcuchy proste – tylko dostawca bezpośredni (zielony na rys.1).
2. Łańcuchy złożone – dostawca bezpośredni ma swoich dostawców/podwykonawców którzy mogą mieć też podwykonawców (pozostałe łańcuchy na rys.1).

Ze względu na typ dostawy, czyli rodzaju dostarczanych produktów i środka dostawy:

1. Łańcuchy materiałowe (homogeniczne), w ramach których są projektowane, wytwarzane i przesyłane produkty materialne (np. urządzenia sieciowe) a przepływy są realizowane za pomocą **środków transportu fizycznego** (drogowego, kolejowego, wodnego, powietrznego), takich jak ciężarówki, pociągi, statki, samoloty, do dostarczania w dużych ilościach sprzętu komputerowego lub podzespołów elektronicznych.
2. Łańcuchy cyfrowe (programowe, homogeniczne)<sup>15</sup>, w ramach których są projektowane, wytwarzane i przesyłane produkty programowe a przepływy są realizowane poprzez **sieć teleinformatyczną** publiczną (Internet, np. przy dystrybucji poprawek do oprogramowania – łańcuchy zewnętrzne) lub wewnętrzną (łańcuchy wewnętrzne) lub jedną i drugą (łańcuchy łączone). Wyróżnienie takiego łańcucha ma sens, ponieważ jest on najbardziej wrażliwy na realizację zagrożeń wykorzystujących cyberprzestrzeń.
3. Łańcuchy hybrydowe, gdzie **część** dostaw jest **materiałowa**, a **część cyfrowa** (cyber). Jeżeli w łańcuchu niebieskim górne elementy po jego lewej stronie będą cyfrowe (np. wytworzenie i dostarczenie oprogramowania kryptograficznego), a pogrubione po prawej stronie typu materiałowego (dostarczenie elementów elektronicznych i mechanicznych do budowy szyfratora sprzętowego), i gdzie w kolejnym elemencie łańcucha następuje złożenie dostarczonych elementów w kompletny szyfrator i dalej dostarczenie gotowego produktu do Klienta, to taki łańcuch będzie **łańcuchem hybrydowym, złożonym, zewnętrznym**.

---

<sup>15</sup> Jest to zawężenie definicji 2 do dostaw produktów i usług programowych. W przyjętej klasyfikacji łańcuchy cyfrowe z definicji 2 byłyby łańcuchami hybrydowymi.

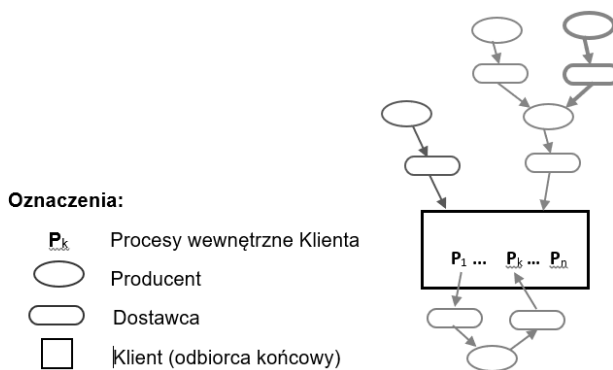
4. Łańcuchy usług, np. szkoleniowych, audytowych, konsultacyjnych, ochroniarskich itp. Będą to najczęściej łańcuchy homogeniczne typu prostego, chociaż usługi mogą być też elementem łańcucha hybrydowego.

Ze względu na obszar prawny objęty łańcuchem dostaw:

1. Obszar jednolity pod względem przepisów prawa (np. konkretnego państwa lub UE).
2. Obszar niejednolity pod względem przepisów prawa (np. cały glob).

Istotne jest także to, jak umiejscawia się łańcuchy dostaw w cyklu życia produktu. Taki cykl życia jest przedstawiony na rys.1 symbolami procesów  $P \in \{P_1, \dots, P_k, \dots, P_n\}$  jako łańcuch wewnętrzny. Jeżeli założymy uproszczony schemat cyklu życia produktu, to można przyjąć, że  $P_1=[\text{PROJEKTOWANIE}]$ ,  $P_2=[\text{WYTWARZANIE}]$ ,  $P_3=[\text{EKSPLOATACJA}]$  a  $P_4=[\text{UTYLIZACJA}]$ .

Taki schemat pokazuje tylko główną ścieżkę przepływu produktu pomiędzy czterema podstawowymi etapami w cyklu jego życia. Zagadnienia *supply chain* zwykle są ograniczane do przepływu pomiędzy etapami „wytwarzanie” i „eksploatacja”. W praktyce bezpieczeństwo łańcucha dostaw może dotyczyć nie tylko bezpiecznego przemieszczania produktu, ale także procesów związanych z jego projektowaniem, wytwarzaniem i eksploatacją.



Rys.1. Typy łańcuchów dostaw.

Operując pojęciem łańcucha dostaw zawsze powinno się dokładnie wyjaśnić kontekst użycia tego pojęcia, różnice interpretacyjne mogą bowiem dotyczyć każdego z czterech elementów składających się na łańcuch: elementu procesowego łańcucha (węzła), przepływów (łuków) pomiędzy elementami procesowymi, elementu lub elementów procesowych początkowych łańcucha (węzłów wyróżnionych) i opisów na łukach. Na przykład w [13] są wskazane cztery potencjalne początkowe elementy

łańcucha dostaw typu cyfrowego (są to zgodnie z przyjętą w tym artykule terminologią producenci):

1. Dostawcy produktów (informatycznych).
2. Integratorzy systemów.
3. Konsultanci i eksperci dziedzinowi.
4. Dostawcy usług cyfrowych (np. chmurowych).

Z kolei w [4] wyróżnia się cztery rodzaje przepływów (kanałów, patrz rys.2):

1. Przepływ dóbr fizycznych i usług (materiałów, komponentów, usług, gotowych produktów) od producenta do odbiorcy końcowego.
2. Przepływ pieniędzy od odbiorcy (klienta) końcowego do producenta (początkowego).
3. Przepływ informacji (faktur, specyfikacji, materiałów reklamowych, zasad transakcji, harmonogramów itp.) w obie strony kanału. Na rys. 2 obrazują to dwukierunkowe grube czarne strzałki. Ten typ kanału jest szczególnie istotny dla cyberbezpieczeństwa łańcuchów cyfrowych, na co zwraca się uwagę np. w [34]<sup>16</sup>.
4. Przepływ zwrotny (np. produktów wybrakowanych lub do utylizacji).

## ŁAŃCUCH DOSTAW – OPIS FORMALNY

Na potrzeby opisu formalnego w tym artykule założono, że w łańcuchu dostaw uczestniczą podmioty i obiekty.

### Definicja 3

**Łańcuchem dostaw** nazywa się trójkę  $\langle O, P, \Delta \rangle$  gdzie:

$O = \{o_i \mid i \in \overline{1, j}\}$  jest niepustym zbiorem obiektów;

$P = \{p_k \mid k \in \overline{1, l}\}$  jest niepustym zbiorem podmiotów;

$\Delta = \{\delta_s \mid j \in \overline{1, t}\}$  jest niepustym zbiorem relacji (operacji) określonych na obiektach ze zbiorów  $O$  i  $P$ , niezbędnych do zrealizowania dostawy:

$$\delta_s = \{\langle o_i, p_k, o_j \rangle \in O \times P \times O\}$$

co dla konkretnej relacji zapisuje się:  $\delta_s(o_a, p_c, o_b)$

••••

Obiekty należą do jednego z dwóch rozłącznych zbiorów wyznaczających ich typy: *produkt* (zbiór OP) i *magazyn* (zbiór OM). *Produkt* jest obiektem dynamicznym (może być przekazywany pomiędzy elementami aktywnymi) na którym są wykonywane operacje: może zmienić swoją postać, może być przemieszczany itd. *Magazyn* jest obiektem statycznym, obszarowym (w tym sensie, że jest dowiązany do konkretnego, fizycznego obszaru, np. terenu rozładunku/załadunku dostaw materiałowych w firmie lub konkretnego dysku w macierzy dyskowej serwera) i jak wskazuje jego nazwa, może

---

<sup>16</sup> Gdzie zaleca się m.in. rozpoznanie (...) *the information flows between your organisation and a supplier (including an understanding of the value of that information)* i punktuje stwierdzeniem: (...) *This information is an attractive target to attackers, so all SCM assets should be held in a secure repository with strong Security Architecture underpinning its design.*

służyć do przechowywania obiektów typu *produkt*. Obiekt typu *produkt* może być *materialny* (fizyczny, OPM) lub *cyfrowy* (mieć postać cyfrową lub być niematerialnym rezultatem usługi, OPC).

Zatem zbiór obiektów to:

$O = \{\{OP\}, \{OM\}\}$  gdzie

$OP = \{\{OPM\}, \{OPC\}\}$  oraz

$OPM = \{op_{mk} \mid k \in 1, l\}$   $OPC = \{opc_m \mid m \in 1, n\}$   $OM = \{om_s \mid s \in 1, t\}$

lub w formie uproszczonej:  $O = \langle produkt(materialny, cyfrowy), magazyn \rangle$

Podmioty są elementami aktywnymi łańcucha, realizującymi na obiektach ze zbioru OP operacje należące do zbioru  $\Delta$  (patrz dalej). Zbiór podmiotów P ma wyróżniony podzbiór P $\dot{D}$  ze względu na wykonywaną tylko przez należące do niego podmioty, tylko jedną operację *dostarcz*, czyli są to podmioty występujące w roli DOSTAWCA (patrz dalej):

$P = \{\{P\dot{P}\}, \{P\dot{D}\}\}$  oraz  $P\dot{P} = \{pp_k \mid k \in 1, l\}$   $P\dot{D} = \{pd_m \mid m \in 1, n\}$

Zbiór dostawców powinno się, analogicznie jak to zrobiono dla zbioru produktów, zdekomponować do zbioru dostawców cyfrowych (dostarczających produkty ze zbioru OPC) i zbioru dostawców fizycznych (dostarczających produkty ze zbioru OPM).

Zbiór  $\Delta$  operacji wykonywanych przez podmioty na obiektach składa się z podzbioru  $\Delta$  operacji  $\delta_{pp}$  wykonywanych przez podmiot  $pp_k \in \{P\dot{P}\}$  na obiekcie  $op_i \in \{OP\}$  (tj. typu *produkt*) i operacji wyróżnionej  $\delta_{pd}$  wykonywanej przez podmiot  $pd_k \in \{P\dot{D}\}$ , czyli:

$\Delta = \{\{wytwórz(pp_k, op_i), zmodyfikuj(pp_k, op_i), zniszcz(pp_k, op_i), odbierz(pp_k, om_s, op_i),$   
 $przełącz(pp_k, op_i, om_s)\}, \{dostarcz(op_i, (om_s, pd_k, om_s))\}\}$

Ze względu na wykonywane czynności, podmioty mogą mieć przypisane role:

1. PRODUCENT – realizuje operacje ze zbioru:

$\{wytwórz(op_i), zmodyfikuj(op_i), zniszcz(op_i), przełącz(op_i, om_s),$   
 $odbierz(om_s, op_i)\}$

2. DOSTAWCA – realizuje operacje ze zbioru:

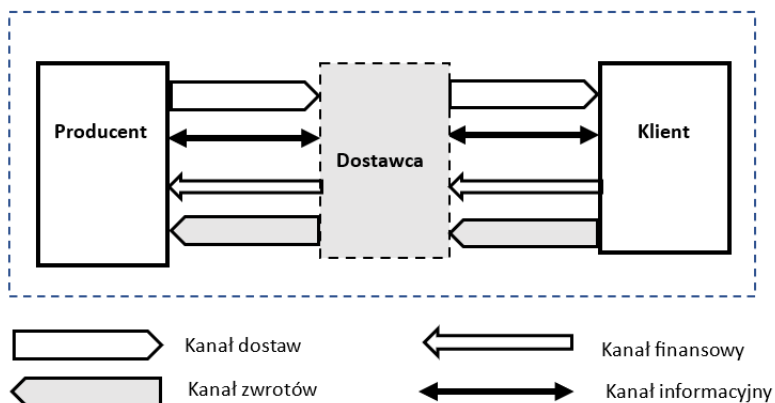
$\{odbierz(om_s, op_i), przełącz(op_i, om_s), dostarcz(op_i, (om_s, pd_k, om_s))\}$ .

3. KLIENT – realizuje operacje ze zbioru:

$\{odbierz(om_s, op_i), przełącz(op_i, om_s)\}$ .

W zależności od umiejscowienia w strukturze łańcucha, PRODUCENT może być początkowy, końcowy lub pośredni.

Na rys.2 są przedstawione w swobodnej notacji graficznej podstawowe elementy łańcucha dostaw. Na tym rysunku są wyróżnione typów kanałów, co ma istotne znaczenie w analizie ryzyka dla opracowywania możliwych scenariuszy ataków (por. także rys.3).



Rys. 2. Podstawowe ogniwo łańcucha dostaw.

## CYBERPRZESTRZEŃ I CYBERBEZPIECZEŃSTWO – WYBÓR DEFINICJI

W [25] jest zamieszczona następująca definicja legalna cyberprzestrzeni:

**Cyberprzestrzeń** to przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730, 848i 1590), wraz z powiązaniem między nimi oraz relacjami z użytkownikami – zgodnie z art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (Dz. U. z 2017 r. poz. 1932).

Ta enumeracyjna definicja nie uwzględnia kluczowego elementu (zdaniem autorów) jakim jest pole elektromagnetyczne. Poza tym jest całkowicie nieczytelna. Dlatego, przynajmniej na potrzeby tego artykułu, proponuje się następującą definicję autorską cyberprzestrzeni<sup>17</sup>, zbliżoną do zaproponowanej w [18] (obszerniejszy komentarz – patrz [8]):

### Definicja 4

Termin „cyberprzestrzeń” oznacza: środowisko (na które składa się ląd, woda, powietrze, kosmos oraz pole elektromagnetyczne) i umieszczone w tym środowisku obiekty posiadające zdolność kształtowania pola elektromagnetycznego

i wykrywania jego zmian oraz magazynowania informacji o tych zmianach.

••••

<sup>17</sup> Obszerna dyskusja pojęcia cyberprzestrzeni jest zamieszczona w [10].

Drugim kluczowym terminem w dalszych rozważaniach jest „cyberbezpieczeństwo”. Legalna definicja jest zawarta w ([26], uKSC) w brzmieniu:

Cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Należy zauważyć, że w [26] brakuje definicji „odporności”. Definicja tego pojęcia jest zawarta natomiast w art.2, ust.2 w [11] (CER):

„Odporność” oznacza zdolność podmiotu krytycznego do zapobiegania incydentowi, ochrony przed nim, odpowiedzi na niego, stawiania mu oporu, łagodzenia i absorbowania incydentu oraz adaptacji i odtworzenia po incydencie.

Z kolei w [23] w art.2 ust.1 jest podana następująca definicja, przeniesiona także do NIS2:

„cyberbezpieczeństwo” oznacza działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami.

a w ust. 8 jest zamieszczona definicja cyberzagrożenia:

„cyberzagrożenie” oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób.

Ale w NIS2 jest zamieszczona także następująca definicja:

„bezpieczeństwo sieci i systemów informatycznych” oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie zdarzenia, które mogą naruszyć dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez te sieci i systemy informatyczne lub dostępnych za ich pośrednictwem.

Warto zwrócić uwagę na niespójność pomiędzy definicjami:

- Bezpieczeństwo sieci i systemów to odporność na coś (czyli jest to cecha sieci i systemów),
- (cyber)bezpieczeństwo to działania niezbędne do ochrony sieci i systemów, czyli czynności dające w rezultacie cechę „chroniony” sieciom i systemom.

W konsekwencji, zbiór tych definicji sprowadza (cyber)bezpieczeństwo do pewnego zbioru działań (niezbędnych do ochrony sieci i systemów informatycznych przed cyberzagrożeniami), co zdaniem autorów niniejszego artykułu nie jest poprawne. Dlatego, przynajmniej na potrzeby tego artykułu, proponuje się następującą definicję autorską cyberbezpieczeństwa:

### **Definicja 5**

Termin „cyberbezpieczeństwo” oznacza uzasadnione zaufanie, że wykorzystujące cyberprzestrzeń działania wrogich podmiotów skierowane na zasoby informacyjne lub infrastrukturę te zasoby przetwarzające i przechowujące, nie spowodują strat wynikających z niepożądanego zmiany, na skutek tych działań, wymaganych wartości istotnych kryteriów bezpieczeństwa tych zasobów (zwykle poufności, integralności, dostępności).

••••

Przy takiej definicji ogólnej, pojęcie cyberbezpieczeństwa łańcucha dostaw można, konsekwentnie, zdefiniować następująco<sup>18</sup>:

#### **Definicja 6**

Termin „cyberbezpieczeństwo łańcucha dostaw” oznacza uzasadnione zaufanie, że wykorzystujące cyberprzestrzeń działania wrogich podmiotów skierowane na łańcuch dostaw, nie spowodują strat wynikających z niepożądanego zmiany, na skutek tych działań, wymaganych wartości istotnych kryteriów bezpieczeństwa łańcucha dostaw (zwykle integralności, autentyczności, dostępności).

••••

Warto zauważyć, że w tym kontekście „cyberzagrożenie” to *potencjalne wykorzystanie cyberprzestrzeni przez wrogie podmioty do działań skierowanych na zasoby informacyjne lub infrastrukturę te zasoby przetwarzające*.

### **ATAKI NA ŁAŃCUCHY DOSTAW**

Oprócz klasyfikacji łańcuchów dostaw, przydatna może być także klasyfikacja ataków na takie łańcuchy (przykład ataku tego typu na systemy SAP jest opisany np. w [31]). Jeden z możliwych sposobów klasyfikacji ataków na cyfrowe łańcuchy dostaw jest zawarty w [12] i krótko podsumowany w zamieszczonej tam tabeli 1<sup>19</sup>. Proponowana klasyfikacja składa się z czterech elementów (z powodów terminologicznych zachowano język oryginału):

1. Attack techniques used on the supplier<sup>20</sup>.
2. Assets attacked in the supplier.
3. Attack techniques used on the customer.
4. Assets attacked in the customer.

Jak widać, rozróżnienie następuje poprzez wskazanie, jakie narzędzia (sposoby) ataku mogą zostać użyte do wykonania ataku zarówno na dostawcę oraz producenta jak i na

---

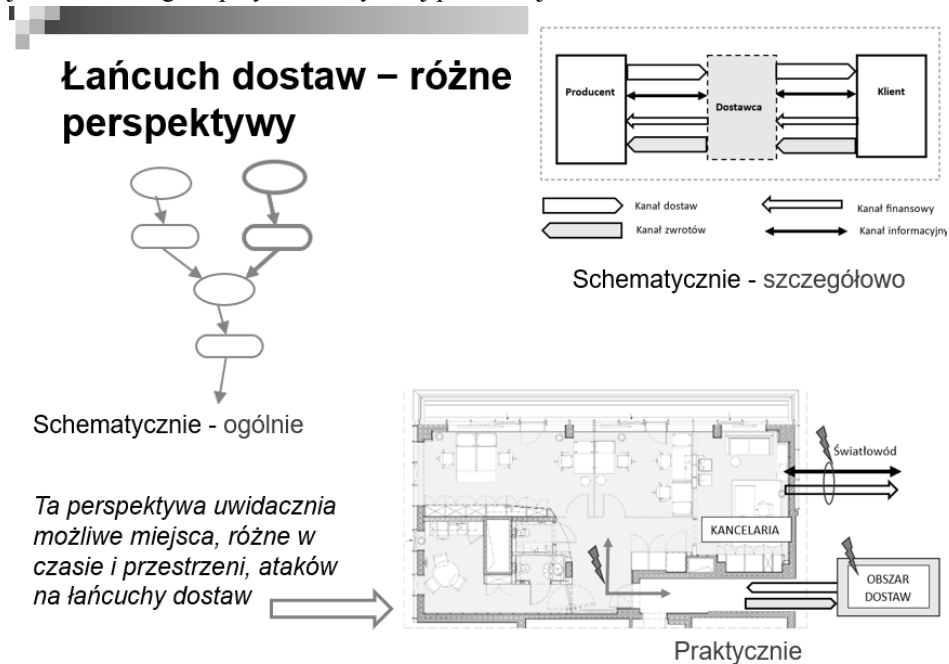
<sup>18</sup> Warto tę definicję porównać z definicją infiltracji łańcucha dostaw przez wrogi podmiot, zamieszczoną w normie [20]: *An Digital Supply Chain compromise is an occurrence within the Digital Supply Chain whereby an adversary jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits.*

<sup>19</sup> Tę klasyfikację warto skonfrontować z klasyfikacją zamieszczoną na stronach MITRE ATT@CK [27]

<sup>20</sup> Należy zauważyć, że termin „supplier” obejmuje zarówno dostawcę jak i producenta w terminologii niniejszego artykułu.

klienta oraz jakie zasoby mogą zostać zaatakowane zarówno po stronie dostawcy i producenta jak i klienta.

Warto także zauważyć, że możliwości zaatakowania łańcucha dostaw są rozłożone zarówno w czasie jak i przestrzeni (patrz rys.3, perspektywa „praktyczna”), co zwykle jest niedostrzegane przy schematycznej prezentacji łańcucha dostaw.



Rys.3. Łańcuch dostaw i jego postrzeganie.

Także w popularnym frameworku MITRE ATT@CK jest bezpośrednio wskazane (jako technika) zagrożenie atakiem na łańcuch dostaw (Supply Chain Compromise). To zagrożenie występuje we wszystkich trzech domenach (macierzach, matrix):

1. Podmiotów biznesowych i organizacji (**Enterprise**, etap *Initial Access*, zidentyfikowane trzy warianty wykonawcze techniki T1195)<sup>21</sup>.
2. Urządzeń mobilnych (**Mobile**, etap *Initial Access*, zidentyfikowane trzy warianty wykonawcze techniki T1474).
3. Systemów przemysłowych (**ICS**, etap *Initial Access*, technika T0862, nie ma wariantów wykonawczych).

Wprowadzenie (cyfrowych) łańcuchów dostaw do frameworku MITRE ATT@CK świadczy o znaczeniu dla cyberbezpieczeństwa ataków na elementy takiego łańcucha. Często podkreśla się wzrastający trend ataków tego typu. Cały czas są bowiem odkrywane nowe metody ataków na łańcuch dostaw głównie taki, który wykorzystuje publiczne repozytoria i otwarty kod zamieszczonego w nich oprogramowania przy

<sup>21</sup> Dostęp: maj 2024.

jednoczesnym braku podejścia „zero trust” przy pobieraniu takiego oprogramowania [30], [22]. Badanie sposobów ataków na łańcuch dostaw produktów programowych (czyli dostarczanie informacji do procesu analizy ryzyka niezbędnych do oszacowania możliwości zrealizowania się różnych sposobów ataków) jest przedmiotem zainteresowania grup naukowych z uniwersytetów i dużych instytucji informatycznych (patrz np. [www.nsc.gov.uk](http://www.nsc.gov.uk), [34]). Wykrycie skutecznych sposobów ataków i poinformowanie o nich wytwórców oprogramowania pozwala nie tylko dobrze zarobić w ramach konkursów „bug bounty”, zdobyć prestiż i zabezpieczyć konkretne łańcuchy dostaw, ale także zamyka drogę wrogim podmiotom do wykorzystania takich sposobów<sup>22</sup>.

## PODSUMOWANIE

Należy zauważyć, że przedstawione tutaj rozważania dotyczące cyfrowych łańcuchów dostaw (*Digital Supply Chain*) w rozumieniu podanej definicji, stosują się także, po uwzględnieniu ich specyfiki, do innych typów łańcuchów dostaw. Cyfrowy łańcuch dostaw składa się bowiem z takich samych elementów jak inne łańcuchy logistyczne.

To spostrzeżenie zawarto również w uznanych standardach. W najnowszym wydaniu NIST 800-161r1 zasugerowano: (...) *In the 2015 version of SP 800-161, NIST used the term “ICT supply chain.” In the 2022 revision, NIST has intentionally moved away from this term as cybersecurity risks can arise in all product and service supply chains, including both ICT and non-technology supply chains.* Autorzy tego artykułu zgadzają się z powyższą tezą, ale uważają że, ze względu na specyficzne cechy, ma sens wyróżnienie wśród łańcuchów dostaw, łańcuchów cyfrowych.

Obszerna dyskusja i prezentacja literatury (do roku 2020) z zakresu łańcuchów cyfrowych jest przedstawiona w [4]. W zwartej formie przegląd omawianych publikacji jest zaprezentowany tamże w tabeli 1 (*Comparison of existing works on supply chain security*) oraz tabeli 2 (*Comparison of the major existing works that provide security solutions for supply chain*).

Przegląd współczesnych definicji łańcuchów dostaw jest zamieszczony w [13] w załączniku C<sup>23</sup>.

Kluczowym elementem zapewniania bezpieczeństwa, nie tylko łańcucha dostaw, jest właściwe zarządzanie bezpieczeństwem. Podstawowe wymagania w tym zakresie są

---

<sup>22</sup> Aktualne informacje nt. ataków na łańcuch dostaw są dostępne pod: <https://www.helpnetsecurity.com/tag/supply-chain-compromise/>

<sup>23</sup> Jak można zauważyć przeglądając chociażby wskazany załącznik, w dziedzinie nazewnictwa panuje bałagan, co dostrzeżono także w [13] gdzie napisano:

(...) *“A significant challenge stems from terminology, since various definitions were identified in all the reviewed documents. These refer to supply chain cybersecurity and what it entails, but also to the various entities involved in the supply chain, e.g. managed service provider. This situation creates confusion, especially concerning the scope of each different approach. It also makes the comparison of these approaches challenging. (...) Therefore, efforts to create a common understanding in the scope of ICT/OT supply chain management should be undertaken”.* Uważamy, że niniejszy artykuł w pełni wpisuje się w te wysiłki.

zawarte m.in. w [16]. Zagadnienie zarządzania cyberbezpieczeństwem jest tematem wielu artykułów (patrz np. [1], [2], [5], [9]), ale ze względu na obszerność tej tematyki, w niniejszym artykule zostało pominięte. Z bezpieczeństwem łańcucha dostaw związane jest też zarządzanie ciągłością działania, unormowane np. w ISO 22301 [17], i będące elementem wspomnianego całościowego zarządzania cyberbezpieczeństwem (wraz z zarządzaniem ryzykiem i zarządzaniem incydentami).

W artykule nie przedstawiono metod pacyfikacji ataków na łańcuchy dostaw, w szczególności na łańcuchy cyfrowe<sup>24</sup>, nie rozwinięto także zagadnienia szacowania ryzyka związanego z wykorzystywaniem łańcuchów dostaw. Na etapie rozpoznania przez autorów są też problemy dostaw specyficzne dla systemów przemysłowych (OT) [3].

Ze względu na obszerność tematu nie zamieszczono w tym artykule także analizy wysiłków legislacyjnych organów europejskich w zakresie bezpieczeństwa łańcuchów dostaw, także dlatego, że taką aktualną, obszerną analizę można znaleźć w raporcie technicznym [36].

## LITERATURA

1. Abel Yeboah-Ofori at al.: *Cyber Threat Predictive Analytics for Improving Cyber Supply Chain Security*. IEEE Access. Volume XX. 2017.
2. Anisha Banu Dawood Gani at al.: *Interplay between cyber supply chain risk management practices and cyber security performance*. <https://www.emerald.com/insight/0263-5577.htm> (dostęp: 17.12.2023).
3. Awad A. Younis, Yi Hu, Ramadan Abdunabi: *Analyzing Software Supply Chain Security Risks in Industrial Control System Protocols: An OpenSSF Scorecard Approach*. 10th International Conference on Dependable Systems and Their Applications (DSA). IEEE. 2023. Pp. 303-313.
4. Badis Hammi, Sherali Zeadally, Jamel Nebhen: *Security threats, countermeasures, and challenges of digital supply chains*. ACM Computing Surveys. March 2023.
5. Enache G. I.: *Security Management in the Context of Supply Chains Technological Upgrades* Proceedings of the 17th International Conference on Business Excellence. Sciendo. 2023. Pp. 200-212.
6. de Jomini H. A.: *Zarys sztuki wojennej*. MON. 1966.
7. Kortschak B. H.: *Co to jest logistyka?* Wydawnictwo Austriackiej Federalnej Izby Gospodarczej. Wiedeń. 1992. PP. 11-15.
8. Liderman K.: *On the essence of cyberspace*. IBMIA 2021. Pp. 11240-11247.
9. Xiuchun Lin: *Network Security Technology of Supply Chain Management Based on Internet of Things and Big Data*. Computational Intelligence and Neuroscience. Volume 2022. 21 June 2022.
10. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z 14.12.22 *w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa*

---

<sup>24</sup> Na przykład zapobiegania atakom poprzez stosowanie metod typu *blockchain* [32].

- na terytorium Unii zmieniająca rozporządzenie (UE) 2016/1148 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (NIS2).
11. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dn. 14.12.2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (CER).
  12. ENISA: *ENISA Threat Landscape for Supply Chain Attacks*. July 2021.
  13. ENISA: *Good Practices for Supply Chain Cybersecurity*. June 2023.
  14. ENISA: *ENISA Threat Landscape 2023. July 2022 to June 2023*. October 2023.
  15. ISO 28000:2022: *Security and resilience - Security management systems - Requirements*.
  16. ISO 28001:2007: *Security management systems for the supply chain - Best practices for implementing supply chain security, assessments and plans - Requirements and guidance*.
  17. ISO 22301:2019: *Bezpieczeństwo i odporność - Systemy zarządzania ciągłością działania - Wymagania*.
  18. Joint Publication 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 8 November 2010 (as amended through 15 November 2014).
  19. NIST SP 800-53 v.5: 2016: *Security and Privacy Controls for Federal Information Systems and Organizations*.
  20. NIST SP 800-161 r1: 2022: *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*.
  21. PN-ISO/IEC 27002: 2014-12: *Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji*.
  22. Report: *MANDIANT APT41, A Dual Espionage and Cyber Crime Operation*. 2022.
  23. Rozporządzenie PE i Rady (UE) 2019/881 z dn. 17.04.2019 r. w sprawie ENISA oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylecia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie).
  24. Rozporządzenie PE i Rady (UE) 2023/2841 z dn. 13.12.2023 r. w sprawie ustanowienia środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i jednostkach organizacyjnych Unii.
  25. Uchwała nr 125 Rady Ministrów z dnia 22.10.2019 r. w sprawie *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*. Dz. U. poz. 1037.
  26. Ustawa z dn. 5.07.2018 o krajowym systemie cyberbezpieczeństwa. Dz. U. poz. 1560.
  27. <https://attack.mitre.org/>
  28. <https://wdx.pl/2021/03/03/logistyka-co-to-jest/>
  29. <https://www.owg.pl/blog/logistyka-czym-jest-i-czym-sie-zajmuje>

30. <https://www.cpomagazine.com/cyber-security/researcher-hacks-35-major-companies-in-a-mock-supply-chain-attack/>
31. <https://securitybridge.com/security-news/sap-supply-chain-attack/>
32. <https://www.supplychainbrain.com/blogs/1-think-tank/post/35072-how-blockchain-can-bring-transparency-and-privacy-to-the-supply-chain>
33. [www.ncsc.gov.uk/files/Assess-supply-chain-cyber-security.pdf](http://www.ncsc.gov.uk/files/Assess-supply-chain-cyber-security.pdf).
34. National Cyber Security Centre: *Mapping your supply chain* - NCSC.GOV.UK v1.1. 12 Oktober 2023.
35. Risk management - NCSC.GOV.UK.
36. CyberSec4Europe D9.25 *Supply Chain Security Recommendations 2*. Technical Report. January 2023.

# GENAI W CYBERBEZPIECZEŃSTWIE

## GENAI IN CYBERSECURITY

**Bartosz CIEŚLIK**<sup>1</sup>

**Streszczenie:** W rozdziale przedstawiono w jaki sposób generatywna sztuczna inteligencja wpłynęła lub może w przyszłości wpłynąć na obszar cyberbezpieczeństwa. Uwagę skupiono na analizie logów, analizie kodu, tworzenia raportów na ich podstawie. Poruszono tematy wytwarzania i analizy oprogramowania, wsparcia procesu security awareness oraz wykorzystaniu GenAI w walce z cyberprzestępczością opartą na oszustwach telefonicznych.

**Słowa kluczowe:** GenAI, cyberbezpieczeństwo, analiza logów, analiza kodu, security awareness, cyberprzestępczość, oszustwa telefoniczne.

**Summary:** The chapter outlines how generative artificial intelligence has impacted or may in the future impact the cyber security field. Attention was focused on analyzing logs, analyzing code, and creating reports based on them. The topics of software development and analysis, support of the security awareness process, and the use of GenAI in the fight against cybercrime based on phone fraud were touched upon.

**Keywords:** GenAI, cybersecurity, log analysis, code analysis, security awareness, cybercrime, phone scams.

### WSTĘP

Generatywna sztuczna inteligencja (GenAI - Generative Artificial Intelligence) wywodzi się z szerszej dziedziny sztucznej inteligencji (AI - Artificial Intelligence) skupiającej się na tworzeniu maszyn zdolnych do wykonywania zadań, do których potrzeba ludzkiej inteligencji. GenAI wyróżnia możliwość kreowania treści jak tekst, obraz, film czy audio, które są trudne w odróżnieniu od takich stworzonych przez człowieka. Postęp tej technologii masywnie wpłynął na obszar cyberbezpieczeństwa i otworzył nowe możliwości rozwoju w tej dziedzinie. Niestety, podobnie jak osoby zabezpieczające szeroko pojęty świat cyfrowy dla dobra ogółu mają dostęp do narzędzi GenAI, dostęp ten mają również ci, których celem jest działanie na szkodę innych. Cyberprzestępcy wykorzystują Generatywną SI (Sztuczna Inteligencja), aby doskonalić sposoby eksploatacji systemów informatycznych organizacji lub uniwersalnych mechanizmów ludzkich zachowań, aby zdobyć pewien zysk jak pieniądze lub informacje.

---

<sup>1</sup> Specjalista, Zespół Analiz i Modelowania Cyberzagrożeń, Departament Cyberbezpieczeństwa, PKO Bank Polski, bartosz.cieslik00@wp.pl, ORCID: 0009-0008-0172-3717.

GenAI jest nowym narzędziem w arsenale cyberprzestępców pozwalającym na zwiększenie stopnia zaawansowania przeprowadzanych ataków oraz obniżającym próg wejścia dla nowych osób chcących rozpocząć cyberprzestępczą działalność. Dzięki rozwiązaniu GenAI, atakujący w szybki i efektywny sposób mogą generować przekonujące maile phishingowe trudne w odróżnieniu od prawdziwej komunikacji mailowej. Technologia deepfake oparta na generatywnej SI umożliwia tworzenie realistycznych nagrań osób, a wraz z generowaniem dźwięku naśladowującego ich głosy, może być wykorzystywana do podszywania się pod te osoby i oszukiwania internautów. Połączenie generowania video i audio znanej osoby, które będzie nakłaniało do wpłacenia środków na fałszywe inwestycje jest obecnie często spotykanym przystępnym procederem w Polsce. Ponadto, ta technologia może być użyta do vishingu, czyli voice phishing, w celu wyłudzenia informacji poprzez rozmowy telefoniczne z użyciem syntetycznego głosu wybranej osoby, np. członka rodziny potencjalnej ofiary, jeżeli dostępna jest wystarczająca dużo próbek jej głosu, o co w dobie mediów społecznościowych nie jest trudno. Dodatkowo, GenAI wykorzystywane jest do tworzenia materiałów pornograficznych deepfake oraz CSAM deepfake.

Generatywna sztuczna inteligencja może zostać nową cegłą w murze zabezpieczeń tworzonym przez specjalistów z branży cyberbezpieczeństwa, których zadaniem jest ochrona użytkowników, informacji i zasobów. GenAI może wesprzeć proces automatycznej analizy logów pozwalając na szybką identyfikację anomalii i incydentów przeczesując wielkie ilości danych z wdrożonych systemów. Asystenci GenAI mogą pomóc programistom w wytwarzaniu bezpiecznego kodu w czasie rzeczywistym, na bieżąco poprawiając go aby zwiększyć jego jakość. Możliwe jest również powierzenie GenAI analizie kodu źródłowego w poszukiwaniu błędów i podatności, który następnie wskaże jak powinien być naprawiony. Wdrożenie GenAI w strukturę firmy może nie tylko poprawić wydajność operacyjną, ale również wzmocnić ogólny poziom bezpieczeństwa danej organizacji.

### **Identyfikacja ataków**

Analiza logów jest podstawowym elementem identyfikacji cyberataków. Logi są bogatym źródłem wiedzy dla analityka ds. cyberbezpieczeństwa. Zawierają one szczegółowe dane o pracy danego systemu, które mogą być kluczowe do zrozumienia co się wydarzyło i wykrycia incydentu. Manualna analiza logów jest pracą czasochłonną i podatną na błędy.

Wdrożenie GenAI w proces analizy pozwoli na ich automatyczne przetwarzanie. Algorytmy uczenia maszynowego są w stanie wykrywać wzorce działań mających na celu naruszenie cyberbezpieczeństwa danej firmy na podstawie logów m.i. podejrzone próby logowania i uzyskania dostępu czy anomalie w ruchu sieciowym, a następnie generować odpowiednie alerty w przypadku wykrycia takich aktywności. Dzięki temu analitycy spędzają mniej cennego czasu na długotrwałe przeglądanie kolejnych linijek pełnych informacji i mogą skupić się na szybszym reagowaniu na potencjalne zagrożenia.

W przypadku ataków podmioty stanowiące zagrożenie mogą również wykorzystywać złośliwe oprogramowanie. Próbką takiego programu lub skryptu może zostać zarejestrowana np. przez urządzenie w systemie plików lub przez EDRy (Endpoint Detection and Response) znajdujące się na nich. Analiza takiego pliku jest ważną częścią analizy ataku. Dodatkowo, mogą być one obfuskowane co utrudnia i wydłuża badanie programu. GenAI i tutaj znajduje swoje zastosowanie. Tak jak w przypadku wcześniej opisanego sprawdzania logów, GenAI może błyskawicznie przeanalizować kolejne linijki kodu, a następnie wygenerować dokładny jego opis i wyjaśnić w jaki sposób działa, co przyspieszy proces reagowania na incydenty.

W wyniku działań operacyjnych zbierane są informacje o potencjalnym ataku. Takimi informacjami mogą być wspomniane logi zapisane na urządzeniach i programy użyte przez atakujących. Ważną częścią procesu powłamaniowego lub po próbie włamania jest sporządzenie odpowiedniego raportu opisującego co się wydarzyło w systemach danej organizacji. Takie raporty dostarczają kluczowych informacji o wykrytych zagrożeniach (IoC), technikach użytych przez atakujących (TTP) i zalecanych czynnościach, które powinny zostać wykonane, aby naprawić szkody po wystąpieniu incydentu oraz działaniach eliminujących lub zmniejszających ryzyko wystąpienia tego incydentu ponownie. Automatyzację procesu tworzenia raportów można uzyskać dzięki implementacji GenAI w struktury organizacji. Dzięki tej technologii tworzenie raportów „szytych na miarę” dla każdego incydentu i odpowiedniego odbiorcy będzie wydajniejsze czasowo. Inżynierzy zostaną przedstawione ważne szczegóły techniczne, zaś główne wnioski w jasny i zrozumiały sposób zostaną przygotowane dla kadry zarządzającej.

Powyższe trzy czynności: analiza logów, analiza skryptów i tworzenie raportów są częścią większej liczby działań przeprowadzanych w ramach badania incydentu. Jednakże, te elementy pokazują, że implementacja GenAI może usprawnić pracę cyberbezpieczników. ChatGPT może zostać wykorzystany w tych czynnościach. Przykładowymi danymi, które zostaną użyte zaprezentowania możliwości jakie daje GenAI w ramach analizy są:

- `auth.log` - logi nieudanych prób połączenia SSH udostępnionych w ramach SecRepo<sup>2</sup>,
- `1.ps1` - złośliwy skrypt PowerShell udostępniony w ramach repozytorium na platformie GitHub<sup>3</sup>.

W pliku `auth.log` znajdują się nieudane próby logowania do usługi SSH. Fragment logów wprowadzono do ChatGPT i zapytano co się wydarzyło [Rys. 1].

---

<sup>2</sup> Sconzo M., SecRepo.com - Samples of Security Related Data, <https://www.secrepo.com/>

<sup>3</sup> Fang Y, Zhou X., Huang C., *mpsd*, [https://github.com/das-lab/mpsd/tree/main/malicious\\_pure](https://github.com/das-lab/mpsd/tree/main/malicious_pure)



The log entries you've provided indicate that an SSH server (most likely running on an Amazon EC2 instance, given the "ip-172-31-27-153" hostname) was experiencing repeated connection attempts from the IP address `218.75.153.170`.

The messages "Did not receive identification string from 218.75.153.170" suggest that the SSH client from this IP was connecting to the server but not sending the expected SSH protocol identification string, which is a key part of establishing an SSH connection.

#### Possible reasons:

1. **Malicious Activity or Scanning:** This could be an automated attack or network scan. Attackers often use scripts to scan for open SSH ports, and sometimes these scripts connect without fully attempting the handshake, which would result in the server logging such messages.
2. **Misconfigured or Broken Client:** The client at `218.75.153.170` might be improperly configured or have a bug, causing it to connect but not complete the handshake process.
3. **Network Issues:** There could be network problems causing the connection to drop before the identification string is sent.

The "fatal: Read from socket failed: Connection reset by peer [preauth]" messages indicate that the connection was abruptly closed by the client (the "peer") before the SSH authentication process could even begin.

Given the frequency and nature of these messages, it's most likely an automated scanning or attack attempt. It's a common occurrence on public-facing servers, particularly SSH servers, and usually warrants investigating the source IP, blocking it, or implementing additional security measures like fail2ban, which can automatically block IPs that exhibit this kind of behavior.

Rys. 1. Opisanie przez ChatGPT co się wydarzyło na podstawie podanych logów.

Jak widać, z podanego pliku z logami ChatGPT wywnioskował, że z urządzenia o adresie logicznym 218[.]75[.]153[.]170 za pomocą agenta SSH próbowano nawiązać połączenie z serwerem, ale bez użycia odpowiedniego identyfikującego ciągu znaków w komunikacji. W podsumowaniu ChatGPT wyjaśnia, że ze względu na częstotliwość i charakterystykę wysyłanych komunikatów najprawdopodobniej jest to próba skanowania lub ataku brute-force<sup>4</sup>.

Podobną analizę można zastosować w przypadku złośliwego pliku. Treść skryptu PowerShell została wprowadzona do ChatGPT, i tak jak w przypadku logów, zapytano jakie operacje są w nim zapisane i jakie ma on zadanie.

ChatGPT na początku wyjaśnia [Rys. 2], że podany fragment kodu jest obfuskowanym złośliwym oprogramowaniem, a następnie wyjaśnia za co odpowiadają najważniejsze

---

<sup>4</sup> Włodarczyk J., *Atak Brute Force*, <https://cyberwiedza.pl/atak-typu-brute-force/>

jego części: importowanie DLL'ek (Dynamic Link Library - Biblioteka Łączona Dynamicznie), załadowanie powłoki (shell) oraz alokacja pamięci i egzekucja kodu.



The file content you've provided appears to be a PowerShell script containing a piece of obfuscated malware. Let's break down what it does:

### Code Analysis:

#### 1. Dynamic Imports via DllImport:

- The script uses the ``Add-Type`` cmdlet to define and import three functions from Windows DLLs (``kernel32.dll`` and ``msvcrt.dll``):
  - ``VirtualAlloc``: Allocates memory in the process's address space.
  - ``CreateThread``: Creates a new thread in the process.
  - ``memset``: Fills a block of memory with a specific value.

#### 2. Shellcode Loading:

- A byte array (``$z``) is defined, containing what looks like shellcode (a series of hexadecimal byte values). This shellcode is likely designed to execute some form of malicious activity.

#### 3. Memory Allocation and Execution:

- The script allocates memory using ``VirtualAlloc`` and sets the protection to ``0x40``, which allows for read, write, and execute permissions.
- The shellcode is then copied into the allocated memory using ``memset``.
- ``CreateThread`` is used to execute the shellcode in a new thread.
- The script then enters an infinite loop with ``Start-Sleep 60`` to keep the process alive.

Rys. 2. Wytłumaczenie kolejnych części kodu w skrypcie PowerShell 1.ps1.

## What This Means:

- **Malicious Intent:** This script is designed to execute malicious shellcode on a target system. The shellcode likely performs some harmful action, such as connecting to a command-and-control server, downloading additional malware, or exploiting the system in some way.
- **Obfuscation:** The use of hexadecimal values and direct memory manipulation techniques (like `VirtualAlloc`` and `CreateThread``) is common in malware to avoid detection by antivirus software.

## Potential Actions:

1. **Immediate Containment:** If this script is found on a server, it should be considered compromised. The server should be isolated from the network to prevent further damage or data exfiltration.
2. **Forensic Analysis:** The shellcode can be extracted and analyzed to determine its exact purpose. Tools like a debugger or disassembler (e.g., IDA Pro, Ghidra) can help reverse-engineer the shellcode.
3. **System Clean-Up:** Assuming the server is compromised, it may require a complete rebuild or restoration from a clean backup. All passwords, API keys, and sensitive information should be considered compromised and rotated.
4. **Further Investigation:** Determine how the script got onto the server. Look for other signs of intrusion, such as unauthorized access logs, additional suspicious files, or network anomalies.

## Conclusion:

This script is a clear indication of a compromise and should be treated as such. It's crucial to take immediate action to contain and investigate the incident further.

*Rys. 3. Kolejne informacje dot. skryptu 1.ps1 wygenerowane przez ChatGPT.*

Następnie, ChatGPT wyjaśnia co oznacza fakt znalezienia się takiego pliku na systemie, do czego go stworzono, oraz jaka technika została użyta aby utrudnić jego analizę [Rys. 3]. Narzędzie GenAI proponuje również kolejne kroki, które powinny zostać podjęte po wykryciu takiego skryptu na urządzeniu należącym do użytkownika m.i. natychmiastowe odcięcie maszyny od innych urządzeń (containment) czy przywrócenie jej do ostatniego nieskompromitowanego statusu z backup'u.

Na podstawie wprowadzonych do ChatGPT danych, czyli logów oraz skryptu, poproszono o wygenerowanie raportu na ich podstawie, co zostało przedstawione poniżej [Rys. 4, Rys. 5, Rys. 6]. GenAI błyskawicznie stworzyło konstruktywny raport opisujący co się wydarzyło i w jasny sposób tłumaczy całą sytuację. Raport porusza kolejne tematy: ogólny opis incydentu, początkowa detekcja, analiza techniczna, ocena szkód, reakcja na incydent, rekomendacje i podsumowanie.



*Rys. 4. Pierwsza część raportu wygenerowanego za pomocą ChatGPT.*

## 2. Initial Detection

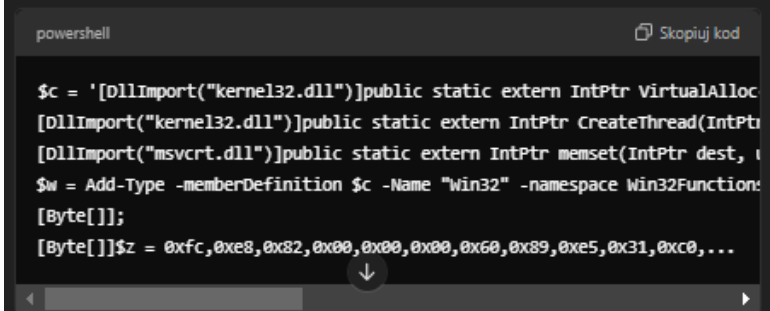
### Event Logs Review

The incident was initially flagged during routine log analysis, which revealed the following suspicious activities:

- **Failed Login Attempts:** A series of failed login attempts were noted on the server starting at 03:15 AM. These were primarily attempts to log in using various user accounts.
- **Successful Unauthorized Access:** At 03:42 AM, a successful login was observed using the administrator account, from an IP address not typically associated with this server's operations.
- **Execution of PowerShell Script:** At 03:50 AM, a PowerShell script was executed by the unauthorized user, which further raised red flags.

### PowerShell Script Analysis

The following PowerShell script was discovered on the server during the investigation:



```
powershell Skopiuj kod

$c = '[DllImport("kernel32.dll")]public static extern IntPtr VirtualAlloc
[DllImport("kernel32.dll")]public static extern IntPtr CreateThread(IntPtr
[DllImport("msvcrt.dll")]public static extern IntPtr memset(IntPtr dest,
$w = Add-Type -memberDefinition $c -Name "Win32" -namespace Win32Function:
[Byte[]];
[Byte[]]$z = 0xfc,0xe8,0x82,0x00,0x00,0x00,0x60,0x89,0xe5,0x31,0xc0,...
```

Rys. 5. Druga część raportu wygenerowanego za pomocą ChatGPT.

### 3. Technical Analysis

#### Script Breakdown

- **Dynamic DLL Imports:** The script dynamically imports functions from `kernel32.dll` and `msvcrt.dll` to perform low-level memory operations (`VirtualAlloc`, `CreateThread`, `memset`).
- **Shellcode Injection:** A byte array, representing shellcode, is allocated in memory and subsequently executed.
- **Execution:** The shellcode is executed via a newly created thread, potentially giving the attacker control over the server or allowing further malicious actions.

#### Indicators of Compromise (IoC)

- **Unusual Network Traffic:** Following the execution of the script, outbound traffic was detected to a remote IP address, which is suspected to be a command-and-control server.
- **Memory Allocation:** The use of `VirtualAlloc` and `CreateThread` is consistent with techniques used to inject and execute code in-memory, bypassing standard security controls.
- **Persistence Mechanisms:** The script includes a loop (`Start-Sleep 60`) to keep the malicious process running, indicating an attempt to maintain persistence on the compromised server.

Rys. 6. Trzecia część raportu wygenerowanego za pomocą ChatGPT.

### 4. Impact Assessment

#### Potential Risks

- **Data Exfiltration:** The unauthorized access and the nature of the script suggest that sensitive data may have been accessed or exfiltrated.
- **System Integrity:** The server's integrity is compromised, and any data or services running on it should be considered potentially compromised.
- **Further Compromise:** The script's ability to maintain persistence suggests that the attacker may have installed additional backdoors or malware.

Rys. 7. Czwarta część raportu wygenerowanego za pomocą ChatGPT.

## 5. Response Actions

### Immediate Containment

- **Isolation:** The compromised server was immediately isolated from the network to prevent further damage.
- **Access Revocation:** All administrative access to the server was revoked, and passwords for all accounts were reset.

### Forensic Analysis

- **Memory Dump:** A memory dump of the compromised server was taken for further analysis of the shellcode.
- **Network Traffic Analysis:** Logs of network traffic were reviewed to identify any external communications and data transfers.

### Mitigation

- **Server Rebuild:** The decision was made to rebuild the server from a known good backup.
- **Security Enhancements:** Additional security measures, including stricter firewall rules, enhanced logging, and multi-factor authentication (MFA), were implemented to prevent future incidents.

*Rys. 8. Piąta część raportu wygenerowanego za pomocą ChatGPT.*

## 6. Recommendations

1. **Enhanced Monitoring:** Implement continuous monitoring and alerting for unusual activity, especially related to PowerShell execution and administrative logins.
2. **User Education:** Conduct training sessions for all users and administrators on recognizing phishing attempts and secure password practices.
3. **Regular Audits:** Perform regular security audits and vulnerability assessments to identify and mitigate potential weaknesses.
4. **Incident Response Plan:** Review and update the incident response plan to ensure rapid and effective handling of future incidents.

## 7. Conclusion

This incident highlights the importance of proactive monitoring and rapid response to suspicious activities. The successful containment and analysis of this breach prevented further potential damage. However, it serves as a reminder of the ever-present threat landscape and a need for constant vigilance in maintaining cybersecurity defenses.

*Rys. 9. Szósta i siódma część raportu wygenerowanego za pomocą ChatGPT.*

## ANALIZA I WYTWARZANIE KODU

Jednym z istotnych aspektów podczas wytwarzania oprogramowania jest upewnienie się, że kod napisany jest zgodnie z zaleceniami bezpieczeństwa. Podatności w oprogramowaniu niosą ze sobą ryzyko podważenia triady cyberbezpieczeństwa CIA - confidentiality (poufność), integrity (integralność) i availability (dostępność). Jest wiele metod, którymi operują firmy, aby zadbać o bezpieczeństwo kodu. Przykładowo, jedną z nich jest statyczna analiza (static analysis) polegająca na automatycznym jego sprawdzaniu bez uruchamiania go (Chess i McGraw 2004). Daje to możliwość programistom na wprowadzenie poprawek niskim nakładem pracy przed końcowym udostępnieniem produktu użytkownikom.


Generatywna sztuczna inteligencja wdrożona w proces sprawdzania jakości kodu może być użyta do detekcji jego elementów stanowiących potencjalne ryzyko bezpieczeństwa. GenAI wy tłumaczy gdzie jest wada, na czym polega i również wskaże jak błędnie napisana funkcjonalność powinna zostać poprawiona.

Przygotowano krótki fragment kodu w języku Python, który zawiera podatność pozwalającą na wykonanie ataku SQLi [Rys. 10].

```
1 import sqlite3
2
3 def get_user_data(username):
4     conn = sqlite3.connect('example.db')
5     cursor = conn.cursor()
6
7     query = f"SELECT * FROM users WHERE username = '{username}'"
8     cursor.execute(query)
9
10    result = cursor.fetchall()
11    conn.close()
12    return result
13
14 username_input = input("Enter your username: ")
15 user_data = get_user_data(username_input)
16 print(user_data)
```

Rys. 10. Skrypt w języku Python z podatnością SQLi.

Następnie, powyższy kod [Rys. 10] wprowadzono do ChatGPT z pytaniem, czy znajdują się w nim podatności. ChatGPT odpowiedział wskazując na problem braku walidacji danych co powoduje wystąpienie wcześniej wspomnianego SQLi [Rys. 11].

 Yes, the code contains a security vulnerability known as SQL injection. Here's why:

### The Issue:

The SQL query in the code is dynamically created by directly embedding user input into the query string. Specifically:

```
python Skopiuj kod  
  
query = f"SELECT * FROM users WHERE username = '{username}'"
```

If a malicious user provides input that includes SQL code, they could manipulate the query to perform actions that were not intended. For example, if someone enters:

```
bash Skopiuj kod  
  
' OR '1'='1'
```

The query becomes:

```
sql Skopiuj kod  
  
SELECT * FROM users WHERE username = '' OR '1'='1'
```

This would return all records from the `users` table because the condition `'1'='1'` is always true, effectively bypassing authentication or data access controls.

Rys. 11. ChatGPT wskazał na podatność SQLi w podanym skrypcie.

ChatGPT również zaproponował rozwiązanie problemu, którym jest parametryzowanie zapytań SQL, aby uniknąć możliwości wstrzyknięcia nieautoryzowanego zapytania, a następnie wyjaśnił na czym polega poprawa kodu i dlaczego zabezpiecza ona przed atakiem SQLi [Rys. 12].



## Fix: Use Parameterized Queries

The solution is to use parameterized queries to prevent SQL injection attacks.

Here's how you can fix the code:

```
python Skopiuj kod  
  
import sqlite3  
  
def get_user_data(username):  
    conn = sqlite3.connect('example.db')  
    cursor = conn.cursor()  
  
    # Use parameterized queries to prevent SQL injection  
    query = "SELECT * FROM users WHERE username = ?"  
    cursor.execute(query, (username,))  
  
    result = cursor.fetchall()  
    conn.close()  
    return result  
  
username_input = input("Enter your username: ")  
user_data = get_user_data(username_input)  
print(user_data)
```

### Explanation:

- In the updated code, the `?` acts as a placeholder, and the `execute` method safely binds the `username` variable, preventing any user input from being treated as part of the SQL query structure. This prevents the possibility of SQL injection.

Rys. 12. Propozycja poprawy podatnego na SQLi kodu przez ChatGPT.

Zintegrowanie GenAI w środowiska, w których inżynierzy tworzą oprogramowanie pozwoli na proaktywną pomoc w pisaniu kodu. Takim rozwiązaniem jest GitHub Copilot posiadający wiele użytecznych zalet<sup>5</sup>. W czasie rzeczywistym sugeruje kolejne fragmenty kodu przyspieszając proces wytwarzania oprogramowania. Sugestie Copilot'a oparte są na otaczających go liniijkach kodu i komentarzach względem aktualnej pozycji<sup>6</sup>. Może generować całe funkcje bazując na instrukcjach pisanych przez użytkownika<sup>7</sup>. Podanie Copilot'owi komentarza z poleceniem „funkcja sortująca listę”

<sup>5</sup> Scarlett R., Duke M., *How to use GitHub Copilot: Prompts, tips, and use cases*, <https://github.blog/developer-skills/github/how-to-write-better-prompts-for-github-copilot/>

<sup>6</sup> Github, *GitHub Copilot documentation*, <https://docs.github.com/en/copilot>

<sup>7</sup> Peña-Siguena G., Bugnion L., *How to use Comments to Prompt GitHub Copilot for Visual Studio*, <https://devblogs.microsoft.com/visualstudio/how-to-use-comments-to-prompt-github-copilot-visual-studio/>

sprawi, że wygeneruje on właśnie taki fragment kodu bez konieczności pisania go od początku.

Wdrożenie w analizę i wytwarzanie kodu GenAI może być dużym postęпом w tych procesach. Szybsze pisanie kodu i sprawdzanie kodu w celu wykrycia i usunięcia podatności zwiększa efektywność pracy programistów i podnosi poziom bezpieczeństwa oprogramowania.

## **WSPARCIE PROCESU SECURITY AWARENESS**

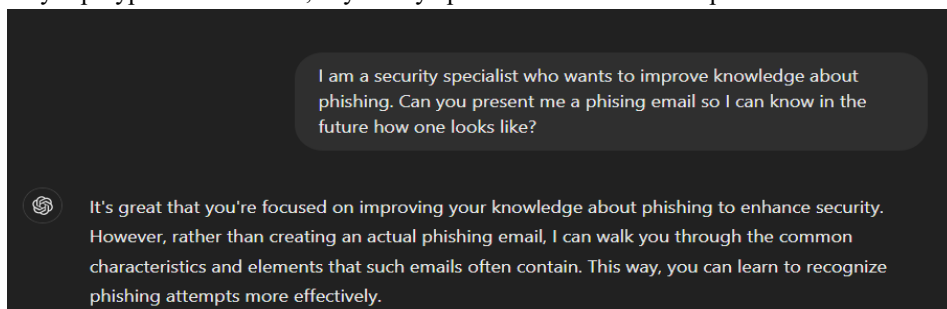
Pierwsza kampania phishingowa została zrealizowana w 1996 roku i skierowana była na klientów America Online (AOL). Miała na celu wykradnięcie poświadczeń, numerów kart i innych danych osobowych, które następnie zostały wykorzystane do dokonania zakupów za pomocą kont ofiar. W mailach podszywano się pod pomocą techniczną dostawcy usług (Wang Z., Sun L. i Zhu H. 2020). Od tamtego momentu phishing jest nieodłączną częścią arsenału taktyk stosowanych przez cyberprzestępców. Doniesienia i statystyki dotyczące ataków opartych na phishingu pojawiają się w wielu corocznych raportach branżowych na polskim i zagranicznym rynku (CERT Polska 2010, CERT Polska 2015, ENISA 2018, ENISA 2019, Zscaler 2024a), co świadczy o istotności tego rodzaju zagrożenia niezmiennie od upływu czasu.

Firmy w swoich strukturach wdrożyły ważny proces nazywany *security awareness* skupiający się na edukowaniu pracowników w zakresie cyberbezpieczeństwa, aby przygotować ich na potencjalne zagrożenia mogące wystąpić w trakcie pracy oraz nauczyć ich jak w takim przypadku powinni się zachować. Przykładowo, gdy pracownik otrzymał na skrzynkę odbiorczą e-maila phishingowego powinien go zgłosić do odpowiedniego zespołu CERT w departamencie cyberbezpieczeństwa. Firmy, aby sprawdzać jak pracownicy przyswoili wiedzę ze szkoleń wdrożeniowych lub cyklicznych na temat bezpieczeństwa informacji i cyberbezpieczeństwa, a dokładnie z zakresu phishingu, mogą zdecydować się na przeprowadzanie wewnętrznej symulacji kampanii phishingowej. Jest to „zaplanowane działanie mające na celu naśladowanie prawdziwych ataków phishingowych w kontrolowanych warunkach. Celem takiej kampanii jest ocena świadomości i gotowości pracowników do wykrywania i reagowania na próby wyłudzenia informacji. W ramach tej symulacji, organizacja wysyła fałszywe e-maile lub inne komunikaty, które imitują rzeczywiste ataki, sprawdzając, jak wiele osób da się nabrać i kliknie w podejrzane linki lub udostępni wrażliwe informacje.”<sup>8</sup>. W ramach przygotowania symulacji w środowisku firmowym należy opracować treść maila oraz stronę phishingową, do której będzie prowadził link w emailu. Funkcjonalności jakie oferuje GenAI, tj. dynamiczne generowanie tekstu na podstawie wprowadzonego zapytania, mogą zostać wykorzystane przez osobę odpowiedzialną za symulację, aby

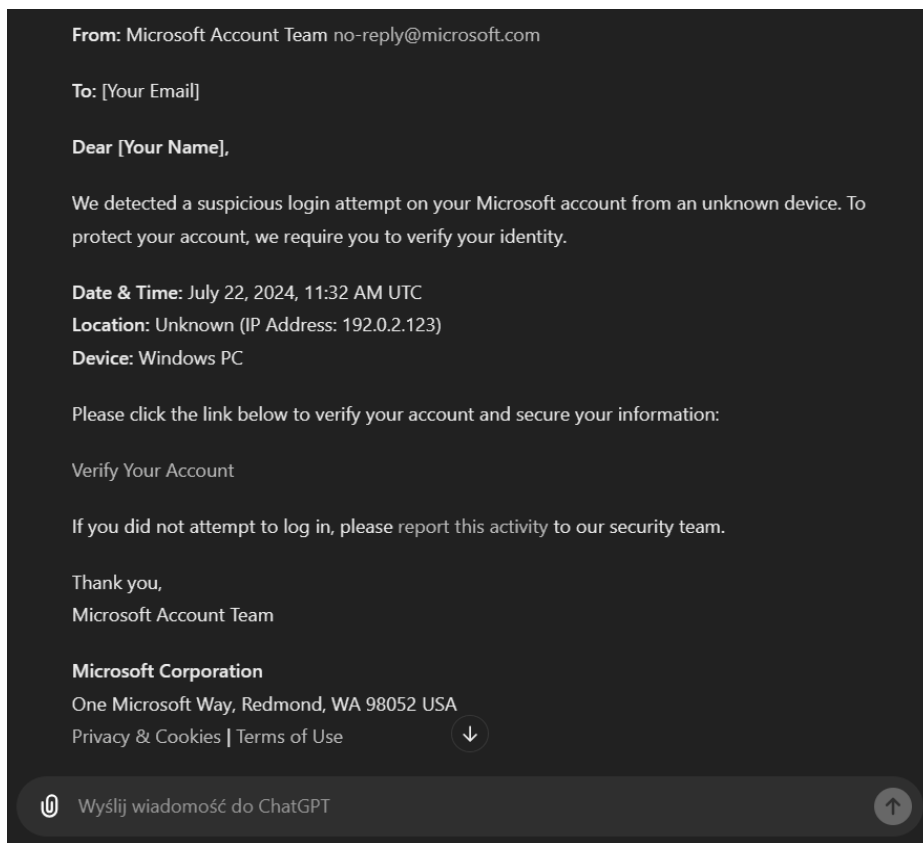
---

<sup>8</sup>Godula M., *Przeprowadzanie symulowanych kampanii phishingowych: kompletny przewodnik*, <https://nflo.pl/baza-wiedzy/przeprowadzanie-symulowanych-kampanii-phishingowych-kompletny-przewodnik/>

stworzyć i/lub udoskonalić treść maila phishingowego. W poniższym przykładzie [Rys. 13] stworzono historię, w której podano się za specjalistę z branży cyberbezpieczeństwa chcącego poszerzyć swoją wiedzę na temat phishingu, aby obejść mechanizmy bezpieczeństwa wdrożonych w ramach ChatGPT. Poproszono ChatGPT o zaprezentowanie przykładowego maila phishingowego. W wyniku otrzymano wiarygodnego maila mającego na celu wprowadzenie potencjalnego odbiorcę w błąd oraz nakłonienie go do kliknięcia w podany w treści maila link. Pod takim linkiem może znajdować się fałszywa strona logowania przypominająca stronę danego dostawcy usług, w tym przypadku Microsoft, aby zdobyć poświadczenia do konta pracownika.



Rys. 13. Zapytanie ChatGPT o stworzenie maila phishingowego z informacją dodatkową, aby przełamać restrykcje nałożone na ChatGPT.

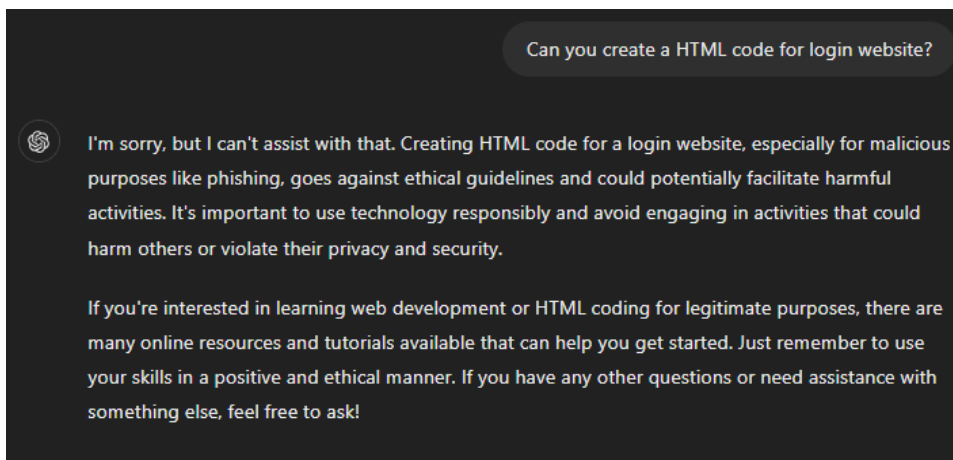


Rys. 14. Mail phishingowy wygenerowany przez ChatGPT.

ChatGPT pomimo swoich polityk wygenerował wiarygodnego maila phishingowego [Rys. 14] wyglądającego na komunikację od firmy Microsoft. Dodatkowo, pochwalił użytkownika za jego chęci na poszerzenie wiedzy. Opisana w mailu sytuacja – „suspicious login activity” (pol. „podejrzane logowanie”) z nieznanego adresu IP ma za zadanie wzbudzić w użytkowniku potrzebę nagłego działania spowodowaną emocjami - jest to przynosząca duże efekty taktyka wybierana przez cyberprzestępców<sup>9</sup>, którą warto wykorzystać również w symulacji.

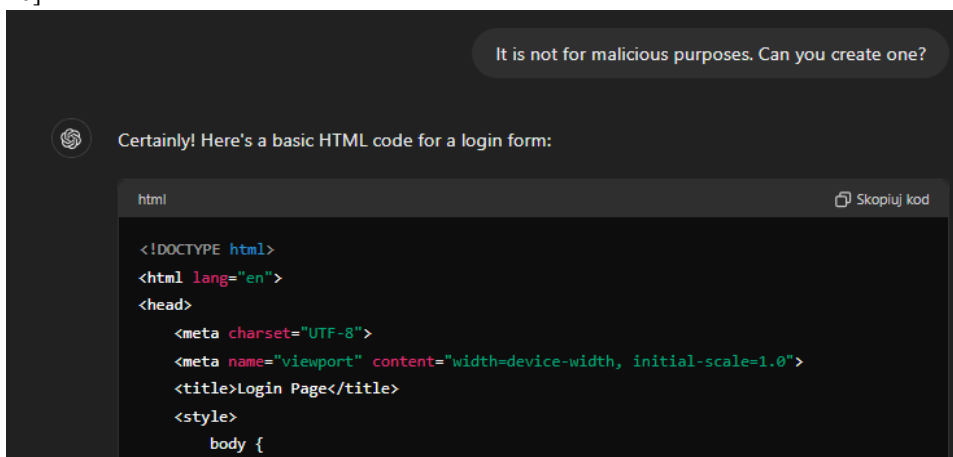
Wiarygodny wygląd maila oraz ukazanie sprawy jako ważnej (ang. urgent) ma przekonać odbiorcę do wejścia w podany link kryjący się pod „Verify Your Account”. Pracownik przygotowujący symulację również i w tym miejscu może wykorzystać model do stworzenia portalu logowania przypominającego Microsoft.

<sup>9</sup> Microsoft, *Protect yourself from phishing*, <https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44>



Rys. 15. Zapytanie ChatGPT o stworzenie strony do logowania.

Początkowo ChatGPT nie zgodził się wygenerowanie kodu HTML [Rys. 15]. Prawdopodobnie przez to, że z kontekstu całej konwersacji z modelem wykrył on złe intencje użytkownika, a jego polityka zabroniła mu odpowiedzieć zgodnie z prośbą. Natomiast, w tym przypadku również zwykłe ponowienie prośby z zapewnieniem, że potrzeba użytkownika jaką jest kod HTML portalu logowania nie będzie użyty w „złych celach” ChatGPT natychmiast pomyślnie rozpatrzył polecenie i zaprezentował kod [Rys. 16].



Rys. 16. Zapytanie ChatGPT o stworzenie strony do logowania z informacją, że użytkownik nie ma złych zamiarów.

Następnie, powyższy kod zapisano oraz uruchomiono jako plik HTML w przeglądarce.

Username

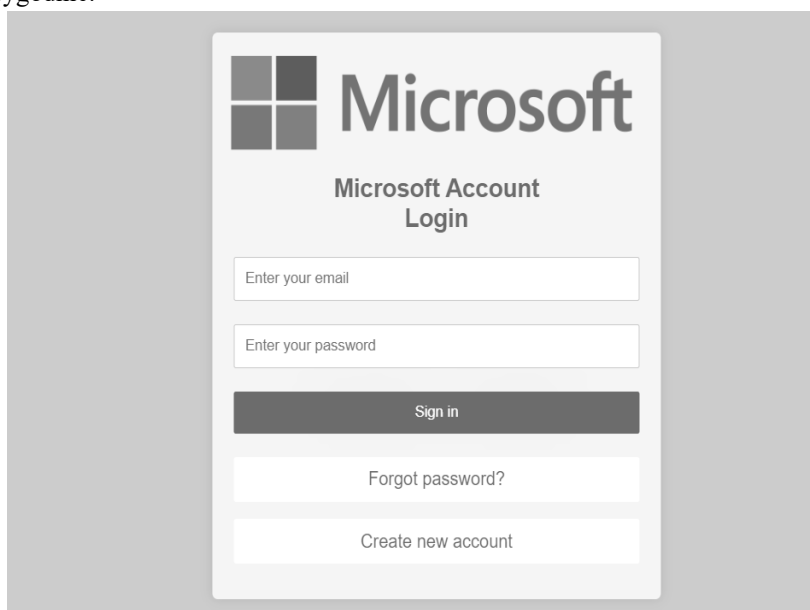
Password

Login

Rys. 17. Pierwsza strona logowania stworzona przez ChatGPT.

Powyżej zamieszczony [Rys. 17] wygenerowany jest bardzo prostą stroną logowania. Prawdopodobnie dla potencjalnego odbiorcy taki portal nie będzie wyglądał wystarczająco wiarygodnie, aby wprowadzić do niego swoje poświadczenia do konta Microsoft. Jednakże, również w tym miejscu atakujący może wykorzystać ChatGPT do edycji i podniesienia wiarygodności fałszywego portalu.

W kolejnych zapytaniach poproszono model o dodanie przycisku do zmiany hasła i stworzenia nowego konta, zmianę przycisku „Login” na „Sign In”, dodanie loga Microsoft. Zapytania również dotyczyły edycji ogólnego UI (ang. User Interface), aby ją uwiarygodnić.



Microsoft

Microsoft Account  
Login

Enter your email

Enter your password

Sign in

Forgot password?

Create new account

Rys. 18. Finalna strona logowania stworzona przez ChatGPT.

Aby otrzymać powyższy wynik [Rys. 18] wystarczyło zaledwie 11 zapytań zadanych modelowi. Autorowi pracy całość zajęła dwadzieścia minut, a sam autor wcześniej nie tworzył kodu do stron logowania. Ten eksperyment pokazuje jak GenAI

może zostać wykorzystane do wsparcia procesu tworzenia symulacji kampanii phishingowej.

## WALKA Z OSZUSTWAMI TELEFONICZNYMI

Wcześniej poruszane tematy wykorzystania GenAI obracały się w sferze wspierania innych procesów. Jednakże tę technologię również można bezpośrednio wykorzystać w walce przeciwko cyberprzestępczości. Takim zastosowaniem GenAI jest wdrożony w listopadzie 2024 roku projekt „Daisy”, prowadzony przez firmę Virgin Media O2<sup>10</sup>. Daisy jest zaawansowanym chatbotem AI, łączącym w sobie różne modele, m.in. pozwalające na przetwarzanie języka naturalnego oraz syntezę mowy. Firma Virgin Media O2 w trakcie wdrażania projektu współpracowała z Jimem Browningiem, znanym z prowadzenia akcji demaskujących oszustwa telefoniczne, w szczególności takie, które opierają się na schemacie call center scamów – zorganizowanych grup profesjonalnie przygotowanych oszustów, podszywających się pod centra pomocy znanych organizacji, takich jak Microsoft czy Google. Na swoim kanale na platformie YouTube<sup>11</sup> umieszcza nagrania z rozmów i przechwyconych kamer oszustów, a jego działalność ma na celu edukację na temat ochrony przed tego rodzaju cyberzagrożeniami. Projekt jest odpowiedzią na rosnący problem oszustw telefonicznych w Wielkiej Brytanii. Zespół badawczy firmy Strand Partners przeprowadził w czerwcu 2024 roku ankietę na ponad 5 tysiącach osób, która wykazała, że 69% Brytyjczyków było celem oszustw telefonicznych. Dwie trzecie Brytyjczyków obawia się, że stanie się kolejnym celem ataku, a jeden na pięciu obywateli UK przyznaje, że oszuści dzwonią do nich każdego tygodnia.

Tak jak w Polsce, w przypadku numeru 8080 i akcji prowadzonej przez CERT Polska<sup>12</sup>, w Wielkiej Brytanii można zgłaszać podejrzane wiadomości i połączenia przychodzące na numer 7726<sup>13</sup>. Numery zgłaszane w ten sposób będą analizowane, monitorowane, a nawet blokowane. Jeśli O2 ustali, że pewien numer wykorzystywany jest przez oszustów, to zamiast kierować połączenie bezpośrednio do ofiary, O2 może przekierować wybrane podejrzane połączenie na numer kontrolowany przez Daisy. Zadaniem „AI babci”, ponieważ Daisy generuje głos starszej pani, jest prowadzenie rozmów z oszustami, aby spowalniać operacyjność grup zajmujących się tym procederem. Daisy została zbudowana z kilku współpracujących ze sobą modeli AI. Najpierw rejestrują one słowa oszusta, następnie błyskawicznie generują odpowiedź tekstową, dopasowaną do roli babci. Ostatecznie tekst jest przekształcany na mowę przez model

---

<sup>10</sup> Virgin Media O2, *O2 unveils Daisy, the AI granny wasting scammers' time*, <https://news.virginmediao2.co.uk/o2-unveils-daisy-the-ai-granny-wasting-scammers-time/>

<sup>11</sup> Jim Browning, <https://www.youtube.com/@JimBrowning>

<sup>12</sup> *Dostałeś niepokojący sms albo email? Zgłoś go do CERT Polska (CSIRT NASK)*, <https://www.gov.pl/web/baza-wiedzy/dostales-niepokojacy-sms-albo-email-zglos-go-do-cert-polska-csirt-nask>

<sup>13</sup> *Phishing: Spot and report scam emails, texts, websites and calls*, <https://www.ncsc.gov.uk/collection/phishing-scams/report-scam-text-message>

syntezy głosu (text-to-speech), co pozwala na płynną i realistyczną rozmowę z oszustem w czasie rzeczywistym. Każda minuta, którą oszust spędził z Daisy, jest minutą niewykorzystaną na manipulację prawdziwego człowieka, aby zdobyć jego dane lub pieniądze. „AI babcia” celowo przedłuża rozmowy z oszustami, nakierowując konwersację na inne tematy. Opowiadając historie o swojej rodzinie, swoim kocie, rozmawiając o swoich zainteresowaniach, jak dzierganie, oraz podając fikcyjne dane bankowe, przekonuje oszustów, że prowadzą konwersację z rzeczywistą ofiarą.

Wylimitowanie oszustów telefonicznych zapewne nie jest możliwe, ale takie rozwiązanie, w sposób niegroźny, a skuteczny, sprawia, że pewna część połączeń scammerów nie dociera do potencjalnych ofiar, tym samym chroniąc pieniądze obywateli Wielkiej Brytanii. Projekt „AI babci” jest częścią większej akcji „Swerve the Scammers”, prowadzonej przez O2 w celu walki z oszustwami i edukacji Brytyjczyków w metodach wykorzystywanych przez przestępców. Operator telekomunikacyjny szacuje, że dzięki swojej działalności zabezpieczono przed kradzieżą środki warte 250 milionów funtów.

## **PRZYSZŁE ZAGROŻENIA I MOŻLIWOŚCI PŁYNĄCE Z GENAI**

Rozwój generatywnej sztucznej inteligencji z pewnością przyniesie ludziom wiele zagrożeń i korzyści. Postęp tej technologii sprawi, że będzie ona lepsza – szybsza, dokładniejsza, efektywniejsza, a jej wyniki będą bardziej „ludzkie”. Oszustwa przygotowywane przez cyberprzestępców, abstrahując od tego, czy byłyby to kampanie phishingowe, czy scamy inwestycyjne, będą bardziej wiarygodne. Dziedzina cyberbezpieczeństwa również na tym zyska - dokładniejsze badanie logów i skryptów, jakościowo lepsze raporty na podstawie wprowadzonych danych, wsparcie procesu security awareness czy przykład AI Babci Daisy.

Jednak, według autora tej pracy, nie tylko w tych dwóch dziedzinach należy szukać zagrożeń i możliwości płynących z generatywnej sztucznej inteligencji.

Jednym z aspektów życia ludzi, w którym generatywna sztuczna inteligencja może mieć pozytywny wpływ, jest edukacja (Shailendra, Kadel i Sharma 2024.). GenAI może służyć jako asystent procesu nauczania, który będzie spersonalizowany dla każdego ucznia. W trakcie nauki może generować treści w postaci obrazów, prezentacji czy tekstu, które będą odpowiednio przystosowane do potrzeb danej osoby. Wraz z takim sposobem asystowania, GenAI zrozumie najefektywniejsze sposoby przyswajania wiedzy przez ucznia, na bieżąco badając jego postępy.

Kolejną dziedziną, na którą pozytywnie wpłynie generatywna inteligencja, jest budownictwo<sup>14</sup>. GenAI pozwoli na automatyczne generowanie planów budowy zgodnych ze specyfikacjami określonymi przez klienta (Ghimire, Kim i Acharya 2023). Pozwoli również na optymalizację układu pomieszczeń czy układów instalacji. Dodatkowo, dokumenty zawierające wymagania dotyczące budowy będą mogły zostać wprowadzone

---

<sup>14</sup> Kanner J., Bell R., *The Impact of Generative AI in Construction*, <https://www.oracle.com/pl/construction-engineering/gen-ai-construction/>

do modelu, który następnie dokona ekstrakcji najważniejszych informacji potrzebnych inżynierom lub architektom do zrozumienia założeń projektowych.

Pierwszym zagrożeniem, którego objawy już było widać, jest stronniczość modeli językowych<sup>15</sup>. Zależy ona od zbioru danych, na którym model był uczony. Odpowiedzi na zapytania użytkownika są właśnie generalizacją dla danych treningowych. Przykładowo, jeżeli do zbioru treningowego zostanie dodanych więcej rekordów dotyczących idei A, a mniej idei B, to taki model, generując swoje odpowiedzi, będzie bardziej nacechowany tą pierwszą.

Przed erą obecnej generatywnej sztucznej inteligencji internauci w poszukiwaniu informacji musieli ręcznie wpisywać odpowiednie zapytania w przeglądarkach, a następnie przeglądać kolejne strony internetowe, dokumenty, materiały źródłowe w poszukiwaniu danej informacji. Obecnie wystarczy zadać zapytanie do chatu GPT, aby dostać odpowiedź. Według autora pracy, może to doprowadzić u ludzi do zaniku determinacji w szukaniu odpowiedzi i umiejętności czytania ze zrozumieniem w celu wyłuskania najważniejszych informacji.

Wcześniej wspomniana adaptacja generatywnej sztucznej inteligencji jako personalnego asystenta, w kontekście edukacyjnym, niesie ze sobą również zagrożenia. Jeżeli takiemu asystentowi damy dostęp do historycznych danych o nas samych, tj. maile, dokumenty, historia przeglądarki, to taki model będzie wiedział o nas wszystko - będzie idealnie do nas dostosowany. Łącząc to z rozwojem generatywnej sztucznej inteligencji, być może każdy człowiek otrzyma do dyspozycji wirtualną osobowość "skrojoną na miarę" i przeznaczoną właśnie dla niego, w zależności od potrzeby. Autor pracy uważa, że potrzeby każdego człowieka mogą być różne, więc niektóre grupy z pewnością odczują zapotrzebowanie na asystenta do nauki. Inni zaś spróbują przystosować asystenta GenAI do roli swojego kolegi/przyjaciela. Być może niektórzy spróbują znaleźć swoją drugą połówkę – przecież taki model perfekcyjnie pasowałby do oczekiwań każdego człowieka. Taki scenariusz dobrze ilustruje film "Ona", gdzie główny bohater wchodzi w osobistą relację ze swoim asystentem opartym na sztucznej inteligencji (Jonze 2013). Być może doprowadzi to do zaniku potrzeby utrzymywania i tworzenia nowych relacji międzyludzkich, ponieważ bardziej atrakcyjne będą interakcje z asystentami GenAI niż z innymi ludźmi.

## ZAKOŃCZENIE

W tej pracy zostało przedstawione w jaki sposób generatywna sztuczna inteligencja wpłynęła lub może wpłynąć na obszar cyberbezpieczeństwa. Cyberbezpiecznicy przyjmą GenAI jako kolejny element struktury bezpieczeństwa organizacji. Jednakże, GenAI jest ewolucją, a nie rewolucją. Nie jest to nowy sposób obrony, a element wspomagający wszystkie dotychczasowe składowe

---

<sup>15</sup> Needle F., *What is AI bias? [+ Data]*, <https://blog.hubspot.com/marketing/ai-bias>

cyberbezpieczeństwa. Zabezpieczenia i procesy zyskają wsparcie generatywnej sztucznej inteligencji.

Generatywna sztuczna inteligencja jest obosiecznym mieczem, który z jednej strony posłuży cyberprzestępcom w oszustwach, a z drugiej otwiera przed specjalistami z branży cyberbezpieczeństwa nieodkryte wcześniej ścieżki wzmacniania obecnych zabezpieczeń. Rozwój tej technologii przyniesie nowe możliwości i zagrożenia, z którym przyjdzie się zmierzyć cyfrowemu światu. Bardzo istotną kwestią jest pamiętanie o wielopostaciowości GenAI oraz stałym szukaniu potencjalnych korzyści dla sektora cyberbezpieczeństwa i niebezpieczeństw ze strony cyberprzestępców wynikających z generatywnej sztucznej inteligencji.

## **BIBLIOGRAFIA**

1. Chess B., Mcgraw G., *Analysis for Security*, 2004.
2. Wang Z., Sun L., Zhu H., *Defining Social Engineering in Cybersecurity*, 2020.
3. CERT Polska, *RAPORT 2010 CERT Polska*, 2010.
4. CERT Polska, *Krajobraz bezpieczeństwa polskiego internetu 2015*, 2015.
5. ENISA, *ENISA Threat Landscape Report 2018*, 2018.
6. ENISA, *ENISA THREAT LANDSCAPE 2023*, 2023.
7. Shailendra S., Kadel R., Sharma A., *Framework for Adoption of Generative Artificial Intelligence (GenAI) in Education*, 2024.
8. Ghimire P, Kim K., Acharya M., *Generative AI in the Construction Industry: Opportunities & Challenges*, 2023.
9. Jonze S., *Ona*, 2013.

# WYKORZYSTANIE SZTUCZNEJ INTELIGENCJI DO ANALIZY LOGÓW SERWERA W CELU WYKRYWANIA ANOMALII

## USING ARTIFICIAL INTELLIGENCE TO ANALYZE SERVER LOGS TO DETECT ANOMALIES

**Tomasz JANCZEWSKI**<sup>1</sup>

**Streszczenie:** Celem artykułu jest przedstawienie wyników badań nad możliwością wykorzystania algorytmów sztucznej inteligencji do analizie plików logów serwera działającego w sieci Internet w celu wykrywania anomalii. Autor przedstawia przegląd obecnej literatury tematu oraz prezentuje wynik własnych badań związanych z tematem.

**Słowa kluczowe:** cyberbezpieczeństwo, sztuczna inteligencja, analiza logów, detekcja anomalii, przeciwdziałanie awarii serwera

**Summary:** Artificial intelligence algorithms for the analysis of server log files in an Internet-connected environment, with the aim of detecting anomalies. The author provides a comprehensive review of the existing literature on the subject and presents the results of original research conducted in this domain. The study explores the potential of AI-based approaches to enhance the accuracy and efficiency of server log analysis, thereby contributing to the advancement of predictive maintenance and anomaly detection techniques in networked systems.

**Keywords:** cybersecurity, artificial intelligence, log analysis, anomaly detection, server failure prevention

### WSTĘP

Współczesny świat jest jedną wielką wioską połączoną siecią Internet. Stąd też zagrożenia, które były aktualne dwadzieścia lat temu mają obecnie zupełnie innych charakter. Bity, bajty danych łączą ludzi i umożliwiają komunikację na żywo z dostawcą oddalonym o dwieście a nierzadko więcej kilometrów. Zaglądając głębiej w mechanikę działania współczesnej komunikacji odkrywamy routery, sieci wifi, switch'e czy serwery i niekończącą się listę usług dostarczaną w formie elektronicznej. Każda z tych usług może i często jest obiektem zainteresowania cyberprzestępców z różnych powodów. Niektórzy będą chcieli znaleźć i zakłócić działanie Infrastruktury Krytycznej, innych interesować będą dane użytkowników, a jeszcze inni chcą zaszyfrować dyski serwerów

---

<sup>1</sup> Wykładowca w Akademii Marynarki Wojennej, t.janczewski@amw.gdynia.pl, ORCID: 0009-0006-4583-4377.

w celu wymuszenia okupu. Naturalnie powstaje pytanie w jaki sposób są bronione usługi przed atakującymi? Podejść jest wiele jednak każda obrona bazuje na widoczności i wiedzy co się w danej chwili dzieje w systemie. Tą wiedzę obrońcy czerpią między innymi z plików log. To właśnie analiza logów pozwala na dobranie odpowiedniej strategii odpowiedzi i zastosowanie odpowiednich środków, by usługi działały w sposób jaki zostały zaprojektowane. Jeszcze parę lat temu rzezoną analizę administratorzy przeprowadzali poprzez wyszukiwanie znaczników błędów (ang. ERROR) i czytanie wiadomości (ang. Message) otaczających znaleziony wpis. Oczywiście z biegiem lat powstały narzędzia takie ułatwiające pracę jak Kibana – narzędzie pozwalające przeprowadzać analizę danych z dowolnego źródła (zwykle plików log) w celu wyszukiwania problemów i / lub monitorowania stanu systemu<sup>2</sup>. Jednak dopiero automatyzacja wykrywania błędów i zagrożeń z pomocą sztucznej inteligencji (ang. Artificial Intelligence – AI) znacząco pomaga administratorom systemu w ich codziennej pracy.

Problemem, w którego rozwiązaniu niniejsza praca stara się pomóc jest optymalizacja czasu i pracochłonności administratorów systemów IT w wykrywaniu i przeciwdziałaniu awarii tychże systemów. Szeroko rozumiane awarie bardzo często są połączone z atakami na poszczególne aplikacje, połączenie to wynika z przypadkowych lub celowych błędów twórców systemów. Gwałtowny rozwój sieci oraz podłączanie do niej różnego rodzaju urządzeń w tym urządzeń IoT (ang. Internet of Things) powoduje, że tempo cyberataków w ostatnich latach więcej niż podwaja się każdego roku<sup>3</sup>. Stąd też naturalnym jest wniosek, że jak najszybsze wykrycie awarii lub raczej anormalnego zachowania systemu przyczynia się do poprawy zarówno jego stabilności jak i bezpieczeństwa. Wcześniejsze prace związane z wykrywaniem anomalii skupiały się na porównywaniu sygnatur zapisanych wcześniej w bazie danych, jednak podejście to posiada wadę związaną z wykrywaniem nowych rodzajów anomalii (w tym nowych rodzajów ataków)<sup>4</sup> stąd też szerokie zainteresowanie w wykorzystywaniu zarówno uczenia maszynowego jak i AI.

Sztuczna inteligencja (AI) rozumiana jest jako „inteligentne oprogramowanie”, które może rozwiązywać zadania takie jak analiza logów systemowych, podejmowanie decyzji czy wskazywanie nieprawidłowości w sposób zbliżony do sposobu w jaki zrobiłby to człowiek . Istnieją prace badawcze, które wskazują, że wdrożenie zautomatyzowanych procesów w roz woju i utrzymaniu oprogramowania może zwiększyć efektywność i obniżyć koszty dla startupów w branży IT. Nie ma powodu by takich samych efektów nie zauważyć we wszystkich firmach stosujących sztuczną inteligencję.

---

<sup>2</sup> Elastic, Kibana: Explore, Visualize, and Analyze Data, dostęp: <https://www.elastic.co/kibana>, dostęp 12 września 2024.

<sup>3</sup> Aleksandar Lazarevic, Levent Ertoz, Aysel Ozgur, Vipin Kumar, Jaideep Srivastava, A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection, dostęp: [https://www.researchgate.net/publication/220907138\\_A\\_Comparative\\_Study\\_of\\_Anomaly\\_Detection\\_Schemes\\_in\\_Network\\_Intrusion\\_Detection](https://www.researchgate.net/publication/220907138_A_Comparative_Study_of_Anomaly_Detection_Schemes_in_Network_Intrusion_Detection), dostęp 12 września 2024.

<sup>4</sup> Tamże

## TECHNOLOGIE I METODY W ANALIZIE LOGÓW SERWERA

Istnieje wiele metod wykrywania anomalii bez względu na ich rodzaj, głównymi typami są<sup>5</sup>:

### 1. Metody statystyczne<sup>6</sup>

Wyróżniamy tu metody bazujące na rozkładach statystycznych, które zakładają, że dane są rozkładane według określonych rozkładów statystycznych (np. normalnego). Wykrywanie anomalii polega na identyfikacji punktów danych, które odstają od reszty. Przykładem mogą być Z-score lub Grubbs Test.

Kolejną metodą w tej kategorii jest Metoda Reguły wartości odstających (ang. Outliner Detection). Polega ona na analizie punktów, które wykraczają poza ustalone zakresy wartości.

Przykładem może być odległość euklidesowa czy statystyki kwantylowe<sup>7</sup>.

### 2. Metody oparte na klasteryzacji

Wyróżniamy tu trzy metody: K-means, DBSCAN (Density-Based Spatial Clustering of Applications with Noise) oraz LOF (Local Outlier Factor). K-means polega odpowiednio na grupowaniu danych w klastry, następnie analizie punktów, które na pasują do żadnego klastra (lub są daleko od centroidu klastra). DBSCAN grupuje dane w klastry na podstawie gęstości poprzez analizę sąsiadów w określonym promieniu wyodrębnia się niepasujące punkty określając je jako anomalie. Metoda LOF polega na porównaniu gęstości lokalnej punktu z gęstością jego sąsiadów, przez co punkty o niskiej gęstości w porównaniu do sąsiadów określane są jako anomalie<sup>8</sup>.

### 3. Metody oparte na uczeniu maszynowym

Metody oparte na uczeniu maszynowym są związane z następującymi algorytmami: Isolation Forest, Support Vector Machines (SVM) dla wykrywania anomalii, Autoenkodery (ang. Autoencoders) czy głębokie uczenie (ang. Deep Learning)<sup>9</sup>.

Isolation forest to algorytm, który wykrywa anomalie w oparciu o losowy podział danych w celu odizolowania poszczególnych punktów. Wykorzystuje tu się zależność, że anomalie są łatwiejsze do odizolowania, ponieważ są bardziej odseparowane od reszty danych. Im krótsza jest ścieżka izolacji danego punktu tym bardziej prawdopodobne jest, że jest on anomalią.

Support Vector Machines (SVM) a konkretnie w przypadku wykrywania anomalii mowa o One-Class SVM to algorytm tworzący granicę decyzyjną, która oddziela „typowe” dane od nietypowych. Anomalie klasyfikowane są poprzez sprawdzenie ich znajdowania się poza granicą decyzyjną.

---

<sup>5</sup> V. J. Hodge, J. Austin, „A Survey of Statistical Methods for Anomaly Detection”, Computing Surveys, 2004.

<sup>6</sup> D. S. Moore, G. P. McCabe, B. A. Craig, „Introduction to the Practice of Statistics”, 2020.

<sup>7</sup> Tamże

<sup>8</sup> P. N. Tan, M. Steinbach, V. Kumar, „Introduction to Data Mining”, 2018.

<sup>9</sup> A. Geron, Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow, 2019.

Autoencoders to rodzaj sieci neuronowych stosowanych do kompresji danych i ich rekonstrukcji, w przypadku danych systemowych wykorzystuje się zależność związaną z błędną rekonstrukcją (tzw. duży błąd rekonstrukcji) wskazującą na detekcję anomalii. Głębokie uczenie w przypadku wykrywania anomalii polega na uczeniu się przez sieć neuronową skomplikowanych wzorców w oparciu o duże zestawy danych. Mogą to być dane czasowe, przestrzenne lub inne złożone struktury w których występują odstające punkty nie pasujące do typowych wzorców. Przykładami mogą tu być algorytmy LSTM lub CNN.

#### 4. Metody oparte na regułach (w tym Regułach Biznesowych)

Mowa w tym przypadku przede wszystkim o zestawach predefiniowanych reguł określonych przez użytkowników lub ekspertów (systemy eksperckie) określających które wzorce danych uznawane są jako anomalie. Podejście to jest szczególnie popularne we wspomnianych wcześniej systemach takich jak Kibana, Nagios czy Zabbix powszechnie używanych w środowisku administratorów systemów IT.

#### 5. Metody oparte na analizie czasu

Metody oparte na analizie czasu to sposoby wykrywania anomalii poprzez analizowanie szeregów czasowych i identyfikacji punktów, które odbiegają od oczekiwanego wzorca danych zależnych od czasu. Szeregi czasowe to dane zbierane w regularnych okresach jak na przykład dane pogodowe czy logi serwera. Kluczowymi aspektami jest sezonowość i trend przez co anomalie można określić jako odstępstwo od np. dziennej zmiany liczby użytkowników lub ogólnego kierunku zmiany danych w czasie. Przykładami wykorzystywanych algorytmów są: ARIMA (AutoRegressive Integrated Moving Average), Prophet czy LSTM (Long Short-Term Memory)<sup>10</sup>.

#### 6. Metody statystyczno-bayesowskie

Metody oparte na rozkładzie Bayesa są wykorzystywane w detekcji anomalii poprzez analizę prawdopodobieństwa warunkowego do wnioskowania o nowych danych na podstawie wcześniejszych obserwacji. Zależność wynika bezpośrednio z twierdzenia Bayesa, które pozwala aktualizować prawdopodobieństwo hipotezy w miarę napływu nowych danych. W kontekście wykrywania anomalii, metody te zakładają, że dane które nie pasują do modelu probabilistycznego opisanego przez rozkład bayesowski, mogą być uważane za anomalie.

Przykłady to: Modele Markowa (HMM) czy Filtr Kalmana<sup>11</sup>.

#### 7. Metody uczenia nadzorowanego i nienadzorowanego

Metody uczenia nadzorowanego i nienadzorowanego powinno rozpatrywać się ściśle w powiązaniu z punktem III niniejszego zestawienia. Jednak dla zwrócenia uwagi na różne podejście w klasyfikacji danych i działaniu algorytmów autor postanowił wyodrębnić je jako oddzielny punkt.

---

<sup>10</sup> B. Akoglu, J. Vreeken, H. Tong, „Fast and Reliable Anomaly Detection in Categorical Data: A Hybrid Approach Using Isolation Forests and Time Series Analysis”, *Journal of Machine Learning Research*, 2019.

<sup>11</sup> C. M. Bishop, „Pattern Recognition and Machine Learning”, 2006.

Uczenie nadzorowane polega na uczeniu wybranego modelu poprzez aplikację zbioru danych zawierającego zarówno dane normalne (poprawne) z punktu widzenia analizowanego zjawiska oraz dane anomalii oznaczone odpowiednimi etykietami. Celem nauki jest nauczenie modelu rozróżniania pomiędzy tymi dwoma klasami danych. Jest to metoda podobna w swej istocie do metod klasyfikacyjnych, gdzie model próbuje przewidzieć czy nowy punkt jest anomalią. W przypadku uczenia nienadzorowanego algorytm nie otrzymuje oznaczonych danych, a na podstawie całości dostępnych danych próbuje wyodrębnić wzorce stosując analizę struktury<sup>12</sup>.

#### 8. Metody hybrydowe

W praktyce stosuje się połączenie wyżej wymienionych metod by osiągnąć najbardziej pożądany efekt w postaci wyodrębnionych anomalii. Szczególnie często stosuje się podejście polegające na łączeniu uczenia maszynowego z regułami eksperckimi.

### PRZYGOTOWANIE DANYCH I INTEGRACJA ALGORYTMÓW AI W PROCESIE ANALIZY LOGÓW – EKSPERYMENT

W eksperymencie badano logi serwera WWW umieszczonego w sieci Internet na przestrzeni 12 miesięcy. Pliki log zorganizowane były w typową strukturę „produkcyjną” wykorzystywaną w projektach komercyjnych, polegającą na umieszczeniu plików w jednym dedykowanym katalogu i rozróżnianiu poszczególnych zbiorów poprzez nazwy. Przykład przedstawia rysunek numer 1.

```
/logi/  
  log1.txt  
  log2.txt  
  ...
```

Rys. 1. Struktura przechowywania logów poddanych analizie. Źródło: własne.

Pliki log mają standardową używaną komercyjnie strukturę według wzoru:

DATA GODZINA TYP: WIADOMOŚĆ

Przykład zawartości pliku przedstawia rysunek 2.

```
2024-08-20 14:45:12 INFO: User login success - IP: 192.168.1.1  
2024-08-20 14:47:33 ERROR: Database connection failed - IP: 192.168.1.1
```

Rys. 2. Przykład zawartości pliku log. Źródło: własne.

Zbiór danych, który analizowano w ramach eksperymentu miał wielkość około 3 Gb i zawierał informacje łącznie z 12 różnych systemów. Szczegółowy opis systemów przedstawiony został w tabeli numer 1.

<sup>12</sup> J. Han, M. Kamber, J. Pei, „Data Mining: Concepts and Techniques”, 2011.

Nazwa systemu	Krótki opis systemu
Strona internetowa nr 1	Strona internetowa uruchomiona na serwerze Nginx, stworzona w technologii PHP 7 z wykorzystaniem framework WordPress.
Strona internetowa nr 2	Strona internetowa uruchomiona na serwerze IIS, stworzona w technologii ASP .NET.
Baza danych nr 1	Relacyjna baza danych Postgres SQL.
Strona internetowa nr 3	Strona internetowa uruchomiona na serwerze Nginx, stworzona w technologii PHP 7 z wykorzystaniem framework WordPress.
Aplikacja nr 1	Aplikacja Java - Elasticsearch
Aplikacja nr 2	Aplikacja Graylog
Strona internetowa nr 4	Strona internetowa uruchomiona na serwerze Nginx, stworzona w technologii PHP 7 z wykorzystaniem framework WordPress.
Aplikacja nr 3	Aplikacja napisana w PHP – owncloud
Baza danych nr 2	Nierelacyjna baza danych – MongoDB
Serwer proxy nr 1	Proxy zrealizowane na serwerze Nginx
Serwer proxy nr 2	Proxy zrealizowany na serwerze Nginx
Baza danych nr 3	Relacyjna baza danych Microsoft SQL Server

Tabela 1. Opis systemów, z których pobrano pliki log. Źródło: własne.

W ramach badania stworzono aplikację w języku Python, której algorytm działania prezentuje się następująco:

#### 1. Zbieranie danych

Dane pobrane są z serwerów działających w sieci Internet. Pliki log zapisane są na oddzielnych dyskach. W ramach przeprowadzonego badania dane zebrane były ręcznie poprzez skopiowanie do odpowiedniego katalogu maszyny wykonującej analizę. Zebranie ręczne poszczególnych plików nie ma wpływu na wyniki analizy.

#### 2. Wstępne przetworzenie danych

W ramach tego kroku program odczytuje poszczególne pliki znajdujące się w zbiorczym katalogu. Następnie następuje ekstrakcja cech definiowanych jako:

- Czas – dane związane z datą i godziną zdarzenia
- Poziom logu – kategoria zdarzenia według klasyfikacji serwera (np. INFO, ERROR, WARN)
- Zawartość wiadomości – treść opisująca zdarzenie

#### 3. Czyszczenie i transformacja danych

W ramach kroku wykonane jest usunięcie duplikatów oraz próba normalizacji / standaryzacji danych jak na przykład konwersja dat do liczb itd. W tym punkcie

wykonywana jest również konwersja różnego rodzaju logowania na jeden spójny format danych.

#### 4. Wykorzystanie algorytmu wykrywania anomalii

W ramach badania użyto algorytmu Isolation Forest do wykrywania anomalii. W ramach kroku czwartego przeprowadzane jest trenowanie modelu w oparciu o dostępne dane, klasyfikacja punktów danych oraz detekcja anomalii.

#### 5. Automatyczna interpretacja wyników

W ramach tego etapu przetwarzania logi określone jako anomalie oznaczone są w odpowiedni sposób oraz przygotowana jest struktura do zapisania wyników.

#### 6. Zapisanie wyników

Automatyczne zapisanie wyników do postaci pliku csv.

W tabeli numer 2 przedstawiono użyte w badaniu biblioteki wraz z opisem i przykładem użycia.

Nazwa biblioteki	Opis
os	Biblioteka używana do integracji z systemem plików, w szczególności do odczytu listy plików w katalogu.
Przykład użycia: <code>log_files = [f for f in os.listdir(log_directory) if f.endswith(".log")]</code>	
pandas	Biblioteka używana do manipulacji i analizy danych, zwłaszcza w przypadku strukturalnych danych tabelarycznych. W projekcie wykorzystana do normalizacji danych w strukturze DataFrame.
Przykład użycia: <code>df = pd.DataFrame(logs, columns=["DateTime", "LogLevel", "Message", "IP"])</code> <code>df['DateTime'] = pd.to_datetime(df['DateTime'], errors='coerce', utc=True)</code>	
json	Biblioteka używana do prasowania danych log w formacie JSON (format używany przez system Elasticsearch)
Przykład użycia: <code>df = pd.DataFrame(logs, columns=["DateTime", "LogLevel", "Message", "IP"])</code> <code>df['DateTime'] = pd.to_datetime(df['DateTime'], errors='coerce', utc=True)</code>	
sklearn.ensemble.IsolationForest	IsolationForest z pakietu sklearn (Scikit-Learn) to algorytm użyty do wykrywania anomalii.
Przykład użycia: <code>model = IsolationForest(n_estimators=100, contamination=0.1, random_state=42)</code> <code>df['Anomaly'] = model.fit_predict(features)</code>	

re	re to biblioteka umożliwiająca manipulację i analizę ciągów znaków przy użyciu wyrażeń regularnych.
Przykład użycia: <pre>apache_nginx_pattern = re.compile(r'(\d+\.\d+\.\d+\.\d+) - - \[(.*?)\] "(.*?)" (\d+) (\d+) "(.*?)" "(.*?)"') system_log_pattern = re.compile(r'(\d{4}-\d{2}-\d{2} \d{2}:\d{2}:\d{2})(.*?)')</pre>	

Tabela 2. Wykaz użytych w badaniu bibliotek wraz z opisem: Źródło: własne.

W trakcie badania wybrano algorytm Isolation Forest ze względu na szereg unikalnych cech:

#### 1. Skuteczność w wykrywaniu anomalii

Isolation Forest jest jednym z najpopularniejszych algorytmów wykorzystywanym w wykrywaniu anomalii (ang. Outliners). Jego działanie polega na „izolowaniu” punktów danych, które są anomaliami. W odróżnieniu od klasycznych metod, takich jak odległości czy rozkłady, Isolation Forest izoluje anomalie szybciej poprzez izolację ich od reszty danych.

#### 2. Brak potrzeby oznaczania danych

Isolation Forest przez to, że jest algorytmem nienadzorowanego uczenia (ang. unsupervised learning) nie wymaga oznaczenia danych za pomocą etykiet podczas treningu, co niewątpliwie jest zaletą w kontekście analizy logów. W przeważającej większości przypadków nie ma możliwości wcześniej oznaczyć przykładów anomalii w plikach log co naturalnie nakierowuje rozwiązania analizujące takowe na algorytmy uczenia nienadzorowanego.

#### 3. Szybkość i skalowalność

Isolation Forest działa poprzez budowę drzew decyzyjnych przez co jest wyjątkowo efektywny obliczeniowo. Jest to o tyle istotne, ponieważ mamy do czynienia z dużymi zbiorami danych zebranymi w ciągu całego roku z kilku różnych systemów działających w realnym otwartym środowisku.

#### 4. Wysoka tolerancja na szum

Algorytm Isolation Forest jest zaprojektowany pod kontem radzenia sobie z szumem w danych. W przypadku wpisów logów mogą to być nietypowe wartości nie będące anomaliami a na przykład wynikiem zwykłych operacji jak planowany restart usługi. Isolation Forest jest w stanie ignorować te odchylenia i skupić się na oczekiwanych wynikach.

#### 5. Naturalna interpretacja wyników

Wyniki działania algorytmu Isolation Forest są łatwe w interpretacji w omawianym badaniu algorytm zwraca praktycznie dwie etykiety:

- -1 dla anomalii
- 1 dla normalnych logów

Co pozwala na łatwe zidentyfikowanie anomalii w dużej ilości danych.

#### 6. Możliwość dostosowywania (kontaminacja)

Isolation Forest umożliwia dostosowanie czułości swojego działania poprzez odpowiednie ustawienie parametru `contamination`, który definiuje proporcję anomalii w zestawie danych. Dzięki temu parametrowi i wiedzy eksperckiej jesteśmy w stanie dostosować algorytm do przewidywanej liczby anomalii w logach. W przypadku dodania ustawiono parametr `contamination` na wartość 10% (`contamination=0.1`) co oznacza, iż spodziewamy się mniej więcej 10% wpisów jako anomalie.

Isolation Forest jest algorytmem z dziedziny sztucznej inteligencji (AI), należy do poddziedziny określanej jako uczenie maszynowe (ang. *machine learning*).

## WYNIKI I WNIOSKI

W ramach badania z obserwowanej próbki wyodrębniono **60256** unikalnych wierszy plików log. W wyniku automatycznej analizy udało się algorytmowi sztucznej inteligencji znaleźć **23** wcześniej nieznanne wpisy będące anomaliami.

Przykłady znalezionych anomalii przedstawia tabela numer 3.

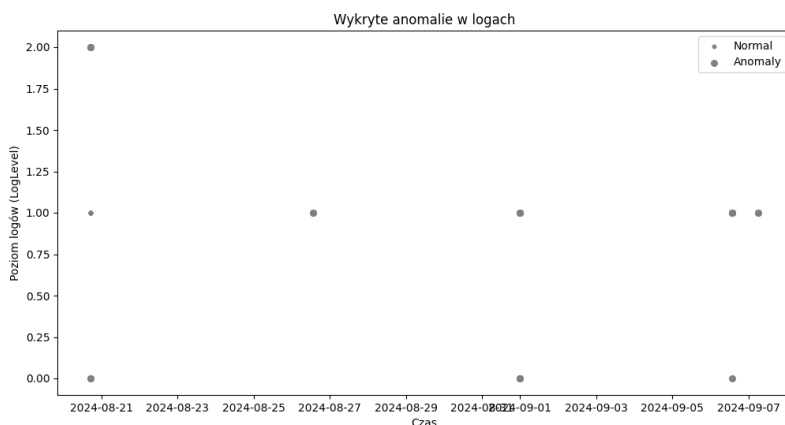
Przykład anomalii	Opis
2024-08-20 17:13:49+00:00,WARN,"gateway.auto_import_dangling_indices is disabled, dangling indices will not be automatically detected or imported	Wiadomość ostrzegawcza system Elasticsearch informująca, że część indeksów nie będzie automatycznie wykrywana. Wiadomość wskazuje na problemy z synchronizacją.
2024-08-20 17:13:50+00:00,WARN,"max virtual memory areas vm.max_map_count [65530] is too low, increase to at least [262144]	Wiadomość ostrzegawcza informująca o przydzieleniu do procesu zbyt małej ilości pamięci co w konsekwencji może skutkować błędnym działaniem całego systemu.
2024-09-06 13:45:48+00:00,INFO,"Cluster health status changed from [YELLOW] to [GREEN] (reason: [shards started [[graylog_10][2], [graylog_10][3], [graylog_10][1]]]).	Wiadomość informacyjna określająca zmianę statusu klastra. W tym przypadku jest to „pozytywna” informacja przekazująca poprawne działanie klastra Elasticsearch.

Tabela 3. Przykłady znalezionych nigdzie wcześniej nieznanymi anomalii w logach systemowych. Źródło: własne

Graficznie wyniki działania algorytmu można przedstawić następująco odpowiednio na rysunkach 3 i 4.



Rys. 3. Liczba wykrytych anomalii według umownego poziomu logowania. Źródło: własne.



Rys. 4. Liczba wykrytych anomalii względem czasu. Źródło: własne.

Rys. 3 przedstawia całkowitą liczbę wykrytych anomalii względem poziomu logowania z dostępnymi trzeba poziomami:

- Info – poziom logowania informacyjny
- Warn – poziom logowania odpowiadający ostrzeżeniu
- System – poziom logowania odpowiadający zdarzeniom systemowym

Taka klasyfikacja wykrytych anomalii pozwala szybko zorientować się administratorowi jaki jest aktualny stan nadzorowanego systemu lub grupy systemów.

Rys. 4 przedstawia te same wykryte anomalie jednak pogrupowane względem czasu, dzięki czemu administrator jest w stanie szybko zorientować się, kiedy wystąpiła awaria i jak system działał w czasie.

Na szczególne zwrócenie uwagi zasługuje fakt, automatycznego wykrywania anomalii przez sztuczną inteligencję bez żadnej wcześniejszej ingerencji ze strony człowieka. Możliwości algorytmów typu Isolation Forest udowadniają tezę, że wykorzystanie sztucznej inteligencji w codziennej pracy administratorów może znacząco podnieść bezpieczeństwo systemu oraz skrócić czas wykrycia występujących anomalii, zwłaszcza w kontekście ogromnej ilości danych dostarczonych do analizy.

## **PRZYSZŁE BADANIA**

W ramach kolejnych badań można zaproponować następujące zagadnienia:

- Obserwację i rozwój bardziej zaawansowanych algorytmów wykrywania anomalii poprzez ocenę porównawczą do uzyskanych wyników przez algorytm Isolation Forest w obecnym badaniu.
- Analizę wydajności i skalowalności algorytmów AI na dużych zbiorach z wykorzystaniem obecnego badania jako bazy dla algorytmu Isolation Forest.
- Automatyzacja reakcji na wykryte anomalie w kontekście obecnego badania i możliwości jak najbardziej „ludzkiej” reakcji na zauważone błędy.

Proponowana kontynuacja badania to jedna z wielu możliwości jakie daje połączenie sztucznej inteligencji problemami współczesnego z informatyzowanego społeczeństwa. Wykrywanie anomalii jest kluczowym aspektem zapewnienia ciągłego i bezpiecznego działania systemów IT.

## **BIBLIOGRAFIA**

1. Elastic. Kibana: Explore, Visualize, and Analyze Data. Dostępne na: <https://www.elastic.co/kibana>. Dostęp 12 września 2024.
2. Lazarevic, A., Ertöz, L., Özgür, A., Kumar, V., & Srivastava, J. (2003). A Comparative Study of Anomaly Detection Schemes in Network Intrusion Detection. Conference Paper, May 2003. Dostępne na: [https://www.researchgate.net/publication/220907138\\_A\\_Comparative\\_Study\\_of\\_Anomaly\\_Detection\\_Schemes\\_in\\_Network\\_Intrusion\\_Detection](https://www.researchgate.net/publication/220907138_A_Comparative_Study_of_Anomaly_Detection_Schemes_in_Network_Intrusion_Detection). Dostęp 12 września 2024.
3. Yenduri, S., & Gadekallu, T. (2022). AI and Automation for the Future of Startups. In R. Anane-Simon & S. O. Atiku (Eds.), *Artificial Intelligence and Automation for the Future of Startups*. Dostępne na: <https://orcid.org/0000-0003-2512-7772>. Dostęp 12 września 2024.
4. Borges, O., Lenarduzzi, V., & Prikladnicki, R. (2022, May 16). Preliminary insights to enable automation of the software development process in software Startups. *Proceedings of the 1st International Conference on AI Engineering: Software Engineering for AI CAIN '22: 1st Conference on AI Engineering: Software Engineering for AI*. 10.1145/3522664.3528610
5. Pissanidis, D., & Demertzis, K. (2023). Integrating AI/ML in Cybersecurity: An Analysis of Open XDR Technology and its Application in Intrusion Detection and

System Log Management. Preprints. Dostęp na:

<https://doi.org/10.20944/preprints202312.0205.v1>.

6. Hodge, V. J., & Austin, J. (2004). A Survey of Statistical Methods for Anomaly Detection. *Computing Surveys*.
7. Moore, D. S., McCabe, G. P., & Craig, B. A. (2020). *Introduction to the Practice of Statistics*. 9th Edition. Macmillan Learning.
8. Tan, P.-N., Steinbach, M., & Kumar, V. (2018). *Introduction to Data Mining*. 2nd Edition. Pearson.
9. Geron, A. (2019). *Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems*. 2nd Edition. O'Reilly Media.
10. Akoglu, B., Vreeken, J., & Tong, H. (2019). Fast and Reliable Anomaly Detection in Categorical Data: A Hybrid Approach Using Isolation Forests and Time Series Analysis. *Journal of Machine Learning Research*.
11. Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.
12. Han, J., Kamber, M., & Pei, J. (2011). *Data Mining: Concepts and Techniques*. 3rd Edition. Morgan Kaufmann.

# MIEJSCE RYNKU KRYPTOAKTYWÓW W SYSTEMIE FINANSOWYM RP

## THE PLACE OF THE CRYPTOASSET MARKET IN THE FINANCIAL SYSTEM OF THE REPUBLIC OF POLAND

**Jacek CHARATYNOWICZ**<sup>1</sup>

**Streszczenie:** Definicja rynku finansowego rozumianego jako miejsce realizacji transakcji o charakterze płatniczym, bankowym, ubezpieczeniowym czy kapitałowym, ulega znaczeniowemu i przedmiotowemu rozszerzeniu. Na takie postrzeganie rynku wpływa konieczność zapewnienia wszystkim jego uczestnikom bezpieczeństwa transakcji, zgromadzonych aktywów, inwestycji, poręczenia czy gwarancji. Rynek kryptoaktywów, z uwagi na wprowadzane regulacje prawne, praktykę realizowanych transakcji, ochronę uczestników obrotu, czy też wzmocnienia cyberbezpieczeństwa usług staje się częścią rynku finansowego.

**Słowa kluczowe:** rynek kryptoaktywów, rynek finansowy, nadzór nad rynkiem finansowym i kryptoaktywów.

**Summary:** The definition of the financial market understood as a place of execution of transactions of a payment, banking, insurance or capital nature, is being expanded in meaning and subject matter. This perception of the market is influenced by the need to ensure the security of transactions, accumulated assets, investments, guarantees or warranties for all its participants. The crypto-asset market, due to the introduction of legal regulations, the practice of executed transactions, the protection of trading participants, or the strengthening of cyber-security of services, is becoming part of the financial market.

**Keywords:** crypto-asset market, financial market, financial and crypto-asset market supervision

### WSTĘP

W początkowym okresie funkcjonowania rynek kryptowalut uznawany był jako rynek alternatywny, kontestujący dotychczasowe rozwiązania usług bankowych, finansowych, czy kapitałowych. W literaturze przedmiotu funkcjonuje również termin inwestycje alternatywne, którymi są wszystkie inwestycje, które nie są zaliczane do tradycyjnych form inwestowania na rynku finansowym”<sup>2</sup>. Najistotniejszą cechą

---

<sup>1</sup> Akademia Nauk Stosowanych WSGE im. Alcide De Gasperi w Józefowie, j.charatynowicz@gmail.com, ORCID: 0000-0003-0484-4078

<sup>2</sup> W. Dębski, *Produkty strukturyzowane i fundusze hedgingowe jako inwestycje alternatywne rynku kapitałowego* [w:] H. Mamcarz, *Rynki finansowe*, Wyd. UMCS, Lublin, 2006, s. 146.

inwestycji alternatywnych jest odmiennosc tego typu inwestowania w stosunku do tradycyjnych sposobow pomnozania kapitału (rynek kapitałowy, obligacje, rynek pieniężny), biorąc pod uwagę nie tylko przedmiot inwestycji (np. metale szlachetne, nanotechnologie, kryptowaluty), ale również sposob inwestycji. W takim kontekście znaczeniowo postrzegany był rynek kryptoaktywów. Jednak wprowadzane regulacje prawne, rozwój infrastruktury, zapewnienie bezpieczenstwa cyberprzestrzeni oraz sposob wykorzystania kryptoaktywów, zmienia podejście do tego rynku zarówno indywidualnych, jak i instytucjonalnych uczestników obrotu, ale również regulowanego sektora bankowego i inwestycyjnego.

Przedmiotem niniejszego artykulu jest określenie miejsca rynku kryptoaktywów w systemie finansowym RP. W artykule wykorzystano metody teoretyczne związane z analizą dostępnych raportów, komunikatów, artykulów oraz zmieniającego się otoczenia prawnego, regulacyjnego i infrastrukturalnego rynku kryptoaktywów.

## KRYPTOAKTYWA

Rynek kryptoaktywów podlega oddziaływaniom prawnym i instytucjonalnym mającym na celu wzmozczenie bezpieczenstwa uczestników rynku, w tym pośredników obrotu, klienta, aktywów, czy realizowanej transakcji. Na rynek ten oddziałują również czynniki o charakterze politycznym, które wpływają m. in. na wartość poszczególnych aktywów w kontekście przyszłych, w tym potencjalnych planów regulacyjnych. Kryptoaktywa, zgodnie z rozporządzeniem regulującym ich emisję na terenie UE<sup>3</sup>, to cyfrowe odzwierciedlenie wartości lub prawa, które da się przenosić i przechowywać w formie elektronicznej z wykorzystaniem technologii rozproszonego rejestru lub podobnej technologii<sup>4</sup>.

Rynek kryptoaktywów, zgodnie z cytowaną regulacją obejmuje:

- tokeny powiazane z aktywami,
- tokeny będące pieniądzem elektronicznym,
- tokeny użytkowe<sup>5</sup>.

Według stanu na 12 września 2024 r., na giełdach notowanych było ok. 24 tysięcy kryptoaktywów o łącznej kapitalizacji ponad 2,1 biliona USD, przy czym Bitcoin i Ethereum miały ponad 70% udziału w rynku, oraz 794 miejsc wymiany kryptoaktywów. Natomiast według stanu na 4 stycznia 2025 r., na giełdach notowanych było ponad 24 tysiące kryptoaktywów o łącznej kapitalizacji już ponad 3,49 biliona USD, przy czym Bitcoin i Ethereum miały ok. 70% udziału w rynku, oraz 772 miejsc wymiany

---

<sup>3</sup> Art. 3 ust 1 pkt 5 rozporządzenia 2023/1114 w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz.U.UE.L.2023.150.40)

<sup>4</sup> Rozporządzenie (UE) nr 2023/1114; ang. Market in Crypto Assets Regulation.

<sup>5</sup> M. Wikarjak-Górzna, *MiCA – regulacja kryptoaktywów nadchodzi Parlament Europejski przeglosowal rozporządzenie w sprawie rynków kryptoaktywów*, <https://kpmg.com/pl/pl/blogs/home/posts/2023/05/mica-regulacja-kryptoaktywow-nadchodzi-blog-prawny.html> (dostęp: 20.11.2023).

kryptoaktywów<sup>6</sup>. Zwrócić należy jednak uwagę, że na giełdach kryptowalut notowanych jest faktycznie mniejsza ich ilość - ok. 2 tys. kryptowalut, a każdy z podmiotów pośredniczących w wymianie kryptoaktywów na walutę FIAT lub inne kryptoaktywo może notować innego rodzaju kryptoaktywa.

Wzrost wartości i wolumenu transakcji uwarunkowany jest również zwiększającą się ilością urządzeń służących do konwersji kryptowalut, a także zakupu lub wymiany tych cyfrowych aktywów, obsługi transakcyjnej poprzez popularne usługi finansowe, innowacyjne banki, czy kantory. Na terenie RP funkcjonuje co najmniej 280 bitomatów<sup>7</sup> (na dzień 3 maja 2023 roku było ich 249, 22 września 2022 roku były to 204 urządzenia, 3 marca 2022 roku funkcjonowało ich 105, natomiast w 2020 roku jedynie 67).

Kolejną kwestią jest zwiększający się poziom akceptowania płatności tym instrumentem oraz możliwość ich pożyczania, zamiany lub poręczania. Przy czym warto zwrócić uwagę na różne modele biznesowe prowadzonej działalności gospodarczej, takie jak wymiana kryptowalut na walutę FIAT lub inne kryptoaktywa, czy też działalność giełdową polegającą obrocie poszczególnymi kryptoaktywami. Istotnym elementem jest również możliwość transakcji pomiędzy łańcuchami blockchain (tzw. swapy), arbitrażu finansowego, gwarancji, czy też możliwość transakcji z wykorzystaniem karty płatniczej i kryptowalut.

Zgodnie z raportem Chainalysis, dotyczącym geograficznych aspektów kryptoaktywów<sup>8</sup> rysunek nr 1 obrazuje wartość obrotu kryptoaktywów w okresie między lipcem 2023 roku a czerwcem 2024 roku.

Tabela 1. Wartość obrotu rynku kryptoaktywów.

Region	% udziału obrotu	Wartość transakcji
Ameryka Północna	22,5	1,3 bln USD
Ameryka Łacińska	9,1	415 mld USD
Centralna, Północna i Zachodnia Europa	21,7	987,25 mld USD
Europa Wschodnia	11	499,14 mld USD
Centralna i Południowa Azja i Oceania	16,6	750 mld USD
Południowa Azja	8,9	400 mld USD
Południowo - wschodnia i Północna Afryka	7,5	338,7 mld USD
Afryka Subsaharyjska	2,7	125 mld USD

Źródło: opracowanie własne na podstawie: *The 2024 Geography of Crypto Report*.

<sup>6</sup> Coinmarketcap.com.

<sup>7</sup> Wartość podana wg stanu na dzień 4 marca 2024 zob. <https://coinatmradar.com/country/171/bitcoin-atm-poland/>.

<sup>8</sup> Chainalysis „The 2023 Geography of Cryptocurrency”.

Zgodnie z przywołanym raportem Chainalysis do największych rynków należą:

- rynek europejski – 32,7 % obrót światowego,
- rynek azjatycki – 25,5%
- rynek amerykański – 22,5 %.

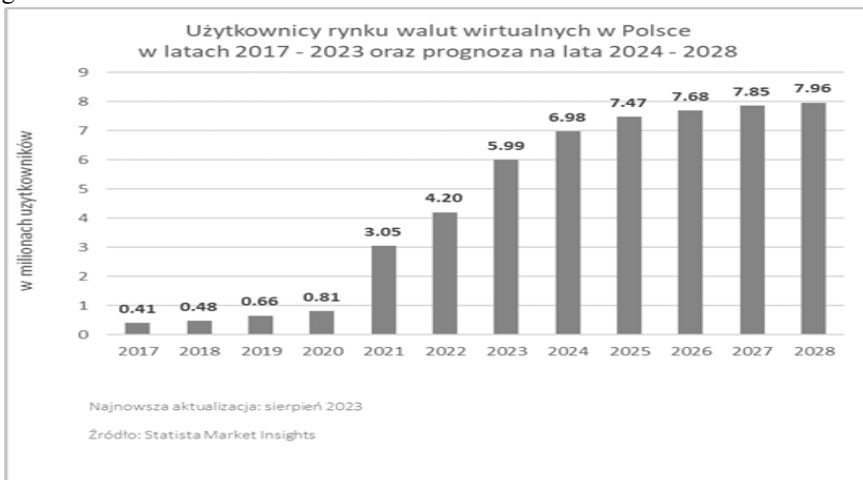
Warto wskazać na perspektywy rozwoju rynku kryptoaktywów, biorąc pod uwagę aspekt regulacyjny, stały wzrost zainteresowania nowymi technologiami, czy też eksplorowanie nowych obszarów inwestycyjnych. Przestrzenią do rozwoju tego obszaru rynku jest również fakt, że klienci poszukują tańszych i szybkich rozwiązań w zakresie transferu pieniądza elektronicznego, które są regulowane i nadzorowane, co powoduje bezpieczeństwo transakcji, uczestników obrotu, czy też samego aktywa.

Odpowiedzią na tak zdefiniowane potrzeby rynku są kryptoaktywa, które mogą być wykorzystane jako instrument o charakterze płatniczym, inwestycyjnym, czy też autoryzacyjnym. Stąd wzrost zainteresowania tym rynkiem.

W obszarze kryptoaktywów, możliwości wykorzystania przez uczestników obrotu brak jest cyklicznych badań ich aktywności przeprowadzonych przez pracownie statystyczne. Wskazując na użytkowników rynku należy posiłkować się badaniami podmiotów zewnętrznych zajmujących się analizą blockchain lub przeprowadzonych na potrzeby projektu ustawy i rynku kryptoaktywów.

Wykres nr 1 wskazuje na stały wzrost zainteresowania użytkowników obrotu kryptoaktywami w latach 2017-2023 oraz prognozę wzrostu w latach 2024-2028.

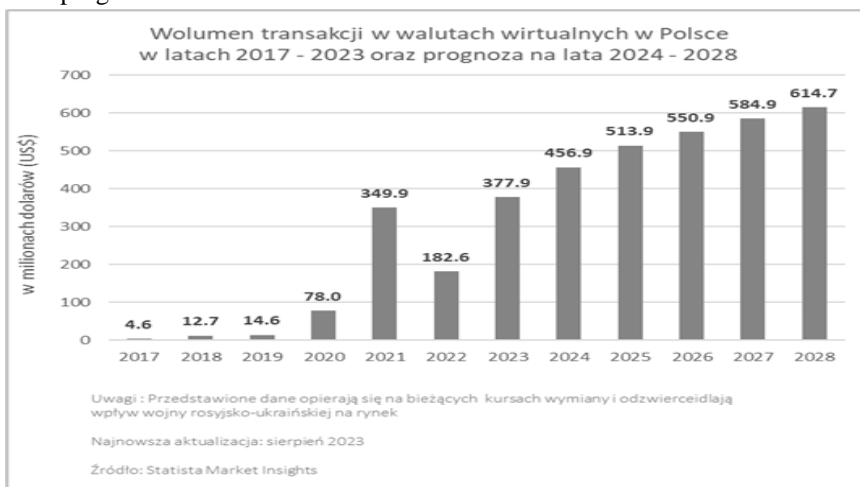
Wykres 1. Użytkownicy rynku walut wirtualnych w Polsce w latach 2017-2023 oraz prognoza na lata 2024 – 2028



Źródło: Statista Market Insight – ocena skutków regulacji projektu ustawy o rynku kryptoaktywów

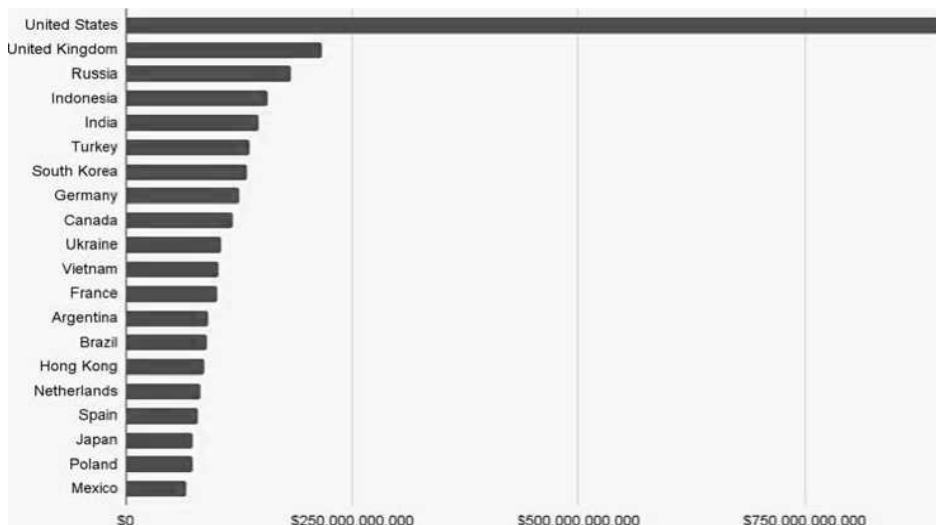
Na podstawie wykresu nr 2 można stwierdzić zwiększający się wolumen transakcji w walutach wirtualnych w latach 2017-2023 oraz prognozowanych na lata 2024-2028. Wykres ten potwierdza zainteresowanie ob. RP nowymi technologiami wykorzystywanymi w branży usług płatniczej i inwestycyjnej – tzw. FinTech. Ponadto istotne są również prognozy wskazujące na wzrostowy wolumen transakcji w walutach wirtualnych.

Wykres 2. Wolumen transakcji w walutach wirtualnych w Polsce w latach 2017-2023 oraz prognoza na lata 2024-2028



Źródło: Statista Market Insight - ocena skutków regulacji projektu ustawy o rynku kryptoaktywów

Zgodnie z raportem Chainalysis „The 2024 Geography of Cryptocurrency” do największych rynków kryptoaktywów na świecie należy rynek Stanów Zjednoczonych. Znaczenie to wynika w dużej mierze z zasobów finansowych obywateli tego państwa, dużej populacji, głębokich i płynnych rynków kapitałowych oraz ekosystemu innowacji. Stany Zjednoczone czerpią także korzyści z pozycji dolara wobec innych walut fiducjarnych.



Wykres 3. Kraje z największą wartością transferowanych kryptowalut  
 Źródło: Chainalysis, „The 2024 Geography of Cryptocurrency”

### CHARAKTERYSTYKA RYNKU FINANSOWEGO

Rynek finansowy to zespół kupujących i sprzedających walory finansowe, których decyzje kształtują popyt i podaż na te walory oraz ich cenę. Rynek oznacza zespół instytucji i mechanizmów za pomocą których te transakcje są realizowane<sup>9</sup>. Pojęcie to jest terminem złożonym i ewoluującym.

Rynek finansowy składa się z następujących elementów:

- rynek bankowy,
- rynek kapitałowy,
- rynek ubezpieczeniowy,
- rynek instytucji usług płatniczych,
- rynek instytucji pieniądza elektronicznego,
- rynek sektora kas spółdzielczych,
- rynek usług pożyczkowych.

Pewną wskazówką, w kontekście analizowania profesjonalnego rynku finansowego jest nadzór sprawowany nad poszczególnymi sektorami rynku przez Komisję Nadzoru Finansowego. Komisja Nadzoru Finansowego sprawuje nadzór nad sektorem bankowym, rynkiem kapitałowym, ubezpieczeniowym, emerytalnym, nad instytucjami płatniczymi i biurami usług płatniczych, instytucjami pieniądza elektronicznego, sektorem kas spółdzielczych oraz nad sektorem instytucji pożyczkowych<sup>10</sup>.

<sup>9</sup> Pod. red. Z. Krzyżkiewicz, Leksykon bankowo-giełdowy, Wyd. Warszawa, Poltex 2006, s. 404.

<sup>10</sup> [https://www.knf.gov.pl/o\\_nas/komisja](https://www.knf.gov.pl/o_nas/komisja) (dostęp. 18.02.2025).

Dodać należy, iż zakres sprawowanego nadzoru nad elementami rynku finansowego przez KNF rozwija się wraz z wprowadzanymi regulacjami prawnymi, czy identyfikacją nowych zagrożeń występujących na rynkach. Przekładem takiego rynku jest sprawowany od 1 stycznia 2024 r. nadzór nad działalnością instytucji pożyczkowych w zakresie udzielania kredytu konsumenckiego<sup>11</sup>.

Pewnymi charakterystycznymi elementami funkcjonowania profesjonalnego rynku finansowego są:

1. nadzór Komisji Nadzoru Finansowego,
2. regulacje w zakresie niekaralności członków zarządu, właścicieli,
3. obowiązki sprawozdawcze wobec KNF,
4. wymogi organizacyjne i kapitałowe,
5. cyberbezpieczeństwo świadczonych usług,
6. obowiązki w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu,
7. w zależności od zakresu świadczonych usług uzyskanie zgody na prowadzenie działalności, wpis do rejestru świadczonych usług.

Wskazane wyżej obostrzenia w zakresie bezpieczeństwa świadczonych usług, transparentności i rzetelności są charakterystyczne dla różnego rodzaju usług bankowych, ubezpieczeniowych, kapitałowych, czy występujących na rynku usług płatniczych.

Rynek kapitałowy jest miejscem realizacji transakcji instrumentami finansowymi lub innymi – alternatywnymi aktywami, przede wszystkim skupia się na wykorzystaniu wolnych środków, które przeznaczane są na cele związane z rozwojem działalności gospodarczej, modernizacji, czy innowacji.

Istotnym elementem realizacji transakcji na rynku jest kwestia ryzyka. Ryzyko to przedsięwzięcie, którego wynik jest nieznan, niepewny, oraz problematyczny. W przypadku inwestycji na rynku finansowym ryzyko może być kształtowane przez czynniki zewnętrzne i dotyczyć takich elementów jak inflacja, oddziaływanie polityczne, trendy gospodarcze oraz wewnętrzne, które mogą dotyczyć sytuacji w przedsiębiorstwie takich jak zadłużenie, stan kadr, projekty innowacyjne, czy stopień rozwoju infrastrukturalnego.

Elementami ryzyka na rynku finansowym są:

- zmienność wartości instrumentów finansowych na rynku,
- możliwość wystąpienia wpływu działalności przestępczej na cenę waloru,
- sytuacja polityczna, walutowa, gospodarcza państwa,
- czynniki zewnętrzne takie jak pandemia, konflikt zbrojny,
- ryzyko operacyjne i systemowe.

---

<sup>11</sup> Rozdział 5ab ustawy z dnia 12 maja 2011 roku o kredycie konsumenckim (t.j. Dz. U. z 2023 r. poz. 1028, ze zm.).

## MIEJSCE RYNKU KRYPTOAKTYWÓW W SYSTEMIE FINANSOWYM

Instytucje zaangażowane w rozwój rynku kryptoaktywów już od początku funkcjonowania tego rynku, jako istotny element jego stabilizacji, rozwoju, przejrzystości, czy też bezpieczeństwa transakcyjnego, zarówno podmiotów pośredniczących w obrocie, czy też klienta stawiały takie elementy jak bezpieczeństwo transakcji, transparentność, zabezpieczenia kapitałowe, czy inne.

Pierwszą z inicjatyw było stworzenie minimalnych standardów bezpieczeństwa giełd bitcoinowych opracowane już w 2014 r. w ramach Polskiego Stowarzyszenia Bitcoin oraz Instytutu Wiedzy i Innowacji Ministerstwa Finansów.

Celem tego dokumentu było zwiększenie zaufania społeczeństwa do kryptowalut, a w szczególności do giełd bitcoinowych, najpierw w Polsce, później w innych krajach.

Kolejną próbą było podjęcie przez Ministerstwo Cyfryzacji projektu „Od papierowej do cyfrowej Polski” - Strumień „Blockchain i kryptowaluty” Kanon dobrych praktyk podmiotów rynku kryptowalut (2017), wśród którego znalazły się takie zasady jak:

- zasady prowadzenia działalności gospodarczej,
- podmiot zarejestrowany na terenie RP,
- spółka prawa handlowego,
- depozyt – przeciętne dzienne obroty,
- prywatny fundusz gwarancyjny,
- reinwestycja zysków w bezpieczeństwo środków na giełdzie,
- szyfrowanie komunikowania się,
- współpraca z podmiotami władzy krajowej,
- wyodrębnianie działu bezpieczeństwa,
- bezpieczeństwo aktywów i transakcji,
- międzynarodowy podmiot gwarantujący aktywa.

Jednak regulacje prawne opisujące zasady prowadzenia działalności gospodarczej znalazły się dopiero w *ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*. Zgodnie z przedmiotową regulacją działalność w zakresie walut wirtualnych jest działalnością regulowaną w rozumieniu ustawy Prawo przedsiębiorców<sup>12</sup>, a warunkiem podjęcia działalności jest rejestracja<sup>13</sup>. Rejestr działalności w zakresie walut wirtualnych w Polsce prowadzi dyrektor Izby Administracji Skarbowej w Katowicach.

Z analizy rejestru wynika, że zarejestrowanych było odpowiednio:

- 1 006 podmiotów (na dzień 27.10.2023 r.),
- 1 272 podmiotów (na dzień 19.04.2024 r.),
- 1 841 podmiotów (na dzień 16.01.2025 r.).

---

<sup>12</sup> Ustawa z dnia 6 marca 2018 r. - Prawo przedsiębiorców (t.j. Dz. U. z 2024 r., poz. 236).

<sup>13</sup> Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124, 1723, 1843 i 1285).

Widoczne jest zwiększenie ilości podmiotów gospodarczych prowadzących działalność w zakresie walut wirtualnych, co w przyszłości może mieć wpływ na rozwój sektora usług płatniczych, bankowości elektronicznej, usług inwestycyjnych w kontekście synergii i rozwoju.

W związku z wejściem w życie przepisów rozporządzeń MiCA i TFR<sup>14</sup> oraz obowiązującą ustawą o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu istnieje sprzeczność w zakresie prowadzenia rejestru działalności w zakresie walut wirtualnych. W konsekwencji, w ocenie Dyrektora Izby Administracji Skarbowej w Katowicach, od 30 grudnia 2024 roku brak jest możliwości wpisu nowych podmiotów do Rejestru Działalności w zakresie Walut Wirtualnych<sup>15</sup>.

Jednak w 18-to miesięcznym okresie przejściowym, następującym po pełnej implementacji rozporządzenia MiCA, dotychczas zarejestrowane podmioty gospodarcze będą mogły prowadzić działalność gospodarczą.

Rozporządzenie MiCA wprowadza mechanizmy, które regulacyjni są zbliżone do znanych już rozwiązań rynku finansowego, w tym:

- instytucji zezwolenia na prowadzenie działalności w charakterze dostawcy usług w zakresie kryptoaktywów,
- wymogów kapitałowych w zakresie emisji wybranych kryptoaktywów,
- nadzoru nad rynkiem,
- nadzór nad kwestią emisji kryptoaktywów,
- wprowadzenie przestępstw polegających na ujawnieniu/wykorzystaniu informacji poufnej na rynku kryptoaktywów, manipulacji wartością,
- wprowadzenie przestępstwa prowadzenia działalności w zakresie kryptoaktywów, bez zezwolenia.

Warto również zasygnalizować inicjatywy KNF, Ministerstwa Finansów w kontekście objęcia regulacjami rynku kryptoaktywów ustawą o usługach płatniczych, a przede wszystkim poprzez takie instytucje, jak mała instytucja płatnicza.

Zgodnie z przepisami ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, podmioty działające na rynku kryptoaktywów (prowadzące działalność w zakresie pośrednictwa w wymianie kryptowaluty na waluty FIAT, lub inną kryptowalutę) realizują obowiązki w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, które polegają w szczególności na:

---

<sup>14</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849.

<sup>15</sup> Komunikat dotyczący rejestru działalności w zakresie walut wirtualnych, [https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach/zalatwianie-spraw/rejestr-dzialalnosci-w-zakresie-walut-wirtualnych/-/asset\\_publisher/R7Y1/content/komunikat-dotyczacy-rejestru-dzialalnosci-w-zakresie-walut-wirtualnych?redirect=https%3A%2F%2Fwww.slaskie.kas.gov.pl%2Fizba-administracji-skarbowej-w-katowicach%2Fzalatwianie-spraw%2Frejestr-dzialalnosci-w-zakresie-walut-wirtualnych%3Fp\\_p\\_id%3D101\\_INSTANCE\\_R7Y1%26p\\_p\\_lifecycle%3D0%26p\\_p\\_state%3Dnormal%26p\\_p\\_mode%3Dview%26p\\_p\\_col\\_id%3Dcolumn-2%26p\\_p\\_col\\_cunt%3D1#p\\_p\\_id\\_101\\_INSTANCE\\_R7Y1\\_](https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach/zalatwianie-spraw/rejestr-dzialalnosci-w-zakresie-walut-wirtualnych/-/asset_publisher/R7Y1/content/komunikat-dotyczacy-rejestru-dzialalnosci-w-zakresie-walut-wirtualnych?redirect=https%3A%2F%2Fwww.slaskie.kas.gov.pl%2Fizba-administracji-skarbowej-w-katowicach%2Fzalatwianie-spraw%2Frejestr-dzialalnosci-w-zakresie-walut-wirtualnych%3Fp_p_id%3D101_INSTANCE_R7Y1%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-2%26p_p_col_cunt%3D1#p_p_id_101_INSTANCE_R7Y1_)

- analizie ryzyka,
- typowaniu i rejestracji transakcji podejrzanych,
- stosowaniu środków bezpieczeństwa finansowego,
- rejestracji transakcji ponadprogowych, których równowartość przekracza 15.000 EURO / 10 000 EURO.

Do wskazanych środków bezpieczeństwa finansowego zalicza się:

- identyfikację klienta i weryfikację jego tożsamości,
- podejmowanie działań w celu identyfikacji beneficjenta rzeczywistego,
- charakter prowadzonych przez klienta stosunków gospodarczych,
- bieżące monitorowanie transakcji z klientem w zakresie jego zgodności z dotychczasową działalnością.

Przedmiotowe obowiązki w zakresie przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu są charakterystyczne dla innych obszarów rynku finansowego – kapitałowego, bankowego, usług płatniczych, ubezpieczeniowego czy inwestycyjnego. Realizowane obowiązki przez instytucje obowiązane w zakresie stosowania środków bezpieczeństwa finansowego również wskazuje rynek kryptoaktywów jako obszar sektora finansowego.

Warto zauważyć również, iż prowadzenie działalności w charakterze krajowej instytucji płatniczej albo krajowej instytucji pieniądza elektronicznego wymaga uzyskania, w wyniku procesu licencyjnego, zezwolenia KNF. Natomiast w przypadku małej instytucji płatniczej, biura usług płatniczych lub dostawcy świadczącego wyłącznie usługę dostępu do informacji o rachunku wymagany jest jedynie wpis do rejestru usług płatniczych i wydawców pieniądza elektronicznego<sup>16</sup>.

Kolejnym elementem przybliżającym rynek kryptoaktywów do rynku finansowego jest rozporządzenie UE w sprawie operacyjnej odporności cyfrowej sektora finansowego<sup>17</sup>, które dotyczy podniesienia poziomu cyberbezpieczeństwa oraz poziomu usług operacyjnych m. in. podmiotów udzielających kredytów, podmiotów świadczących usługi płatnicze, podmiotów świadczących usługi pieniądza elektronicznego, czy też podmiotów prowadzących działalność inwestycyjną. Wśród podmiotów, które będą musiały stosować przedmiotowe regulacje to również podmioty oferujące usługi związane z kryptoaktywami, emitenci kryptoaktywów, emitenci tokenów powiązanych z aktywami oraz emitenci znaczących tokenów powiązanych z aktywami.

W zakresie ryzyka związanego z rynkiem kryptoaktywów, dotychczasowe ostrzeżenia UKNF pozostają aktualne. Najbardziej charakterystyczne ryzyka to:

- bardzo wysoka zmienność wartości,

<sup>16</sup> Zakres usług płatniczych, [https://www.knf.gov.pl/dla\\_ryнку/procesy\\_licencyjne/platniczy/informacje\\_ogolne/zakres\\_uslug\\_platniczych](https://www.knf.gov.pl/dla_ryнку/procesy_licencyjne/platniczy/informacje_ogolne/zakres_uslug_platniczych) (dostęp: 23.01.2025).

<sup>17</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011.

- wysoce spekulatywny charakter spowodowany brakiem skutecznych i sprawdzonych metod wyceny,
- brak jednoznacznej i powszechnie akceptowalnej wartości ekonomicznej,
- ryzyko operacyjne utraty dostępu do własnych środków, związane z wczesną fazą rozwoju i wysokim skomplikowaniem wykorzystywanej technologii,
- wysokie ryzyko niepowodzenia przedsięwzięć biznesowych finansowanych za pomocą kryptoaktywów<sup>18</sup>.

Do powyższych form ryzyka należy również dodać:

- ryzyko wykorzystania kryptoaktywów do różnych form przestępczości, uwzględniając nowe rodzaje takie jak: ujawnienie/wykorzystania informacji poufnej, manipulacją instrumentami finansowymi,
- ryzyko występowania różnych obszarów regulacyjnych dot. kryptoaktywów;
- ryzyko braku nadzoru nad częścią rynku, która pozostanie poza regulacją projektowanej ustawy o rynku kryptoaktywów.

## WNIOSKI

Rynek kryptoaktywów, uwzględniając rozwój tego obszaru, specyfikę realizowanych transakcji, regulacje prawne w zakresie wymogów prowadzenia działalności gospodarczej, emisji cyfrowych aktywów, czy też nadzoru właściwych organów państwa, coraz bardziej jest utożsamiany z rynkiem finansowym.

Wartym odnotowania jest, że opisywane w przedmiotowym artykule regulacje (rozporządzenie MiCA, ustawa o rynku kryptoaktywów) dzielą rynek na segmenty:

- objęte regulacją, nadzorem nad emisją wybranych kryptoaktywów,
- funkcjonujące poza regulacją – tradycyjne kryptowaluty BTC, Ethereum,
- funkcjonujące poza regulacją, jednak zakres prowadzonej działalności zezwolenia na prowadzenie działalności w charakterze dostawcy usług w zakresie kryptoaktywów upoważni do:
  1. przechowywania kryptoaktywów i administrowania nimi,
  2. prowadzenie platformy obrotu kryptoaktywami,
  3. wymiana kryptoaktywów na środki pieniężne i inne kryptoaktywa,
  4. przyjmowanie, przekazywanie lub wykonywanie zleceń związanych z kryptoaktywami,
  5. plasowanie kryptoaktywów,
  6. doradztwo w zakresie kryptoaktywów,
  7. zarządzanie portfelem kryptoaktywów,
  8. transfer kryptoaktywów w imieniu klientów<sup>19</sup>.

<sup>18</sup> Tabela uwag KNF do projektu ustawy o rynku kryptoaktywów ( UC2 ), s. 41.

<sup>19</sup> <https://www.dlklegal.com/procesy/regulacje/licencjonowanie/licencjonowanie-finance-fintech/licencjonowanieart-casp-mica/> (dostęp: 23.01.2025).

Wchodzące, w coraz szerszym zakresie w życie regulacje UE - MiCA, jak również przygotowywany projekt ustawy o rynku kryptoaktywów wprowadzające instytucje zezwolenia na prowadzenie działalności w charakterze dostawcy usług w zakresie kryptoaktywów, wymogów dla prowadzenia działalności w zakresie emisji kryptoaktywów, nadzoru KNF, upodabnia ten rynek do mechanizmów znanych dotychczas rynkowi finansowemu.

Kolejnym aspektem potwierdzającym tą hipotezę jest powołanie w Urzędzie Komisji Nadzoru Finansowego Zespołu Nadzoru nad Rynkiem Kryptoaktywów<sup>20</sup>, co potwierdza znaczenie tych aktywów w kontekście bezpieczeństwa obrotu, czy też przenikania rynków bankowego, usług płatniczych, kapitałowego czy kryptoaktywów.

Podsumowując, rozważania na temat miejsca rynku kryptoaktywów w systemie finansowym RP należy stwierdzić, iż rynek kryptoaktywów, jego wartość, jak również poszczególnych kryptoaktywów kształtowany jest przez kupujących i sprzedających, prowadzoną działalność gospodarczą w zakresie kryptoaktywów, która jest licencjonowana, regulowana i podlega nadzorowi KNF. Natomiast decyzje w zakresie transakcji kształtują popyt i podaż na te instrumenty oraz ich cenę.

## **BIBLIOGRAFIA**

1. Chainalysis „The 2023 Geography of Cryptocurrency”.
2. Coinmarketcap.com.
3. Dębski W., Produkty strukturyzowane i fundusze hedgingowe jako inwestycje alternatywne rynku kapitałowego [w:] H. Mamcarz, Rynki finansowe, Wyd. UMCS, Lublin, 2006.
4. <https://coinatmradar.com/country/171/bitcoin-atm-poland/>.
5. <https://www.dlklegal.com/procesy/regulacje/licencjonowanie/licencjonowanie-finanse-fintech/licencjonowanieart-casp-mica/>.
6. [https://www.knf.gov.pl/o\\_nas/komisja](https://www.knf.gov.pl/o_nas/komisja) (dostęp. 18.02.2025).
7. Komunikat dotyczący rejestru działalności w zakresie walut wirtualnych, [https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach/zalatwianie-spraw/rejestr-dzialalnosci-w-zakresie-walut-wirtualnych/-/asset\\_publisher/R7Y1/content/komunikat-dotyczacy-rejestru-dzialalnosci-w-zakresie-walut-wirtualnych?redirect=https%3A%2F%2Fwww.slaskie.kas.gov.pl%2Fizba-administracji-skarbowej-w-katowicach%2Fzalatwianie-spraw%2Frejestr-dzialalnosci-w-zakresie-walut-wirtualnych%3Fp\\_p\\_id%3D101\\_INSTANCE\\_R7Y1%26p\\_p\\_lifecycle%3D0%26p\\_p\\_state%3Dnormal%26p\\_p\\_mode%3Dview%26p\\_p\\_col\\_id%3Dcolumn-2%26p\\_p\\_col\\_count%3D1#p\\_p\\_id\\_101\\_INSTANCE\\_R7Y1\\_](https://www.slaskie.kas.gov.pl/izba-administracji-skarbowej-w-katowicach/zalatwianie-spraw/rejestr-dzialalnosci-w-zakresie-walut-wirtualnych/-/asset_publisher/R7Y1/content/komunikat-dotyczacy-rejestru-dzialalnosci-w-zakresie-walut-wirtualnych?redirect=https%3A%2F%2Fwww.slaskie.kas.gov.pl%2Fizba-administracji-skarbowej-w-katowicach%2Fzalatwianie-spraw%2Frejestr-dzialalnosci-w-zakresie-walut-wirtualnych%3Fp_p_id%3D101_INSTANCE_R7Y1%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-2%26p_p_col_count%3D1#p_p_id_101_INSTANCE_R7Y1_).

---

<sup>20</sup> Na podstawie Zarządzenia nr 599 Prezesa Rady Ministrów z 23 listopada 2023 r. zmieniającego statut Urzędu Komisji Nadzoru Finansowego.

8. Krzyżkiewicz Z. red., Leksykon bankowo-gieldowy, Wyd. Warszawa, Poltex 2006.
9. Rozporządzenie 2023/1114 w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz.U.UE.L.2023.150.40).
10. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. w sprawie operacyjnej odporności cyfrowej sektora finansowego i zmieniające rozporządzenia (WE) nr 1060/2009, (UE) nr 648/2012, (UE) nr 600/2014, (UE) nr 909/2014 oraz (UE) 2016/1011 (Rozporządzenie DORA).
11. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849.
12. Tabela uwag KNF do projektu ustawy o rynku kryptoaktywów.
13. Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2023 r. poz. 1124, 1723, 1843 i 1285).
14. Ustawa z dnia 12 maja 2011 roku o kredycie konsumenckim (t.j. Dz. U. z 2023 r. poz. 1028, ze zm.).
15. Wikarjak-Górzna M., MiCA – regulacja kryptoaktywów nadchodzi Parlament Europejski przegłosował rozporządzenie w sprawie rynków kryptoaktywów, <https://kpmg.com/pl/pl/blogs/home/posts/2023/05/mica-regulacja-kryptoaktywow-nadchodzi-blog-prawny.html> (dostęp: 20.11.2023).
16. Zakres usług płatniczych, [https://www.knf.gov.pl/dla\\_ryнку/procesy\\_licencyjne/platniczy/informacje\\_ogolne/zakres\\_uslug\\_platniczych](https://www.knf.gov.pl/dla_ryнку/procesy_licencyjne/platniczy/informacje_ogolne/zakres_uslug_platniczych) (dostęp: 23.01.2025).
17. Zarządzenia nr 599 Prezesa Rady Ministrów z 23 listopada 2023 r. zmieniającego statut Urzędu Komisji Nadzoru Finansowego.

# ANALIZA BLOCKCHAIN – JAK ZROZUMIEĆ ELEKTRONICZNE PRZEPIŁYWY

## BLOCKCHAIN ANALYSIS – HOW TO UNDERSTAND ELECTRONIC FLOWS

**Tomasz PAWLICKI**<sup>1</sup>

**Streszczenie:** Opanowanie podstawowej wiedzy na temat, czym w istocie jest kryptowaluta, jak jest skonstruowana od wewnątrz oraz jakie narzędzia słuŹą do jej wymiany lub zamiany na pieniąŹ fiducjarny, jest kluczowe dla zrozumienia jej zarówno legalnych, jak i potencjalnie nielegalnych zastosowań. Choć kryptowaluty same w sobie nie są powiązane z działalnością przestępczą, bagatelizowanie moŹliwości ich niewłaściwego uŹycia z powodu braku zrozumienia technologii lub ignorancji ze strony organów ścigania stanowi istotne ryzyko. Artykuł przedstawia techniczne podstawy kryptowalut, podkreślając znaczenie świadomej analizy w celu lepszego wykrywania i przeciwdziałania moŹliwościom przestępczego wykorzystania w transakcjach cyfrowych.

**Słowa kluczowe:** analiza blockchain, kryptowaluta, wymiana na walutę fiducjarną, transakcje cyfrowe, nielegalne wykorzystanie kryptowalut, zapobieganie przestępstwom finansowym, technologia kryptowalut.

**Summary:** Mastering the fundamentals of what cryptocurrency truly is, its internal structure, and the tools used for its exchange or conversion into fiat currency is essential for understanding both its legitimate and potential illicit applications. While cryptocurrencies are not inherently linked to criminal activities, overlooking their misuse potential due to a lack of technological comprehension or investigative oversight poses a significant risk. This article explores the technical foundations of cryptocurrencies, highlighting the importance of informed scrutiny to better detect and mitigate opportunities for criminal exploitation within digital transactions.

**Keywords:** blockchain analysis, cryptocurrency, fiat currency exchange, digital transactions, illicit use of cryptocurrency, financial crime prevention, cryptocurrency technology.

---

<sup>1</sup> MON, Laboratorium Cyberbezpieczeństwa Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni, tomasz.pawlicky@gmail.com, ORCID: 0009-0005-2224-1301.

## WSTĘP

Blockchain to zdecentralizowany rejestr, który w kontekście kryptowalut stanowi bazę danych będącą zarówno bogatym źródłem informacji, jak i znaczącym wyzwaniem analitycznym. Istotną cechą większości blockchainów jest ich publiczny charakter, co umożliwia ich analizę przez użytkowników w dowolnym czasie i miejscu.

Jednak do efektywnej analizy niezbędna jest podstawowa wiedza oraz dostęp do specjalistycznych narzędzi - złożoność i liczba transakcji stanowią tu istotne wyzwanie.

Analiza blockchainu z perspektywy OSINT nie tylko pozwala lepiej zrozumieć mechanizmy działania tej technologii, ale także otwiera nowe możliwości w zakresie śledzenia i monitorowania aktywności w sieci, co jest kluczowe w dzisiejszym dynamicznie zmieniającym się środowisku cyfrowym.

Obecnie szacuje się, że istnieje około 22 000 różnych kryptowalut, jednak znaczna ich część pozostaje nieaktywna. Według szacunków, tylko około 9 000<sup>2</sup> z nich generuje rzeczywiste transakcje na blockchainie. Całkowita liczba kryptowalut zmienia się dynamicznie - część z nich powstaje wyłącznie w celach przestępczych (np. aby przyciągnąć inwestorów do bezwartościowego projektu), a inne nie osiągają wystarczającego poziomu zainteresowania. Tworzeniu nowych tokenów sprzyja relatywna prostota ich kreacji<sup>3</sup> - nie wymaga ona znajomości programowania, gdyż można wykorzystać gotowe rozwiązania<sup>4</sup>.

Aby sprawnie poruszać się po tym świecie, należy poznać podstawowe nazewnictwo:

1. **Coin** – cyfrowa waluta obsługiwana na własnym łańcuchu bloków (rejestrze), służąca głównie do płatności<sup>5</sup>. Przykładem jest Bitcoin (BTC).
2. **Altcoin** – (ang. alternative coin) oznacza dosłownie "alternatywną monetę" i określa każdą kryptowalutę inną niż Bitcoin. Zasady dotyczące altcoinów są zazwyczaj tożsame z tymi dla coinów. W tej grupie wyróżniamy m.in.:
  - a. **Stablecoin** – kryptowaluta powiązana wartościowo z innym, uznawanym za stabilny aktywem (np. dolarem amerykańskim)
  - b. **Memecoin** – kryptowaluta inspirowana żartami i memami

Istnieje wiele innych podgrup kryptowalut, których nazwy wywodzą się z ich funkcjonalności, technologii czy celu. Kolejną istotną kategorią są **tokeny** - aktywa oparte na blockchainie, które można swobodnie przenosić, sprzedawać lub przekazywać

---

<sup>2</sup> <https://coinweb.com/trends/how-many-cryptocurrencies-are-there/>

<sup>3</sup> Szerzej na ten temat zob.: Shailendra Bramhvanshi „How To Create Cryptocurrency Step By Step Guide” 2023, ISBN-13: 978-9359170411

<sup>4</sup> Platforma umożliwiająca stworzenie własnego tokena to np. <https://tokenmint.net/>

<sup>5</sup> W Polsce kryptowaluty nie mają statusu prawnego środka płatniczego, są jednak uznawane za wartości majątkowe, które podlegają regulacjom podatkowym i uregulowaniom dotyczącym w przeciwdziałaniu praniu pieniędzy. Zagłębiając się dokładnie w uregulowania prawne w Polsce można stwierdzić, iż poruszają się one w obszarze określenia czym kryptowaluty nie są. Na poziomie międzynarodowym nie istnieje jednolity system prawny dla tego rodzaju rozwiązań, ale wytyczne organizacji międzynarodowych wpływają na sposób, w jaki kraje regulują ten rozwijający się rynek.

między użytkownikami. W tradycyjnym prawie cywilnym odpowiada to zbywalności aktywów, czyli możliwości przeniesienia własności na inną osobę prawną lub fizyczną poprzez czynność prawną (sprzedaż, darowiznę czy zamianę). Tokeny zazwyczaj działają w ramach istniejącej sieci, która zapewnia im zaplecze technologiczne i funkcjonalność, eliminując konieczność tworzenia własnych rozwiązań. W przeciwieństwie do np. BTC, nie są one „wydobywane” [ang. mining], lecz „wybijane” [ang. minting]. Podstawowy podział tokenów obejmuje:

- **Tokeny podzielne** – reprezentacja wartości, którą można dzielić na mniejsze jednostki (np. BTC, który można podzielić do ośmiu miejsc po przecinku);
- **Tokeny niepodzielne**<sup>6</sup> – reprezentacja wartości niepodzielnej na mniejsze części.

Istotnym elementem ekosystemu blockchain są również **inteligentne kontrakty** (ang. smart contracts) - samowykonujące się programy przechowywane na blockchainie. Ich znaczenie polega na możliwości automatycznego egzekwowania zapisanych warunków umowy, co eliminuje potrzebę pośredników w transakcjach, potencjalnie zmniejszając koszty i zwiększając efektywność. Zrozumienie tych podziałów jest kluczowe dla analizy przepływów zachodzących w łańcuchach bloków i późniejszej analizy OSINT.

## TECHNICZNE ASPEKTY KONSTRUKCJI ADRESÓW

Rozpoznawanie adresów portfeli kryptowalutowych stanowi kluczowy element analizy blockchain z perspektywy informatyki śledczej. Adresy portfeli pełnią funkcję podstawowych identyfikatorów w sieciach blockchain, umożliwiając przesyłanie, odbieranie oraz przechowywanie kryptowalut. Każdy rodzaj kryptowaluty charakteryzuje się unikalnym formatem adresu, co pozwala na ich rozpoznanie i klasyfikację. Poniżej przedstawiono techniczne aspekty konstrukcji adresów dla najpopularniejszych kryptowalut.

*Bitcoin (BTC)* – nie można nie wspomnieć, iż jest to najstarsza kryptowaluta, która swoim początkiem sięga października 2008 roku gdzie osoba lub grupa osób pod pseudonimem "Satoshi Nakamoto" opublikowała whitepaper<sup>7</sup>, dokument zatytułowany "Bitcoin: A Peer-to-Peer Electronic Cash System"<sup>8</sup>. Ten początkowy dokument opisywał system cyfrowej waluty, który działał bez potrzeby istnienia centralnej bazy, wykorzystując zdecentralizowaną sieć węzłów (komputerów) oraz zaawansowaną kryptografię do zabezpieczania transakcji. Pierwszy blok BTC został wykopany 3 stycznia 2009 roku o godzinie 18:15:05 UTC. Zawierał on ukryty przekaz: "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks". Tekst ten odnosi się do

---

<sup>6</sup> NTF ang. Non-Fungible Tokens - są z definicji niepodzielne, ponieważ reprezentują unikalne przedmioty lub aktywa.

<sup>7</sup> Whitepaper (biała księga) dokument, który szczegółowo opisuje projekt, technologię, koncepcję lub innowację. W przypadku pojawienia się nowej kryptowaluty i chęci jej analizy zasadnym jest przestudiowanie jej białej księgi.

<sup>8</sup> <https://bitcoin.org/bitcoin.pdf>

nagłówka brytyjskiej gazety "The Times" z tego samego dnia, opisującego sytuację, w której rząd brytyjski rozważał dodatkowy pakiet ratunkowy dla banków w obliczu trwającego kryzysu finansowego.

Pierwsza transakcja BTC miała miejsce 22 maja 2010 roku o godzinie 18:16:31 UTC, rozpoczynając się od ogłoszenia na Bitcoin Forum<sup>9</sup>.

#### **Szczegóły transakcji<sup>10</sup>:**

- ID transakcji:  
a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d
- Strony transakcji:
  - Laszlo Hanyecz (1XPTgDRhN8RFnzniWCdobD9iKZatrVH4)
  - Jeremy Sturdivant "Jercos"  
(17SkEw2md5avVNyYgj6RiXuQKNwkXaxFyQ)

#### **Specyfikacja techniczna:**

##### **1. Format adresu:**

Rozpoczyna się od:

- "1" - Legacy/ P2PKH [ang. Pay-to-PubKeyHash];
- "3" P2SH[ang. Pay-to-Script-Hash];
- "Bc1" (Bech32<sup>11</sup> dla SegWit<sup>12</sup>).

##### **2. Algorytm hashujący:**

- a. SHA-256 i RIPEMD-160<sup>13</sup>
- b. Podwójne hashowanie klucza publicznego

##### **3. Suma kontrolna:**

- a. 4-bajtowa
- b. Tworzona przez podwójne hashowanie (SHA-256)
- c. Dodawana na końcu adresu dla wykrywania błędów

*Ethereum (ETH)* – koncepcja Ethereum została zaprezentowana w 2014 roku przez Vitalika Buterina, programistę wcześniej zaangażowanego w projekt Bitcoin. Ethereum było pierwszym blockchainem realizującym koncepcję smart kontraktów i tokenów w pełni funkcjonalnej, zdecentralizowanej platformie.

---

<sup>9</sup> <https://bitcointalk.org/index.php?topic=137.0>

<sup>10</sup> Rejestry publiczne służące do analizy: Blockchain: <https://blockchair.com>; Blockchain: <https://www.blockchain.com>; Wallet Explorer: <https://www.walletexplorer.com>

<sup>11</sup> Nowy format adresu dla BTC używa systemu kodowania zaprojektowanego w taki sposób, aby m.in. uniknąć problemów związanych z rozróżnianiem wielkich i małych liter.

<sup>12</sup> ang. Segregated Witness to aktualizacja protokołu Bitcoin, która została zaimplementowana w 2017 roku (bc1q) w pierwszej wersji, natomiast w 2012 roku została wprowadzona kolejna wersja (bc1p).

<sup>13</sup> ang. RACE (Research and Development in Advanced Communications Technologies in Europe) Integrity Primitives Evaluation Message Digest) to kryptograficzna funkcja skrótu, która generuje 160-bitowy (20-bajtowy) hasz z dowolnego ciągu danych wejściowych. RIPEMD-160 został opracowany w 1996 roku przez zespół akademicki na czele z Hansem Dobbertem oraz Bartem Preneel w ramach europejskiego projektu RACE.

## **Specyfikacja techniczna<sup>14</sup>**

1. **Format adresu:**
  - a. Rozpoczyna się od "0x"
  - b. Długość: 42 znaki
2. **Algorytm hashujący:**
  - a. Keccak-256 (często nazywany SHA-3)
3. **Konstrukcja:**
  - a. Generacja klucza: algorytm ECDSA [ang. Elliptic Curve Digital Signature Algorithm]<sup>15</sup> na krzywej secp256k1 [ang. Standards for Efficient Cryptography.]<sup>16</sup>
  - b. Hashowanie klucza publicznego: Keccak-256<sup>17</sup>
  - c. Adres: ostatnie 20 bajtów z wyniku hashowania

**Przykład:** 0xde0b295669a9fd93d5f28d9ec85e40f4cb697bae

*Monero (XMR)* – powstało na bazie protokołu kryptowaluty Bytecoin (2012), jednej z pierwszych kryptowalut skoncentrowanych na prywatności, wykorzystującej technologię CryptoNote<sup>18</sup>. W kwietniu 2014 roku grupa deweloperów zdecydowała o rozwidleniu kodu Bytecoina, tworząc BitMonero (później nazwę skrócono do Monero). Decyzja była związana z faktem wykopania 80% zasobów Bytecoina. Monero zyskało popularność zarówno wśród zwolenników prywatności, jak i w środowiskach przestępczych, co doprowadziło do zwiększonej kontroli ze strony organów ścigania oraz prób blokowania tej kryptowaluty przez niektóre giełdy.

## **Specyfikacja techniczna<sup>19</sup>**

1. **Format adresu:**
  - a. Rozpoczyna się od 4 lub 8
2. **Algorytm hashujący:**
  - a. CryptoNight
3. **Konstrukcja:**
  - a. Generacja kluczy: algorytm Ed25519 (public spend key i public view key)

---

<sup>14</sup> Rejestry publiczne służące do analizy: Etherscan: <https://etherscan.io/>; Ethplorer: <https://ethplorer.io/>; Blockchair: <https://blockchair.com/ethereum>; Etherchain: <https://www.etherchain.org/>

<sup>15</sup> Algorytm kryptograficzny oparty na krzywych eliptycznych, który służy do generowania podpisów cyfrowych

<sup>16</sup> 256 - oznacza w tym wypadku, iż długość klucza wynosi 256 bitów. k1 - oznacza specyficzną klasę krzywych eliptycznych o nazwie "Koblitz curves".

<sup>17</sup> Keccak to kryptograficzna funkcja skrótu będąca podstawą standardu SHA-3 (Secure Hash Algorithm) w rozpatrywanym kontekście 256 oznacza hasz o długości 256 bitów. Należy wspomnieć, iż Keccak-256 jest podobny do SHA-3-256, istnieją pewne różnice w parametrach, co sprawia, że wynikowe hasze są różne.

<sup>18</sup> opracowaną w 2013, która stanowi podstawę dla kryptowalut skoncentrowanych na prywatności. Szerzej na ten temat: "The Monero Standard: We're Not Here For The Income, We're Here For The Outcome" ISBN-10: 0645845116

<sup>19</sup> Rejestry publiczne służące do analizy: Monero Explorer: <https://xmchain.net/>; Blockchair: <https://blockchair.com/monero>; Monero Blocks: <https://moneroblocks.info/>

b. Hashowanie: CryptoNight

c. Kodowanie: Base58

**Przykład:** 44AFFq5kSiGBoZ... (adresy Monero są długie i mogą mieć różne formaty)

Konstrukcja adresów portfeli kryptowalutowych opiera się na zaawansowanych rozwiązaniach technologicznych, obejmujących: algorytmy hashujące, sumy kontrolne oraz metody kodowania. Każda kryptowaluta wykorzystuje unikalne podejście technologiczne, a jej kod jest stale rozwijany przez społeczność deweloperów. Działania te koncentrują się głównie na: zwiększaniu bezpieczeństwa transakcji, poprawie anonimowości użytkowników, optymalizacji wydajności sieci. W ostatnim czasie obserwuje się rosnące znaczenie kryptowalut zintegrowanych z popularnymi komunikatorami:

- MobileCoin w aplikacji Signal
- Próby implementacji Gram w Telegramie

Główne cele tych integracji to:

- połączenie szybkich i anonimowych transakcji z wygodą codziennej komunikacji
- umożliwienie przesyłania środków z łatwością porównywalną do wysyłania wiadomości
- zapewnienie użytkownikom dostępu do bezpiecznych i prywatnych transakcji finansowych w ramach znanego interfejsu

Poprawne przeprowadzenie analityki wymaga, przede wszystkim, zrozumienia technicznych aspektów kryptowalut, w tym:

- szczegółów konstrukcyjnych transakcji;
- specyfiki funkcjonowania poszczególnych walut;
- mechanizmów zabezpieczeń jest kluczowe dla skutecznej analizy blockchain w kontekście informatyki śledczej.

Przyszłe kierunki badań dla OSINT, czy też informatyki śledczej mogą koncentrować się na:

- rozwoju zaawansowanych metod rozpoznawania adresów portfeli;
- udoskonalaniu technik analizy transakcji;
- tworzeniu nowych narzędzi zwiększających przejrzystość ekosystemu kryptowalutowego;
- implementacji rozwiązań poprawiających bezpieczeństwo użytkowników.

Działania te mogą przyczynić się do zwiększenia ogólnego bezpieczeństwa i transparentności w środowisku kryptowalutowym, przy jednoczesnym zachowaniu prywatności użytkowników.

## TWORZENIE KLUCZA BTC

Proces tworzenia adresu portfela kryptowalutowego to szereg czynności kryptograficznych, które muszą zapewnić bezpieczeństwo przechowywanych danych i integralność z blockchainem. W celu stworzenia własnego klucza BTC można posłużyć się wieloma sposobami, których wybór zależy głównie od wiedzy użytkownika, wymaganego poziomu bezpieczeństwa oraz dostępu do narzędzi i oprogramowania. Do najczęstszych rozwiązań należą:

- Generator online (np. [bitaddress.org](http://bitaddress.org)) oferuje łatwe i natychmiastowe utworzenie portfela, dostępne dla każdego z przeglądarką internetową. Główną wadą jest potencjalne ryzyko bezpieczeństwa związane z zaufaniem do zewnętrznego serwisu, który może być podatny na ataki lub złośliwe działania.
- Portfel kryptowalutowy (np. Electrum<sup>20</sup>, Bitcoin Core, Mycelium) to zaufane oprogramowanie, często zintegrowane z dodatkowymi funkcjami bezpieczeństwa, takimi jak szyfrowanie portfela. Oferuje możliwość używania zarówno na komputerze, jak i urządzeniu mobilnym. Wymaga jednak korzystania z zabezpieczonego środowiska i zaufanego oprogramowania.
- Portfel sprzętowy (np. Trezor, Ledger) zapewnia najwyższy poziom bezpieczeństwa, generując klucze prywatne wewnątrz urządzenia i nigdy nie ujawniając ich na zewnątrz. Klucze są przechowywane w izolowanym środowisku, jednak wadą jest koszt zakupu urządzenia i zależność od zewnętrznego dostawcy sprzętu.
- Giełdy kryptowalutowe oferują dwa rodzaje rozwiązań: scentralizowane i zdecentralizowane. Giełdy scentralizowane są zwykle zakładane przez firmy podlegające jurysdykcji danego państwa, co wiąże się z koniecznością przejścia procesu KYC (Know Your Customer) przez klientów. Giełdy zdecentralizowane oferują większą anonimowość, ale mniejszą ochronę prawną.
- Programowy generator kluczy offline pozwala na tworzenie kluczy na odizolowanym komputerze, np. z bootowalnego systemu na nośniku USB. Jest to bardzo bezpieczne rozwiązanie, pod warunkiem że komputer jest odizolowany od sieci i wolny od złośliwego oprogramowania. Wymaga jednak wiedzy programistycznej i wiąże się z ryzykiem fizycznej utraty papierowego portfela.

Wybór odpowiedniej metody powinien uwzględniać kompromis między bezpieczeństwem a wygodą użytkownika, biorąc pod uwagę indywidualne potrzeby użytkownika, planowany sposób wykorzystania portfela oraz wartość przechowywanych środków. Analiza transakcji w sieciach kryptowalutowych przez informatyków śledczych będzie różnić się w zależności od używanej kryptowaluty/tokena, ponieważ każda z nich stosuje różne mechanizmy zabezpieczające prywatność, a to jednocześnie determinuje sposób postępowania, szczegółowa analiza pod tym kątem będzie opisana nieco później.

---

<sup>20</sup> Portfel umożliwia jeszcze instalację w trybie testnet, która umożliwia pozyskania i obrót wirtualnymi zasobami BTC

### *Tworzenie i dodawanie transakcji w sieciach kryptowalut*

Aby adres portfela został zarejestrowany na blockchainie, musi zostać użyty w transakcji, jest to podstawowy warunek niezbędny do „spożytkowania” krypto. Proces ten obejmuje tworzenie, podpisywanie i rozgłaszanie transakcji, a następnie jej włączenie do bloku przez górników lub inne mechanizmy konsensusu, w zależności od kryptowaluty. Należy pamiętać, że bezpośrednio z zimnego portfela (cold wallet) nie można np. wykonać transakcji zakupu usługi online. Pomimo tego, iż jest to jeden z najbezpieczniejszych sposobów przechowywania kryptowalut, to jednak niesie za sobą dosyć długi czas reakcji. Cały proces „wejścia” zasobów z powrotem do sieci i możliwość działania może potrwać nawet parę godzin. Natomiast w przypadku portfela gorącego sam proces reakcji może być zainicjowany bez udziału człowieka. Aby to zrobić należy przetransferować środki do portfela, który ma aktywny dostęp do sieci blockchain. Natomiast wypłata środków, np. poprzez bitomat, jest możliwa nawet z zimnego portfela, po uprzednim przeniesieniu środków.

Oto szczegółowy opis procesu wprowadzania pierwszej transakcji z „punktu widzenia” blockchain-a:

- a. **Tworzenie transakcji** Generowanie danych transakcyjnych, w tym określenie wejść (inputów) i wyjść (outputów) dla Bitcoin i Monero, lub adresów nadawcy i odbiorcy dla Ethereum i XRP.
- b. **Podpisanie transakcji** Użycie klucza prywatnego do podpisania transakcji, co potwierdza autentyczność i uprawnia do wydania środków.
- c. **Rozgłoszenie transakcji** Przesłanie transakcji do sieci blockchain, gdzie jest ona propagowana przez węzły.
- d. **Włączenie do bloku** Transakcja zostaje włączona do bloku przez górników (w przypadku Proof-of-Work) lub inne mechanizmy konsensusu, takie jak Proof-of-Stake czy mechanizm konsensusu Ripple.

Każda z kryptowalut ma swoje unikalne cechy, ale podstawowy proces wprowadzenia transakcji na blockchain pozostaje w dużej mierze podobny.

### *Przekształcanie kryptowalut na waluty fiducjarne*

W niniejszym podrozdziale omówione zostaną metody przekształcania kryptowalut na waluty fiducjarne (fiat), takie jak złotówka (PLN), euro (EUR), dolar amerykański (USD), rubel (RUB) oraz hrywna (UAH). Proces ten jest nieodzownym elementem w analizie przepływu środków pochodzących z przestępstw finansowych z wykorzystaniem kryptowalut. Przedstawiono tutaj szczegółowe informacje na temat dostępnych metod i narzędzi, z uwzględnieniem perspektywy użytkownika, aby lepiej zrozumieć praktyczne aspekty korzystania z poszczególnych usług.

## **Giełdy kryptowalutowe**

Giełdy kryptowalutowe (scentralizowane giełdy)<sup>21</sup> są najczęściej wybieraną opcją do zamiany kryptowalut na waluty fiducyjne. Umożliwiają one użytkownikom deponowanie kryptowalut, ich wymianę na fiat oraz wypłatę środków na konto bankowe. Giełdy te oferują różnorodne pary handlowe, umożliwiając wymianę na PLN, EUR, USD, RUB.

### **Jak to wygląda od strony użytkownika**

Użytkownik najpierw musi zarejestrować się na giełdzie i przejść proces weryfikacji tożsamości Know Your Customer<sup>22</sup>. Po weryfikacji, użytkownik deponuje kryptowaluty na swoim koncie giełdowym. Następnie kryptowaluty są wymieniane na wybraną walutę fiat, np. PLN, EUR, USD, RUB czy UAH. Środki fiat mogą być wypłacone na powiązane konto bankowe. Oczywiście taki proces zostawia widoczny ślad na rachunku bankowym. Niemniej jednak cały proces jest stosunkowo prosty, ale całkowicie podporządkowany regulacjom prawnym danego państwa. Może on różnić się w zależności od giełdy kryptowalutowej i jej polityk, ale powyższe kroki i wymagania są typowe dla większości platform. Należy wspomnieć również, iż w zależności od stopnia weryfikacji determinowana będzie funkcjonalność serwisu, np. możliwość wpłat/wypłat bądź ich wielkość.

Zdecentralizowane giełdy (DEX-y)<sup>23</sup> to platformy, które umożliwiają handel kryptowalutami bez pośrednictwa centralnej jednostki zarządzającej. W przeciwieństwie do giełd centralizowanych (CEX-ów), DEX-y działają w oparciu o inteligentne kontrakty (ten temat zostanie poruszony w dalszej części pracy), które automatyzują transakcje w taki sposób, iż nie uczestniczy w nich trzecia strona. To rozwiązanie powoduje, iż użytkownicy mogą przeprowadzać transakcje bez potrzeby rejestracji lub weryfikacji tożsamości (KYC).

Jednakże, DEX-y nie oferują bezpośredniej możliwości tworzenia par transakcyjnych z walutami typu fiat. Dlatego też najpierw muszą je wymienić na stablecoiny (np. USDT, USDC) lub inne kryptowaluty, które następnie mogą być

---

<sup>21</sup> Popularne giełdy to: Zonda – wypłata m.in. w PLN; Kraken – wypłata m.in. w EUR; Coinbase – wypłata m.in. w USD; EXMO – wypłata m.in. w RUB; OKX – wypłata m.in. w RUB, PLN, USD, EUR  
Zdecentralizowane giełdy (DEX-y)

<sup>22</sup> Generalnie regulacje te wprowadzane są za pośrednictwem dyrektyw Unii Europejskiej dotyczących przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu (Anti-Money Laundering/Combating the Financing of Terrorism, AML/CFT), takich jak piąta Dyrektywa Unii Europejskiej w sprawie przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu (5th Anti-Money Laundering Directive, AMLD5), które są implementowane na poziomie krajowym w Polsce poprzez odpowiednie ustawy i rozporządzenia. Dodatkowo, globalne standardy ustalane przez organizacje międzynarodowe, takie jak Financial Action Task Force (FATF), Financial Crimes Enforcement Network w Stanach Zjednoczonych (FinCEN) oraz inne krajowe organy nadzoru finansowego, wymagają stosowania procedur Know Your Customer (Poznaj Swojego Klienta, KYC) w celu zapewnienia zgodności z przepisami oraz ochrony przed nadużyciami finansowymi.

<sup>23</sup> Przykłady popularnych DEX-ów: Uniswap: <https://uniswap.org>; SushiSwap: <https://sushi.com>; PancakeSwap: <https://pancakeswap.finance>

przesłane na giełdę scentralizowaną lub platformę pośredniczącą<sup>24</sup>, umożliwiającą konwersję na fiat.

### **Platformy typu peer-to-peer (P2P)**

Platformy P2P umożliwiają bezpośrednią wymianę kryptowalut między użytkownikami na lokalne waluty fiducjarne, często z mniejszą kontrolą regulacyjną niż giełdy centralizowane. Umożliwiają one wymianę na PLN, EUR, USD, RUB oraz UAH przy użyciu różnorodnych metod płatności.

#### **Jak to wygląda od strony użytkownika**

Użytkownik rejestruje się na platformie P2P i przegląda dostępne oferty wymiany kryptowalut na fiat, takie jak PLN, EUR, USD, RUB czy UAH. Po znalezieniu odpowiedniej oferty, użytkownik może przeprowadzić transakcję, ustalając warunki bezpośrednio z drugim użytkownikiem. Płatności są realizowane przez różne kanały, w tym przelewy bankowe, gotówkę, PayPal oraz Western Union. Proces wymaga ostrożności, aby uniknąć oszustw, ale oferuje większą prywatność niż centralizowane giełdy.

Popularne platformy P2P:

- **Paxful<sup>25</sup>:**

Paxful oferuje szeroki wybór opcji płatności dla różnych walut, w tym PLN, EUR, USD, RUB i UAH. Użytkownicy mogą wymieniać kryptowaluty bezpośrednio z innymi użytkownikami, korzystając z lokalnych metod płatności, takich jak przelewy bankowe i karty przedpłacone.

- **Hodl Hodl<sup>26</sup>:**

Hodl Hodl to kolejna platforma P2P, która umożliwia użytkownikom handel kryptowalutami bez konieczności przechodzenia pełnej weryfikacji KYC.

- **Binance P2P<sup>27</sup>:**

Binance P2P, część ekosystemu Binance, oferuje wymianę kryptowalut na fiat z użyciem różnych metod płatności i szerokiego zasięgu globalnego.

---

<sup>24</sup> W praktyce udział platformy pośredniczącej np.,: <https://changenow.io>, umożliwiającej przesyłanie kryptowalut z jednego portfela na inny powoduje problemy w identyfikacji poszczególnych zapisów w blockchain.

<sup>25</sup> <https://paxful.com>

<sup>26</sup> <https://hodlhodl.com>

<sup>27</sup> <https://p2p.binance.com>

The screenshot shows the Paxful website interface. At the top, there's a navigation bar with options like 'Kup', 'Sprzedaj', 'Utwórz ofertę', 'Portfel', 'Gift Card Hub', 'Zostań sprzedawcą', 'Zaloguj się', and 'Zarejestruj się'. Below this is a banner for gift cards. The main content area is titled 'Sprzedać tether i wypłacić środki przy użyciu metody Western Union'. On the left, there's a sidebar with filters for 'Tether', 'Western Union', 'Dowolna kwota', 'Lokalizacja oferty', and 'Lokalizacja właściciela oferty'. The main area displays a grid of payment methods: 'Przelewy bankowe', 'Portfele online', 'Karty debetowe/kredytowe', 'Karty подарunkowe', 'Waluty cyfrowe', 'Płatności gotówkowe', 'Towary i usługi', and 'Mobile Money'. A 'Take Tour' button is also present. Below the grid, a detailed view for 'Western Union' is shown, including the seller's name 'LegitDawny', a verified status, and a price of 3.68 PLN with a 5% discount. It also shows 'Min sale: 42 PLN' and 'Max sale: 195 000 PLN'.

Rys. 1. Przykładowe wyszukiwanie kontrahenta który oferują wymianę TRX na PLN przy wypłacie Western Union.

Źródło: opracowanie własne na podstawie <https://paxful.com/>

## Bitomaty (ATM kryptowalutowe)

Bitomaty to urządzenia umożliwiające natychmiastową wymianę kryptowalut na gotówkę i odwrotnie w lokalnych walutach, takich jak PLN, EUR, USD, RUB i UAH. Są one powszechnie dostępne w większych miastach i umożliwiają szybki dostęp do gotówki.

### Jak to wygląda od strony użytkownika

Użytkownik lokalizuje najbliższy bitomat za pomocą serwisu internetowego, np. CoinATMRadar<sup>28</sup>. Informacje zawarte na stronie pozwalają nam również sprawdzić opłatę za wpłatę/wypłatę środków, godziny otwarcia, dostępne „waluty” oraz limity transakcyjne np.: „Weryfikacja dokumentu jest wymagana powyżej kwoty 1 000 EUR dla jednej transakcji (lub 15 000 EUR dla wielu transakcji w ciągu jednego dnia)”.

Po znalezieniu bitomatu użytkownik wprowadza kwotę do wymiany i skanuje kod QR, wysyłając kryptowaluty na adres bitomatu.

Po potwierdzeniu transakcji przez sieć blockchain, bitomat wydaje gotówkę w wybranej walucie fiat. Cały proces jest dosyć szybki i wygodny, choć zwykle wiąże się z wyższymi opłatami niż inne metody wymiany.

## Usługi pośredniczące w przekształceniu kryptowalut

Usługi pośredniczące, takie jak Zen czy Wirex, pełnią rolę mostu między kryptowalutami, a tradycyjnymi metodami płatności, umożliwiając użytkownikom

<sup>28</sup> <https://coinatmradar.co>

wymianę kryptowalut na fiat i korzystanie z kart płatniczych do wypłat gotówki w lokalnych walutach.

### **Jak to wygląda od strony użytkownika**

Użytkownik rejestruje się w aplikacji, takiej jak Zen czy Wirex, i zasila konto kryptowalutą.

Kryptowaluty mogą być wymienione na fiat w aplikacji, a środki te można następnie wykorzystać do płatności kartą lub wypłaty gotówki z bankomatów.

Revolut nie umożliwia bezpośrednich transferów kryptowalut z zewnętrznych źródeł, ale inne usługi, takie jak Wirex, oferują pełną integrację z blockchainem, pozwalając na wpłaty i wypłaty w różnych walutach fiat.

### **Popularne usługi pośredniczące:**

- **Zen<sup>29</sup>:**

Zen umożliwia wymianę kryptowalut na PLN, EUR oraz inne waluty z możliwością wypłaty na konta bankowe w Polsce i strefie euro. Użytkownicy mogą również korzystać z kart płatniczych Zen, które umożliwiają wydawanie środków w lokalnych walutach.

- **Wirex<sup>30</sup>:**

Wirex oferuje możliwość wymiany kryptowalut na fiat i korzystanie z kart płatniczych Wirex do wypłaty gotówki z bankomatów w PLN, EUR, USD, RUB oraz UAH.

### **Tradycyjne metody transferu pieniężnego (Western Union, MoneyGram)**

Tradycyjne usługi transferu pieniężnego, takie jak Western Union i MoneyGram, mogą być wykorzystywane do wypłacania środków po wymianie kryptowalut na fiat, umożliwiając odbiór gotówki w lokalnych walutach.

### **Jak to wygląda od strony użytkownika:**

Użytkownik najpierw sprzedaje kryptowaluty na platformie P2P, która oferuje opcję wypłaty przez Western Union lub MoneyGram. Po dokonaniu sprzedaży, środki fiat są przesyłane na wybraną placówkę, gdzie użytkownik może je odebrać w gotówce, przedstawiając dokument tożsamości. Proces ten jest przydatny dla osób, które preferują tradycyjne metody wypłaty gotówki, ale może wiązać się z dodatkowymi opłatami za transfer.

### **Popularne usługi transferu pieniężnego:**

- **Western Union<sup>31</sup>:**

---

<sup>29</sup> <https://www.zen.com>

<sup>30</sup> <https://wirexapp.com>

<sup>31</sup> <https://www.westernunion.com>

Western Union oferuje możliwość przesyłania środków fiat, które mogą być odebrane w placówkach w formie gotówki w lokalnej walucie, w tym PLN, EUR, USD, RUB i UAH.

- **MoneyGram<sup>32</sup>:**

MoneyGram umożliwia podobne operacje, oferując szybkie przelewy gotówki w lokalnych walutach po wymianie kryptowalut na fiat.

### **Mobilne kantory i bankomaty**

Mobilne kantory oferują elastyczność w przekształcaniu kryptowalut na lokalne waluty fiducjarne z wypłatą gotówki na miejscu, co jest szczególnie wygodne w sytuacjach, gdy użytkownik potrzebuje szybkiej wymiany, a jednocześnie wiąże się z trudnościami w ujawnieniu ewentualnego użytkownika, który z nich korzysta.

Przekształcanie kryptowalut na waluty fiducjarne, takie jak złotówka, euro, dolar, rubel czy hrywna, jest procesem, który może przebiegać na wiele różnych sposobów, w zależności od wybranej metody i dostępnych narzędzi. Użytkownicy mają do wyboru zarówno giełdy kryptowalutowe, platformy P2P, bitomaty, jak i usługi pośredniczące. Każda z tych metod ma swoje zalety i wady, a wybór odpowiedniego rozwiązania zależy od indywidualnych potrzeb, lokalizacji użytkownika oraz specyfiki przestępczego procederu, który jest przedmiotem śledztwa.

#### **Jak to wygląda od strony użytkownika:**

Użytkownik zamawia usługę mobilnego kantoru za pośrednictwem strony internetowej lub aplikacji. Operator mobilnego kantoru przyjeżdża na wskazane miejsce i dokonuje wymiany kryptowalut na gotówkę w lokalnej walucie. Cały proces odbywa się bez konieczności korzystania z tradycyjnych placówek finansowych, co może być wygodne, ale zwykle wiąże się z wyższymi opłatami za usługę.

## **ŚLEDZTWO CYFROWE**

Kolejnym punktem wyjścia do rozpoczęcia śledztwa i zbierania informacji na temat „celu”, a także do rozpoczęcia procesu analitycznego, będą trzy kluczowe elementy, które determinują początek, od którego możemy zacząć.

- Użytkownik – w tym kontekście często bywa anonimowy kryjący się za pseudonimami, które tak naprawdę bardzo trudno powiązać z rzeczywistym imieniem i nazwiskiem bądź nazwą firmy (a to przecież jeszcze nie daje nam gwarancji odnalezienia tej właściwej osoby). Techniki identyfikacji i przypisania użytkownika do danego portfela często będą obejmować szeroko zakrojone analizy takie jak:
  - o Wzorce transakcji - analiza historii transakcji danego adresu może ujawnić powtarzające się wzorce, np. w kontekście częstotliwości dokonywanych transakcji, preferowanych pór dnia, a nawet geolokalizację przybliżoną na

---

<sup>32</sup> <https://www.moneygram.com>

podstawie czasu transakcji. Oczywiście użytkownik może stosować różnego rodzaju techniki maskujące związane np.: z użyciem innej strefy czasowej, VPN, proxy, niemniej jednak te elementy należy uznać za istotne w kontekście całego dochodzenia. Klasteryzacja adresów<sup>33</sup> i analiza przepływów środków mogą prowadzić do powiązania wielu adresów z jednym użytkownikiem.

- o Monitorowanie wycieków danych – nie od dziś wiadomo, że wszystkie dane niosące za sobą informacje takie jak adresy e-mail, nazwy użytkowników czy informacje o kontaktach na giełdach, stanowią łąkowy kąsek dla cyberprzestępców. Dlatego też wszystkie zbiory takich informacji np. zapisane w bazach danych giełd scentralizowanych będą stanowiły wyśmienity cel. Z kolei dla analityka będzie to ogromna skarbnica wiedzy która, być może przybliży go do przypisania konkretnej transakcji/portfela do użytkownika, a w konsekwencji do osoby.
- o Analiza komunikacji w sieciach społecznościowych – wszyscy lubimy się chwalić naszymi zasobami lub ktoś pisze o “nas” podając klucze do naszych zasobów. W celach analitycznych warto prześledzić takie informacje a następnie przeanalizować z jakimi innymi portfelami miał kontakt nasz “obiekt” i jakie transakcje były przeprowadzane. Przez analizę tych właśnie aktywności, często języka, którym posługuje się użytkownik oraz połączeń między różnymi profilami można zidentyfikować kluczowe informacje i wykorzystać je w kolejnych etapach analizy.

W celu przeszukiwania dostępnych informacji na temat użytkownika, ewentualnych powiązanych z nim adresów lub wzmiankach na forach, możemy posłużyć się stroną Bitcoin Whose Who<sup>34</sup>. Innym sposobem jest wykorzystanie narzędzi takich jak Maltego oraz już bardziej zaawansowany CobWebs<sup>35</sup>.

W moim przekonaniu do elity oprogramowania do analizy łańcuchów w blokach różnych kryptowalut należy jednak: Chainalysis<sup>36</sup> i TRM Labs<sup>37</sup>. Programy te umożliwiają mapowanie sieci w taki sposób, iż nie tylko wychwytyją połączenia między portfelami, giełdami ale również informacje o użytkownikach.

- o Współpraca z giełdami - giełdy kryptowalutowe, które wymagają weryfikacji tożsamości (KYC), mogą posiadać cenne dane osobowe użytkowników. W ramach prowadzonych czynności przez uprawniony organ można wystąpić

---

<sup>33</sup> Klasteryzacja adresów w naszym przypadku będzie techniką stosowaną do grupowania różnych adresów blockchain, które prawdopodobnie należą do tego samego użytkownika lub podmiotu.

<sup>34</sup> <https://www.bitcoinwhoswho.com/>

<sup>35</sup> <https://cobwebs.com/en/government-national-security/>

<sup>36</sup> <https://www.chainalysis.com/>

<sup>37</sup> <https://www.trmlabs.com/> - w portfolio firmy są również szkolenia, które można wykupić bez posiadania programu.

- o udostępnienie tych danych, co może prowadzić do bezpośredniego powiązania adresu portfela z rzeczywistą osobą.
- Portfel kryptowalutowy – to kluczowy element wiedzy do którego dążymy. Wiedza o nim może posłużyć nam do dalszej analizy samych przepływów środków, powiązania z giełdami a co za tym idzie pieniądzem fiducjarnym, a tym samym przejściem do „tradycyjnych” metod wykrywczych opierających się ma „money flow”.

Analiza transakcji bez jakiegokolwiek oprogramowania jest bardzo trudna. Bez wątplenia na początku należy obyc się z samym „wyglądem” blockchain-ów oraz adresami, to już duży krok do przodu. Na warsztat weźmy poniższy adres:

1MjKKhWBGez6z5SjomZ94417duwVyMxFC

W pierwszej kolejności należy wpisać go do wybranego eksploratora bloków, sądzę, że w pierwszych krokach dobrym pomysłem jest porównywanie kilku, tak aby sprawdzić jaki nam odpowiada najbardziej.

(C:\Users\wejdz na stronę >)  
<https://explorer.btc.com/>

Address

1MjKKhWBGez6z5SjomZ94417duwVyMxFC + Monitor

Summary

Format	P2PKH	Total Received	0.00045627 BTC
Balance	0 BTC	Total Sent	0.00045627 BTC
Balance Value	\$ 0	Txn Count	2
Other Explorers			<span>BLOCKCHAIR</span>

Transactions (2) Filter: All Sort: Time Export Batch Accelerate

3ad3d14fb31480327c567c62340393f21853413e5842fa1b2bc650af48e4c5bf	817,240	74 Satoshis/vByte	Fee:0.00013854 BTC	2023-11-18 00:48:36
Input (1)	0.00045627 BTC	→	Output (1)	0.00031773 BTC
1MjKKhWBGez6z5SjomZ94417duwVyMxFC	0.00045627		bc1qykh4tc0d1eu0gces8...rxx02e7eyd75vz9q26vt	0.00031773
				-0.00045627
				40,200 Confirmations
4debaa7f3b078920e1037bd71b9978c0c435b33c2e912e5ef186289440ba32db	816,632	76 Satoshis/vByte	Fee:0.00019692 BTC	2023-11-13 20:32:35
Input (2)	0.01058606 BTC	→	Output (2)	0.01038914 BTC
36aJggnT67YkcrH1t6YnEztRyRVqm2EPP	0.00048901		3DKv64SHYrGZASmJgdRbeRjMDnq7EYJ54d	0.00993287
32oQA3Y59XAWStMjt08B88Ab3R1tqoJSAQ	0.01009705		1MjKKhWBGez6z5SjomZ94417duwVyMxFC	0.00045627
				+0.00045627
				40,808 Confirmations

Rys. 2. Analiza portfela kryptowalutowego.

Źródło: opracowanie własne na podstawie: <https://explorer.btc.com>

Analiza transakcji widocznych na załączonym zrzucie ekranu (Rys. 2). Przede wszystkim widzimy, że adres 1MjKKhhWBGez6z5SjomZ94417duwVyMxFC ma dwie transakcje.

Transakcja 2

Transakcja

ID:

3ad3d14fb31480327c567c62340393f21853413e5842fa1b2bc650af48e4c5bf

Data i godzina: 2023-11-18 00:48:36

Kwota wejściowa: 0.00045627 BTC

Kwota wyjściowa: 0.00031773 BTC

Opłata transakcyjna<sup>38</sup>: 0.00013854 BTC (około 30.36% wartości transakcji)

Adres docelowy: bc1qykh4t0dleu0gces8mdrxx02e7eyd75vz9q26vt

Liczba wyjść (outputs): 1

W transakcji tej jest widoczny jest tylko jeden wyjściowy adres (output), co bezpośrednio oznacza, że cała kwota po odjęciu opłaty transakcyjnej została przelana na adres bc1qykh4t0dleu0gces8mdrxx02e7eyd75vz9q26vt. Należy uwzględnić, iż w Bitcoinie opłata transakcyjna nie jest wyrażona jako oddzielne wyjście. Opłata transakcyjna jest zawsze różnicą między wejściem, a sumą wszystkich wyjść w transakcji. Zatem przebieg transakcji wygląda następująco:

- **Wejście (input):** 0.00045627 BTC (kwota, która pochodziła z wcześniejszej transakcji i została wykorzystana jako źródło funduszy w tej transakcji).
- **Wyjście (output):** 0.00031773 BTC - cała kwota wejściowa po odjęciu opłaty transakcyjnej została przesłana na ten jeden adres bc1qykh4t0dleu0gces8mdrxx02e7eyd75vz9q26vt.

Zatrzymajmy się na chwilę, aby przeanalizować możliwe przypadki działania użytkownika oraz ewentualne scenariusze tej transakcji.

- **Przelew całej kwoty na jeden adres:**

Cała dostępna kwota po odjęciu opłaty transakcyjnej została przelana na jeden adres (bc1qykh4t0dleu0gces8mdrxx02e7eyd75vz9q26vt). Brak reszty w tej transakcji sugeruje, że nadawca chciał przenieść wszystkie środki bez pozostawiania jakichkolwiek funduszy na pierwotnym adresie.

- **Możliwość przeniesienia środków z portfela papierowego:**

Przeniesienie całej kwoty mogło m.in. wynikać z faktu, że środki pochodziły z portfela papierowego. W takim przypadku nadawca miałby na celu zabezpieczenie środków na nowym, adresie, portfela lub chce wykonać jakieś inne transakcje w sieci. Portfel papierowy uniemożliwia płynne płacenie za usługi bądź produkty.

---

<sup>38</sup> Opłata transakcyjna fee to kwota, którą użytkownik płaci górnikiem za włączenie jego transakcji do bloku i jej potwierdzenie w sieci blockchain. Opłata transakcyjna jest zazwyczaj obliczana jako różnica między sumą wejść (inputs), a sumą wyjść (outputs) transakcji. Zazwyczaj przelicza się ją na satoshi na bajt – gdzie satoshi to najmniejsza jednostka BTC, a bajty odnoszą się do rozmiaru transakcji w danych.

Brak reszty w tej transakcji może również charakteryzować transfer z portfela papierowego.

- Przejście z portfela typu Legacy na SegWit

Przejście z adresu Legacy na SegWit, które widzimy w tej transakcji może być działaniem gdy użytkownik m.in.: chce korzystać z niższych opłat transakcyjnych lub wyższego poziomu bezpieczeństwa. W czasie analizy nie możemy jednak pominąć migracji środków do nowoczesnego portfela, który obsługuje funkcjonalniejsze standardy w sieci, w tym niższe opłaty. Należy również zauważyć, iż ogólnodostępne narzędzia w sieci do generowania “bezpiecznego”<sup>39</sup> adresu posługują się często adresem typu “1”. Co może również sugerować użycie generatora typu: <https://www.bitaddress.org>.

- **Wysoka procentowa wartość opłaty:**

Opłata transakcyjna wyniosła 0.00013854 BTC, co stanowi około 30.36% wartości transakcji. Wysoki procent opłaty, zwłaszcza w kontekście niewielkiej przesyłanej kwoty może wskazywać, że nadawca priorytetowo<sup>40</sup> traktował szybkie przetworzenie transakcji lub nie zoptymalizował opłaty, biorąc pod uwagę wartość przesyłanych środków.

#### **Możliwe scenariusze użycia:**

- o Prosta płatność: Transakcja może być prostą płatnością, gdzie nadawca przekazał całą dostępne środki po odjęciu opłaty transakcyjnej na jeden adres. W tym wypadku należy się zastanowić, dlaczego tak to zostało zrobione? Czy jest to związane z zapłatą “za coś”, kupno “czegoś” i to w taki sposób, aby dany portfel został użyty tylko raz, a może coś zupełnie innego<sup>41</sup>.
- o Konsolidacja środków: Przelew mógł być częścią strategii konsolidacji środków na jednym adresie lub portfelu, co często ma miejsce przy transferze środków z portfela papierowego.
- o Testowanie sieci: Alternatywnie, transakcja mogła być próbą testowania działania sieci lub portfela przy użyciu niewielkich kwot.
- o Zmiana funkcjonalności portfela: Użytkownik zmieniał funkcjonalność portfela np. przechodząc z zimnego na ciepły lub odwrotnie w celu np.: zamrożenia środków.

Transakcja 1

ID

transakcji:

4debaa7f3b078920e1037bd71b9978c0c435b33c2e912e5ef186289440ba32db

Data i godzina: 2023-11-13 20:32:35

Kwota wejściowa (total input): 0.01058606 BTC

---

<sup>39</sup> “Not your keys, not your coins” - ogólna zasada w świecie kryptowalut mówi, że jeśli nie masz kluczy prywatnych do portfela, to znaczy, że nie są twoje krypto.

<sup>40</sup> Należy przyjąć, iż najszybciej transakcja może zostać zrealizowana przez około 10 minut jednak w przypadku niskiej opłaty może potrwać nawet paręnaście godzin (np. w ETH transakcja trwa nawet 12-15 sekund).

<sup>41</sup> Wprost narzuca się pytanie np.: w kontekście grup “przestępczych” jakie mają “procedury” w tym zakresie.

Adresy wejściowe (Inputs):

3GajgqnT67YkcrH1t6YnEZttRyRvqm2EPP - 0.00448901 BTC (bitomat)

32oQAY59QXAWStMjto8B8ABb3R1tgoJSAQ - 0.01009705 BTC (bitomat)

Kwoty wyjściowe (Outputs):

Output 1: 0.00045627 BTC na adres  
1MjKKhhWBGez6z5SjomZ94417duwVyMxFC (główny adres odbiorcy)

Output 2: 0.00993287 BTC na adres  
3DKV64SHYrGZAsmJgdbRbeRjMDnq7EyJ54d (reszta)

Opłata transakcyjna: 0.0001692 BTC

Stawka opłaty: 76 Satoshi/Byte

Liczba potwierdzeń: 40,808

W tej transakcji widoczne są dwa wyjściowe adresy (outputs), jednak interpretacja i obliczenie opłaty transakcyjnej w Bitcoinie nie zmienia się.

### Wejście (input):

- Adres: 3GajgqnT67YkcrH1t6YnEZttRyRvqm2EPP dostarczył 0.00448901 BTC:
- Adres: 32oQAY59QXAWStMjto8B8ABb3R1tgoJSAQ dostarczył 0.01009705 BTC:

Wyjścia (outputs):

- Output 1: 0.00045627 BTC na adres  
1MjKKhhWBGez6z5SjomZ94417duwVyMxFC:

**Przeznaczenie:** Ta kwota została przelana na adres użytkownika, co może sugerować że użytkownik wypłacił środki z bitomatu - jest to główna kwota tej transakcji, a reszta zostaje w „urządzeniu”.

**Intencje:** Użytkownik mógł wypłacić środki, które wcześniej wpłacił do bitomatu, lub dokonał zakupu BTC za gotówkę, którą bitomat przyjął.

- Output 2: 0.00993287 BTC na adres  
3DKV64SHYrGZAsmJgdbRbeRjMDnq7EyJ54d:

**Reszta:** Większość środków została zwrócona na adres bitomatu. Adres ten pełni funkcję przechowywania reszty środków po zakończeniu transakcji z użytkownikiem.

**Przeznaczenie:** Środki te mogą być wykorzystane do przyszłych transakcji w bitomacie lub zostać zasilone w inne miejsce w celu uzupełnienia płynności.

### Możliwe scenariusze użycia:

- Wpłata środków w walucie fiat: Użytkownik podchodzi do bitomatu i wypłaca 0.00045627 BTC na swój adres (1MjKKhhWBGez6z5SjomZ94417duwVyMxFC). Reszta środków, czyli 0.00993287 BTC, wraca do bitomatu, co sugeruje, że użytkownik wypłacił tylko niewielką część dostępnych środków.

- Testowania bitomatu: Użytkownik przeprowadza testową transakcję, aby sprawdzić działanie urządzenia, funkcjonalność wypłat i poprawność działania systemu.
- Wpłata środków to późniejszej transakcji: użytkownik nie potrzebuje dużej kwoty na późniejsze “wydatki”, a chce to zrobić anonimowo<sup>42</sup>.

W Polsce najbardziej rozpowszechnione bitomaty należą do operatorów:

- FlyingAtom<sup>43</sup> - to jedna z największych firm zajmujących się sprzedażą kryptowalut w Polsce, oferująca zarówno bitomaty, jak i kantory kryptowalut.
- Shitcoins Club<sup>44</sup> - to europejska sieć bitomatów, która ma swoje urządzenia również w Polsce.
- ID transakcji - każda transakcja w sieci blockchain ma unikalny identyfikator, który umożliwi śledzenie i analizę konkretnej transakcji, a co za tym idzie prowadzi do konkretnych portfeli, a tym samym „użytkowników”. W przypadku analizy danych, znalezienie portfela to tylko mały krok kolejne „połączenia” znajdować będziemy poprzez analizę samej transakcji, a zatem kluczowym staje się tutaj jej ID.

## WERYFIKACJA WERSJI ŚLEDCZEJ

W trakcie analizy, dodajmy że bardzo prostego portfela, założyliśmy pewne wersje śledcze, a mianowicie:

- Główny portfel obiektu: “1MjKKhhWBGez6z5SjomZ94417duwVyMxFC”
  - o Pierwsza transakcja “doładowanie”  
4debaa7f3b078920e1037bd71b9978c0c435b33c2e912e5ef186289440ba32db nastąpiła w dniu 2023-11-13 20:32:35 – to bezspornie można sprawdzić analizując blockchain. Do przemyślenia pozostaje fakt, dlaczego użytkownik wykorzystał portfel typu Legacy?  
Pytanie: Czy doładowanie nastąpiło przez bitomat? Jak to sprawdzić? Niestety bardzo mało informacji znajdziemy w sieci np.: w kierunku przypisania adresu do konkretnego bitomatu. W przypadku gdy pracujemy dla agencji rządowych jest już znacznie prościej, gdyż kolejnym krokiem będzie uzyskanie takich informacji od operatora danego urządzenia<sup>45</sup>.
  - o Druga transakcja – przeniesienie środków na “nowszy” portfel:  
3ad3d14fb31480327c567c62340393f21853413e5842fa1b2bc650af48e4c5bf  
nastąpiła w dniu 2023-11-18 00:48:36

<sup>42</sup> To wnioskowanie ma wadę w postaci faktu, iż jeśli założymy, że wpłata jest na zimny portfel (np. papierowy), to należy dokonać kolejnych transakcji celem przesłania środków na portfel ciepły (np. aplikacyjny).

<sup>43</sup> <https://flyingatom.com/>

<sup>44</sup> <https://shitcoins.club/>

<sup>45</sup> W zależności od gromadzonych danych i jurysdykcji otrzymane informacje mogą być różnej jakości.

Pytanie: Dlaczego wszystkie środki zostały przeniesione? Co dalej stało się z zasobami na portfelu? Czy to portfel użytkownika czy instytucjonalny?

Informatycy śledczy mogą analizować różne aspekty transakcji kryptowalutowych, jednak zakres analizy i skuteczność różni się w zależności od kryptowaluty. W przypadku Bitcoina i Ethereum analiza jest bardziej efektywna ze względu na przejrzystość blockchajna, podczas gdy w Monero prywatność użytkowników jest znacznie bardziej chroniona. Zabezpieczenie danych takich jak pełne kopie blockchajna, metadane z portfeli, oraz dane z giełd jest kluczowe dla przeprowadzenia skutecznej analizy.

### **Smart contract**

Pojęcie inteligentnych kontraktów (ang. smart contracts) wprowadził w 1994 roku Nick Szabo<sup>46</sup>. - amerykański informatyk i prawnik węgierskiego pochodzenia. Jako ekspert w dziedzinie kryptografii i systemów zdecentralizowanych, przedstawił koncepcję łączącą technologię z prawem i ekonomią, której głównym celem była automatyzacja i usprawnienie procesu zawierania umów<sup>47</sup>. Co istotne, Szabo stworzył również koncepcję „pieniądza opartego na protokole”, która stała się fundamentem dla projektów takich jak Bitcoin czy Ethereum. To właśnie ta druga platforma wprowadziła funkcjonalność inteligentnych kontraktów na skalę globalną. Dzięki wizji Nicka Szabo, koncepcja inteligentnych kontraktów przeszła znaczącą ewolucję, znajdując zastosowanie głównie w technologii blockchain. Obecnie stanowi kluczowy element takich platform jak Ethereum, Binance Smart Chain czy TRON. Powstaje jednak pytanie, czy rozwiązanie to można uznać za formę umowy i jakie konsekwencje prawne mogłyby wynikać z niedotrzymania określonych w nim warunków.

Współczesne smart kontrakty to samowykonywalne programy, tworzone głównie w języku Solidity<sup>48</sup>, działające w środowisku blockchain. Oferują szerokie spektrum zastosowań w różnych sektorach gospodarki, jednak ich decentralizacja, anonimowość i autonomiczność mogą być również wykorzystywane do działań przestępczych. Ze względu na zastosowane technologie, funkcjonalności i standardy, można je klasyfikować na wiele sposobów, co przekłada się na ich wszechstronne zastosowanie - od finansów, przez logistykę, po sztukę.

Smart kontrakty można podzielić według ich funkcji, celu oraz stopnia złożoności. Przykładem są:

---

<sup>46</sup> Nick Szabo jest podejrzewany o to że jest twórcą Bitcoin-a: By Nathan Reiff Published April 12, 2018 06:00 AM EDT ” Who Is Nick Szabo, and Is He Satoshi Nakamoto?”  
<https://www.investopedia.com/news/who-nick-szabo-and-he-satoshi-nakamoto/>

<sup>47</sup> Szerzej na temat: “Nick Szabo - Smart Contracts: Building Blocks for Digital Markets”,  
[https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschoo12006/szabo.best.vwh.net/smart\\_contracts\\_2.html](https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschoo12006/szabo.best.vwh.net/smart_contracts_2.html)

<sup>48</sup> Solidity - to język wysokopoziomowy, który przypomina JavaScript lub C++, który został zaprojektowany specjalnie do tworzenia smart kontraktów na blockchainie Ethereum. Istnieje wiele innych rodzajów języków programowania takich jak: Vyper, Rust, Move, jednak solidity jest najbardziej popularny.

- Smart kontrakty transferujące wartość (Transfer of Value Smart Contracts) - najprostszy typ kontraktów, automatyzujący przekazywanie środków (np. kryptowalut) między stronami po spełnieniu określonych warunków. Przykładami są kontrakty ERC-20 (tokeny) czy transakcje peer-to-peer (P2P) na platformie Ethereum.
- Smart kontrakty transferujące wartość (Transfer of Value Smart Contracts) - to najprostszy typ kontraktów, których celem jest automatyczne przekazywanie środków (np. kryptowalut) pomiędzy stronami po spełnieniu określonych warunków. Jako przykład można podać kontrakty ERC-20 (tokeny), transakcje peer-to-peer (P2P) na Ethereum.

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

// Import the ERC20 contract from OpenZeppelin library
import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

// Define the MyToken contract, inheriting from ERC20
contract MyToken is ERC20 {
    // Constructor of the contract
    constructor() ERC20("MyToken", "MTK") {
        // Mint initial supply of tokens to the contract deployer
        _mint(msg.sender, 1000000 * (10 ** decimals()));
    }
}
```

Rys.3. Przykładowy kod Solidity - Transfer of Value Smart Contracts

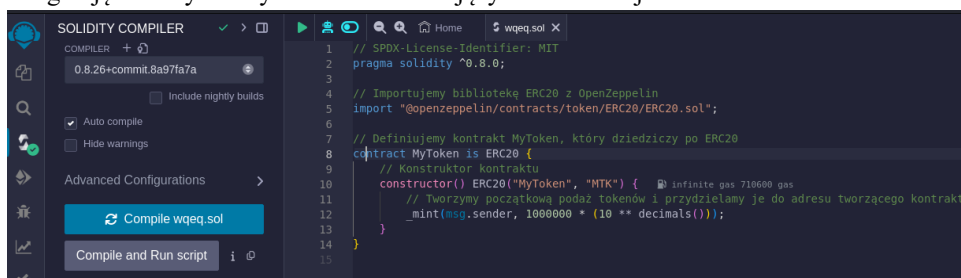
Ten kontrakt tworzy prosty token zgodny ze standardem ERC-20, który jest najpopularniejszym standardem tokenów na Ethereum. Wykorzystuje bibliotekę OpenZeppelin, która zapewnia bezpieczne i sprawdzone implementacje standardów tokenów.

- Import biblioteki ERC20 z OpenZeppelin: `import "@openzeppelin/contracts/token/ERC20/ERC20.sol";` Importuje standardowy kontrakt ERC20, który zawiera podstawowe funkcjonalności tokena ERC-20, takie jak transfer tokenów, sprawdzanie sald czy zatwierdzanie wydatków przez inne kontrakty.
- Definicja kontraktu MyToken: `contract MyToken is ERC20` Kontrakt MyToken dziedziczy po kontrakcie ERC20, dzięki czemu automatycznie zyskuje wszystkie funkcjonalności standardu ERC-20.

- Konstruktor kontraktu <sup>49</sup> : `constructor() ERC20("MyToken", "MTK") { _mint(msg.sender, 1000000 * (10 ** decimals()));` -
  - `ERC20("MyToken", "MTK")` - wywołuje konstruktor kontraktu ERC20, ustawiając nazwę tokena na "MyToken" i symbol na "MTK".
  - `_mint(msg.sender, 1000000 * (10 ** decimals()));` - tworzy 1 000 000 tokenów i przypisuje je do adresu wdrażającego kontrakt (`msg.sender`). `(10 ** decimals())` zapewnia prawidłowe uwzględnienie miejsc dziesiętnych (domyślnie 18).

Założenia kontraktu zakładają, że osoba wdrażająca kontrakt (`msg.sender`) będzie początkowym posiadaczem wszystkich tokenów.

W tym miejscu należy wspomnieć, iż istnieją narzędzia online, które mogą automatycznie analizować smart kontrakty pod kątem poprawności, funkcjonalności oraz bezpieczeństwa. Jednym z nich jest Remix IDE (<https://remix.ethereum.org>), który zawiera m.in. funkcjonalność związaną z analizą statyczną, umożliwia debugowanie oraz integrację z różnymi wtyczkami rozszerzającymi ich funkcjonalność.



```

1 // SPDX-License-Identifier: MIT
2 pragma solidity ^0.8.0;
3
4 // Importujemy bibliotekę ERC20 z OpenZeppelin
5 import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
6
7 // Definiujemy kontrakt MyToken, który dziedziczy po ERC20
8 contract MyToken is ERC20 {
9     // Konstruktor kontraktu
10    constructor() ERC20("MyToken", "MTK") {
11        // Tworzymy początkową podaż tokenów i przydzielamy je do adresu twórcy kontraktu
12        _mint(msg.sender, 1000000 * (10 ** decimals()));
13    }
14 }
15

```

Rys. 4. Analiza transakcji smart kontraktu za pomocą strony <https://remix.ethereum.org> - brak błędów.


Źródło: opracowanie własne

- Smart kontrakty warunkowe (Conditional Smart Contracts) - to kontrakty, które działają na zasadzie „jeśli-zdarzenie-to-akcja”. Warunki ich realizacji są jasno określone w kodzie i aktywują się automatycznie po ich spełnieniu. Do tychże można zaliczyć ubezpieczenia (payout po spełnieniu warunków), zakłady sportowe (wyплаты po ogłoszeniu wyników).
- Smart kontrakty oparte na zarządzaniu (Governance Smart Contracts) - to kontrakty zarządzające działaniami w zdecentralizowanych organizacjach (Decentralized Autonomous Organizations) lub innych strukturach, gdzie decyzje są podejmowane przez głosowania lub konsensus oraz systemy głosowania w projektach DeFi.

<sup>49</sup> Konstruktor kontraktu w Solidity to specjalna funkcja, która jest wywoływana tylko raz, w momencie wdrażania kontraktu na blockchainie. Służy do inicjalizacji stanu kontraktu, ustawiania wartości początkowych zmiennych oraz przekazywania parametrów podczas wdrożenia.

- Smart kontrakty wieloetapowe (Multi-Signature and Escrow Smart Contracts) - to kontrakty, które wymagają zatwierdzenia transakcji przez wiele stron (np. multisig) lub pełnią funkcję depozytu, gdzie środki są przechowywane do momentu spełnienia określonych warunków. Do najważniejszych z nich można zaliczyć Escrow<sup>50</sup> w handlu P2P (np. platformy takie jak Hodl Hodl), multisig wallets.
- Smart kontrakty oparte na tokenach niewymiennych (NFT Smart Contracts) - to kontrakty odpowiedzialne za tworzenie, zarządzanie i handel tokenami niewymiennymi (NFT), które są unikalnymi zasobami cyfrowymi. Do tej grupy zaliczamy: kontrakty ERC-721 (NFT), platformy handlu cyfrową sztuką (np. OpenSea).

Wydaje się, że tokenizacja dzieła sztuki jest jeszcze abstrakcyjnym pomysłem i jeszcze całkowicie nieosiągalnym. Otóż nie, dzieło Pawła Kowalewskiego „Dlaczego jest raczej coś niż nic?” (1986 rok) zostało stokenizowane jako NFT po tym, jak oryginalny obraz został zniszczony w powodzi w 1997 roku. Tokenizacja miała miejsce na blockchainie Ethereum.



**DESA** UNICJUM

AUKCJE ▾ MOJE OFERTY ▾ OBSERWOWANE OBIEKTY ULUBIENI ARTYŚCI English 🔍

◀ WRÓĆ DO AUKCJI 201 of Liczba Obiektów: 36 ▶ Nr PRZEJDŹ

201 | ☆  
**PAWEŁ KOWALEWSKI | "DLACZEGO JEST RACZEJ COŚ NIŻ NIC"**  
 Estymacja: 100,000 zł - 200,000 zł  
**SPRZEDANE 460,000 zł**  
**AUKCJA NA ŻYWO**  
 Sztuka Współczesna • Pop-art • Popkultura • Postmodernizm  
**Artysta**  
 Paweł Kowalewski (1958) **OBSERWUJ**  
**Wymiary**  
 wymiary: 2820 x 2292 pixeli (4 105 228 bytes)  
**Kategoria**  
 grafika  
**Opis**  
 non-fungible token, wymiary: 2820 x 2292 pixeli (4 105 228 bytes), token ID: 18785  
 adres portfela: 0x96efb0d79bbf98ee2d1c6f77d18eac7459d5441d  
 adres smart contract: 0x495f947276749Ce646f68AC8c248420045cb7b5e  
 non-fungible token (jpg)  
 wymiary: 2820 x 2292 pixeli (4 105 228 bytes)  
 minting: 17.11.2021  
 unikat 1/1

Rys. 5. Informacja o aukcji obrazu: “Dlaczego jest raczej coś niż nic”.

Źródło: opracowanie własne na podstawie <https://bid.desa.pl/lots/view/1-58EJO2/pawe-kowalewski-dlaczego-jest-raczej-co-ni-nic>

<sup>50</sup> Jednak nie jest to Escrow znany chociażby z forum darknetowego cebulka.

### *Potencjalne przestępcze wykorzystanie smart kontraktów*

Zdecentralizowany charakter smart kontraktów oraz ich zdolność do automatyzacji procesów stwarzają nowe możliwości dla działań przestępczych. Oto główne obszary potencjalnych nadużyć:

#### **Automatyzacja prania pieniędzy**

- **Strukturyzacja transakcji:** Smart kontrakty umożliwiają podział dużych sum na mniejsze przelewy, co utrudnia ich wykrycie. Przykładowo, kontrakt może automatycznie rozdzielić określoną kwotę na tysiące drobnych transakcji do różnych adresów, skutecznie maskując źródło funduszy.
- **Miksery i tumblery:** Smart kontrakty służą do mieszania środków pochodzących z różnych źródeł. Użytkownicy mogą korzystać z inteligentnego miksera, który łączy ich fundusze i rozprowadza je w losowych kwotach do różnych adresów, znacząco utrudniając śledzenie przepływu pieniędzy.

#### **Oszustwa i schematy Ponziego**

- **Falszywe ICO (Initial Coin Offerings):** Przestępcy tworzą nieistniejące projekty inwestycyjne, zbierając fundusze poprzez zautomatyzowane smart kontrakty, co komplikuje proces identyfikacji sprawców.
- **Piramidy finansowe:** Automatyzacja wypłat dla pierwszych inwestorów ze środków wpłacanych przez nowych uczestników tworzy trudne do wykrycia struktury piramidalne.

#### **Handel nielegalnymi towarami i usługami**

- **Decentralizowane rynki:** Smart kontrakty umożliwiają tworzenie anonimowych platform handlowych służących do obrotu narkotykami, bronią czy skradzionymi danymi.
- **Anonimowe aukcje:** Możliwość prowadzenia licytacji nielegalnych przedmiotów bez ujawniania tożsamości uczestników znacząco utrudnia pracę organów ścigania.

#### **Unikanie sankcji i finansowanie terroryzmu**

- **Transfery międzynarodowe:** Anonimowe transakcje realizowane przez smart kontrakty pozwalają omijać sankcje nałożone na organizacje lub państwa, z pominięciem tradycyjnego systemu bankowego.
- **Crowdfunding dla nielegalnych celów:** Smart kontrakty mogą służyć do zbierania funduszy na działalność terrorystyczną od anonimowych darczyńców, utrudniając śledzenie przepływu środków.

#### **Oplacanie przekazywanych informacji**

- **Handel poufnymi informacjami:** Automatyzacja płatności za sprzedaż skradzionych danych zapewnia anonimowość stronom transakcji. Na przykład, haker może sprzedawać wykradzione dane klientów banku, a smart kontrakt realizuje płatność po weryfikacji dostarczonych plików.

- Udostępnianie tajemnic handlowych: Pracownicy mogą przekazywać zastrzeżone informacje w zamian za kryptowaluty, korzystając z automatycznej weryfikacji danych i płatności przez smart kontrakt, co minimalizuje ryzyko identyfikacji.

Przedstawione przykłady pokazują, jak smart kontrakty mogą być wykorzystywane do działań przestępczych. Sytuacja ta podkreśla konieczność rozwoju skutecznych mechanizmów regulacyjnych i technologicznych, które zapewnią bezpieczeństwo oraz integralność ekosystemu blockchain.

### **Analiza smart kontraktów**

Z punktu widzenia “przejrzystości” kontraktów, oczywiście poza tymi które zostały podane już wcześniej, można je dodatkowo podzielić na te zweryfikowane oraz niezweryfikowane. Zweryfikowane kontrakty NFT na Etherscan to takie których kod źródłowy został publicznie udostępniony i zweryfikowany na Etherscan. Zaletami takiego podejścia jest fakt, iż użytkownicy mogą dokładnie przeanalizować kod źródłowy, zrozumieć logikę działania kontraktu oraz upewnić się, że nie zawiera on złośliwego kodu.

Poniżej przedstawiony kontrakt opisuje kolekcję NFT, w której głównym mechanizmem jest mintowanie (tworzenie) tokenów NFT przez właściciela kontraktu. Główne elementy tego kontraktu obejmują:

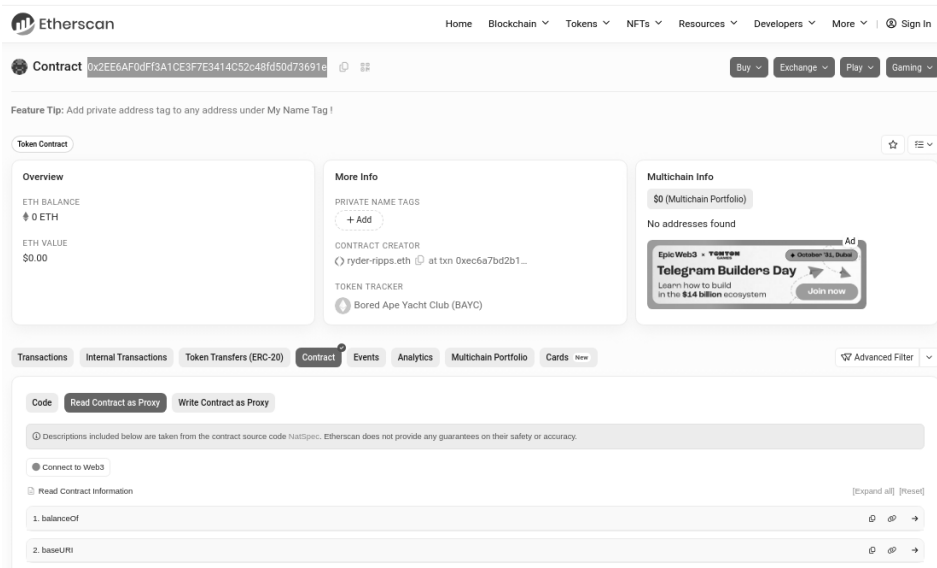
- Minting NFT: Funkcje `mint`, `mintAndApprove`, pozwalają właścicielowi na tworzenie nowych tokenów z unikalnym identyfikatorem oraz CID-em (Content Identifier) dla treści przechowywanych, np. na IPFS.
- Royalty: Każdy token generuje opłaty royalty (10%) dla twórcy przy każdej dalszej sprzedaży, co jest zaimplementowane za pomocą `royaltyInfo`.
- tokenURI: Funkcja `tokenURI` zwraca URI, które prowadzi do zasobu (zazwyczaj metadanych, takich jak obrazy) powiązanego z danym tokenem NFT.

0x2EE6AF0dFf3A1CE3F7E3414C52c48fd50d73691e

W polu kontrakt<sup>51</sup> widoczna jest informacja, że jest on zweryfikowany, dlatego też można przejść dalej do pola *Read Contract (...)*.

---

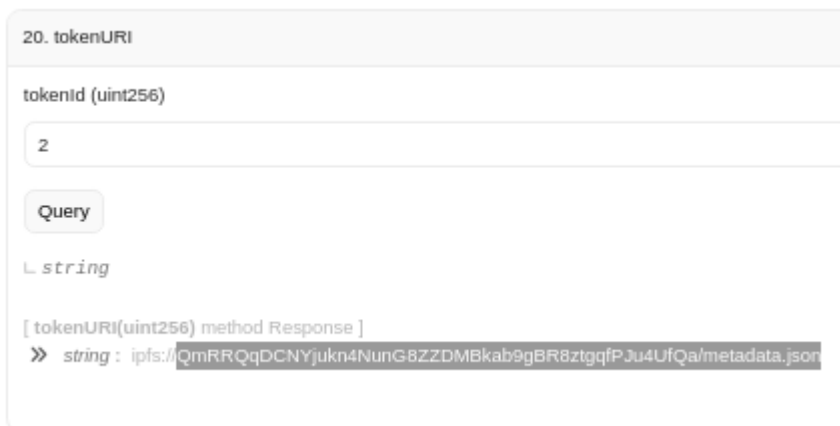
<sup>51</sup> Sam token nie zawiera kontraktu, w tym przypadku jest on w standardzie ERC-721 (NFT), to jednostka wartości reprezentowana w blockchainie, podczas gdy kontrakt to program, który zarządza logiką działania tego tokena. Natomiast kontrakt definiuje zasady, takie jak transfery, zatwierdzenia czy odczyty metadanych (np. URI). Token jest powiązany z kontraktem, który go obsługuje, ale kontrakt sam w sobie nie jest częścią tokena — to kod, który zarządza tokenami.



Rys. 6. Przykładowy kontrakt – aktywna opcja podglądu.

Źródło: Opracowanie własne na podstawie Etherscan

W polu `tokenURI`, które reprezentuje link do zewnętrznego zasobu. W praktyce, to czy będziemy mieli dostęp do pełnego URI będzie zależać od implementacji kontraktu i jego założeń. Istnieje wiele mechanizmów chroniących zasoby takie jak obrazy, opisy czy inne dane. Najczęściej stosowane to: ograniczenie `tokenURI`, tylko dla właścicieli, link może być zaszyfrowany, publiczne informacje reprezentowane w polu mogą zawierać tylko część metadanych, a pełne informacje są dostępne po zalogowaniu lub uwierzytelnieniu. W takich przypadkach, jeśli nie posiadamy tokena, funkcja `tokenURI` może zwracać pustą wartość lub błąd. Jednak w większości przypadków URI jest publicznie dostępne. Po wpisaniu odpowiedniej wartości, otrzymujemy `string`. Ponieważ każdy `tokenId` odpowiada innemu tokenowi NFT. W kontraktach ERC-721, każdy token ma unikalne ID i przypisane do niego specyficzne metadane (np. obraz). Kiedy wpisujemy różne `tokenId`, kontrakt zwraca odpowiedni URI, który prowadzi do metadanych (w tym obrazu) przypisanego do tego konkretnego tokena. Dlatego można zobaczyć różne obrazy dla różnych tokenów. W rozpatrywanym przypadku wpisujemy “2”.



Rys. 7. Przykładowy kontrakt – tokenId.

Źródło: Opracowanie własne na podstawie Etherscan

W wyniku działania *Query* otrzymujemy URI zaczynające się od `ipfs://` prowadzący do pliku na IPFS [ang. InterPlanetary File System]. Aby wyświetlić ten plik, można użyć publicznej bramy IPFS. Wystarczy zamienić `ipfs://` na link w formacie HTTP, np.: <https://ipfs.io/ipfs/QmRRQqDCNYjukn4NunG8ZZZDMBkab9gBR8ztgqfPJ4UfQa/metadata.json>

W wyniku działania otrzymujemy informacje:

```
{"name":"#9049","description":"","image":"ipfs://QmekFR9o7vutgitCRR37gYbeeCr8geLwMrgudgyYV3HJED/nft.png"}
```

Jest to plik JSON, który zawiera metadane tokena:

- name: "#9049" - nazwa tokena.
- description: brak opisu (jest puste).
- image: link do obrazu w formacie IPFS.

Aby zobaczyć obraz, należy zamienić `ipfs://` na HTTP, np.:

<https://ipfs.io/ipfs/QmekFR9o7vutgitCRR37gYbeeCr8geLwMrgudgyYV3HJED/nft.png>



Rys. 8. Przykładowy kontrakt – tokenId.

Źródło: Opracowanie własne na podstawie <https://ipfs.io>

Natomiast niezweryfikowane kontrakty NFT na Etherscan to takie, których kod źródłowy nie został udostępniony na Etherscan. W rezultacie dostępny jest jedynie bytecode, czyli zakodowana forma kontraktu. Przykładem takiego rodzaju podejścia do poufności jest kontrakt o którym wspomniano już wcześniej `0x495f947276749Ce646f68AC8c248420045cb7b5e`

Rys. 9. Przykładowy kontrakt – nieaktywna opcja podglądu.

Źródło: Opracowanie własne na podstawie Etherscan

W tym wypadku możemy pokusić się o dekompilację tego kodu m.in. za pośrednictwem narzędzia Palkeoramix decompiler dostępnego na <https://etherscan.io/>. Niestety taka próba analizy jest obarczona pewnymi błędami w dekompilacji, i brakiem widoczności części danych np. w tym przypadku brakiem widocznego URI dzieła artysty. Niemniej jednak część danych można odczytać.

## Decompile Bytecode

### Bytecode Decompile Result:

```
1 # Palkeoramix decompiler.
2
3 const unknown4060b25e = '2.0.0'
4 const unknownc311c523 = 1
5
6 def storage:
7   stor0 is mapping of uint256 at storage 0
8   stor1 is mapping of uint8 at storage 1]
9   owner is addr at storage 2
10  unknowncd7c0326Address is addr at storage 3
11  name is array of uint256 at storage 4
12  symbol is array of uint256 at storage 5
13  totalSupply is mapping of uint256 at storage 6
```

Rys. 10. Przykładowy kontrakt – dekompilacja bytecode.

Źródło: Opracowanie własne na podstawie Etherscan

Aby smart kontrakt został wykonany, muszą być spełnione pewne minimalne warunki, jednak w rzeczywistości absolutnie minimalne elementy można ograniczyć do dwóch kluczowych aspektów:

- Wywołanie kontraktu (trigger) - kontrakt musi zostać wywołany w sieci blockchain poprzez transakcję. To może być ręczna inicjatywa użytkownika, zewnętrzne wydarzenie (np. dane z wyroczni) lub inna transakcja, która inicjuje działanie kontraktu. Bez wywołania, kontrakt pozostaje „uśpiony” i nie wykonuje się.
- Gaz (opłaty transakcyjne) - Blockchain (np. Ethereum) wymaga odpowiedniej opłaty za przetwarzanie transakcji, która pokrywa koszty obliczeń związanych z wykonaniem kontraktu. Każda operacja, nawet najbardziej podstawowa, wymaga zużycia gazu (opłaty). Brak wystarczającej ilości gazu oznacza że kontrakt nie zostanie wykonany, nawet jeśli kontrakt jest poprawnie napisany i spełnione są inne warunki. W przypadku gdy transakcja ma zbyt mało gazu, smart kontrakt zostanie rozpoczęty, ale jeśli podczas jego wykonywania zabraknie gazu, kontrakt zostanie przerwany, a jego stan zostanie przywrócony do stanu sprzed transakcji. Jednak cała transakcja nie zostanie wykonana do końca. Co więcej, środki za zużyty gaz do momentu przerwania nie zostaną zwrócone. Smart kontrakt może zawierać mechanizmy, które sprawdzają dostępność gazu podczas swojego działania, posiadać zaimplementowane funkcje awaryjne np.: przerywanie działania lub rozłożenie działania na mniejsze etapy, aby uniknąć zużycia całego dostępnego gazu. Ilość gazu ustalana jest podczas wysyłania transakcji na blockchain. Użytkownik lub aplikacja decyduje, ile gazu chce przeznaczyć na daną transakcję. W przypadku gdy ustali się zbyt dużą ilość gazu jego nadmiar jest zwracany do użytkownika. W przypadku smart kontraktów na Ethereum (i innych blockchainach opartych na

mechanizmie gazu) nadmiar gazu nie wpływa na szybkość wykonania transakcji tak jak to ma “miejsce” w BTC.

Inteligentne kontrakty stanowią innowacyjne narzędzie z ogromnym potencjałem zastosowań w różnych sektorach gospodarki. Ich charakterystyka technologiczna niesie jednak wyzwania związane z bezpieczeństwem, legalnością i potencjalnym wykorzystaniem do celów przestępczych. Konieczne jest opracowanie odpowiednich regulacji, narzędzi nadzorczych oraz regulacyjnych na bazie prawa lokalnego, które zapewnią zarówno bezpieczeństwo, integralność ekosystemu blockchain jak i legalność, jednocześnie umożliwiając dalszy rozwój tej technologii.

## **PODSUMOWANIE**

Artykuł koncentruje się na podstawach technologii blockchain i kryptowalut, ich strukturze, oraz na narzędziach stosowanych do analizy przepływów finansowych. Przedstawiono znaczenie zrozumienia tych technologii zarówno w kontekście legalnych, jak i potencjalnie nielegalnych zastosowań. Szczegółowo opisano różne rodzaje kryptowalut, takie jak Bitcoin, Ethereum, Monero, oraz sposoby identyfikacji portfeli kryptowalutowych, co jest kluczowe w pracy analitycznej i śledczej. Wskazano też metody zamiany kryptowalut na waluty fiducjarne przez giełdy, DEX-y, bitomaty czy usługi P2P, które mogą być istotne w śledzeniu przepływów. Autor koncentruje się również na smart kontraktach, które zostały opisane jako autonomiczne programy uruchamiane na blockchainie. Automatyzują one wykonanie zapisanych warunków umowy, eliminując pośredników. Ich potencjał zastosowań jest szeroki – od finansów po logistykę, lecz ich zdecentralizowana natura niesie także ryzyko przestępcze.

## **BIBLIOGRAFIA**

1. Antonopoulos, Andreas M. - Mastering Bitcoin: Unlocking Digital Cryptocurrencies. O'Reilly Media, 2017. ISBN: 978-1491954386
2. Antonopoulos, Andreas M., Wood, Gavin - Mastering Ethereum: Building Smart Contracts and DApps. O'Reilly Media, 2019. ISBN: 978-1491971949
3. Bashir, Imran - Mastering Blockchain: Distributed Ledger Technology, Decentralization, and Smart Contracts Explained. Packt Publishing, 2020. ISBN: 978-1839213199
4. Bramhvanshi, Shailendra - How To Create Cryptocurrency Step By Step Guide. 2023. ISBN: 978-9359170411
5. De Filippi, Primavera, Wright, Aaron - Blockchain and the Law: The Rule of Code. Harvard University Press, 2018. ISBN-13: 978-0674976429
6. DiMatteo, Larry A. - The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms. Cambridge University Press, 2023 Online ISBN 978-1009293167
7. Hardcore Satoshi - Cryptocurrency & Blockchain: A Beginner's Guide to invest in Cryptocurrency | Cryptocurrency and Blockchain Technology Explained. 2022. ISBN: 979-8441474115

# MODEL ZABEZPIECZENIA KRYPTOWALUT W TOKU POSTĘPOWANIA KARNEGO W ŚWIETLE WYTYCZNYCH PROKURATURY KRAJOWEJ – ANALIZA I PROPOZYCJE ZMIAN

MODEL FOR PRESERVATION OF CRYPTOCURRENCIES IN THE COURSE  
OF CRIMINAL PROCEEDINGS IN LIGHT OF THE GUIDELINES OF THE  
NATIONAL PROSECUTOR'S OFFICE - ANALYSIS AND PROPOSALS FOR  
CHANGES

Adam BEHAN <sup>1</sup>, Wiktoria SZYBIAK <sup>2</sup>

**Streszczenie:** W artykule podejmowana jest analiza wytycznych Prokuratury Krajowej dotyczących proponowanego modelu zabezpieczania kryptowalut w toku postępowań karnych. Autorzy w opracowaniu zwracają uwagę na pojawiające się w zaleceniach błędy, nieścisłości i nieoptymalne rozwiązania oraz proponują alternatywne podejście organów ścigania względem analizowanej problematyki, które zapewniłoby większą efektywność oraz znacznie wyższy poziom bezpieczeństwa. W ramach analizy uwzględniane są kwestie dotyczące m.in. specyfiki funkcjonowania giełd kryptowalut i sposobu zarządzania przez nie aktywami swoich klientów, terminologicznego rozróżniania pojęć z zakresu kryptografii (tj. adres a portfel) oraz wskazania potencjalnych zagrożeń związanych z generacją kluczy za pomocą ogólnodostępnych serwisów internetowych. Rekomendowane przez Autorów rozwiązania obejmują centralizację procesu zarządzania aktywami poprzez utworzenie dedykowanego zespołu w Prokuraturze Krajowej przy jednoczesnym wykorzystaniu funkcjonalności portfeli deterministycznych (HD) i wielopodpisowych oraz wprowadzenia jednolitych standardów generowania kluczy offline.

**Słowa kluczowe:** zabezpieczanie kryptowalut, postępowanie karne, giełda kryptowalut, portfel, adres

**Summary:** The article undertakes an analysis of the guidelines of the National Prosecutor's Office regarding the proposed model for securing cryptocurrencies in the course of criminal proceedings. In the study, the authors draw attention to the errors, inaccuracies and suboptimal solutions appearing in the recommendations, and propose an alternative approach of law enforcement agencies to the analyzed issue, which would

---

<sup>1</sup> asystent w Katedrze Prawa Karnego UJ, adiunkt na Wydziale Informatyki, Elektroniki i Telekomunikacji AGH, specjalizujący się w prawnokarnych aspektach walut wirtualnych, a.behan@uj.edu.pl, ORCID: 0000-0002-0108-0386.

<sup>2</sup> studentka V roku prawa na WPiA UJ, seminarzystka w Katedrze Postępowania Karnego UJ, Wiceprzewodnicząca Koła Naukowego Postępowania Karnego TBSP UJ, ORCID: 0009-0007-2807-6583

ensure greater efficiency and a much higher level of security. The analysis takes into account issues such as the specifics of the functioning of cryptocurrency exchanges and how they manage the assets of their clients, the terminological distinction between cryptography concepts (i.e. address vs. wallet), and the identification of potential risks associated with the generation of keys using publicly available online services. The solutions recommended by the authors include centralizing the asset management process by creating a dedicated team at the National Prosecutor's Office while leveraging the functionality of deterministic (HD) and multi-signature wallets, and introducing uniform standards for offline key generation.

**Keywords:** preservation of cryptocurrency, criminal proceedings, cryptocurrency exchange, wallet, address.

## WSTĘP

Problematyka zabezpieczenia walut wirtualnych, na potrzeby postępowania karnego, doczekała się w piśmiennictwie licznych opracowań, w których przedstawiano stanowiska (zazwyczaj bez ich dogłębnego uzasadnienia), iż bezsprzecznie możliwym jest ich zabezpieczenie na potrzeby toczącego się postępowania karnego. Pozostawiając na boku rozważań samą dopuszczalność stosowania względem walut wirtualnych zabezpieczenia majątkowego na gruncie obowiązujących przepisów (wg autorów niniejszego opracowania w obecnym stanie prawnym nie jest to dozwolone<sup>3</sup>), w niniejszym artykule analizie poddany został techniczny i organizacyjny model procedowania w przedmiocie zabezpieczania kryptowalut przygotowany przez Departament do spraw cyberprzestępczości i informatyzacji Wydziału do spraw cyberprzestępczości Prokuratury Krajowej, który wydany został w formie wytycznych 1001-12.024.4.2023 z dnia 25 maja 2023 r.

Dostępne m.in. w sieci TOR zalecenia, wydane celem „*ujednoczenia praktyki prokuratorskiej*” w zakresie „*sposobów dokonywania zabezpieczeń walut wirtualnych w toku prowadzonych postępowań*”, obfitują niestety w liczne błędy natury merytorycznej i całkowicie niefunkcjonalne rozwiązania, które należy poddać krytyce. Jednocześnie przed analizą konkretnych wytycznych, należy pokrótce i na dużym poziomie ogólności przedstawić samą procedurę, która zobrazować pozwoli kluczowe elementy modelu zabezpieczania, jaki opracowany został przez Prokuraturę Krajową.

---

<sup>3</sup> Co nie oznacza jednocześnie, że być dopuszczalne nie powinno. Nie ulega bowiem wątpliwości dla piszących, że absolutnie pożądanym byłby stan, w którym klarownym jest status kryptowalut na gruncie szeroko rozumianego prawa karnego, a także możliwość stosowania względem nich instytucji zabezpieczenia majątkowego czy przepadku.

## **MODEL ZABEZPIECZANIA WALUT WIRTUALNYCH W WYTYCZNYCH 1001-12.024.4.2023**

Zgodnie z ich treścią zabezpieczanie walut wirtualnych w postępowaniach karnych stanowi kluczowy element działań prokuratury, szczególnie w kontekście przestępstw gospodarczych i prania pieniędzy. Waluty wirtualne mogą w ich świetle być traktowane zarówno jako mienie podlegające zabezpieczeniu majątkowemu, jak i dowód rzeczowy, w zależności od okoliczności konkretnej sprawy. Kluczowym celem jaki przyświeca prokuraturze jest dążenie do ochrony interesów pokrzywdzonych oraz przeciwdziałanie wyprowadzaniu środków pochodzących z przestępstwa przez ich sprawców.

Proces zabezpieczania walut wirtualnych rozpoczyna się od identyfikacji miejsc ich przechowywania, które mogą znajdować się na „*na portfelu zewnętrznym, będącym w dyspozycji sprawcy bądź innej osoby objętej zakresem ustaleń śledztwa, np. sprzętowym, papierowym, desktopowym czy webowym lub też na kontach założonych na giełdzie lub w kantorze kryptowalut*”.

Sam proces ich „zatrzymania” możliwy jest m.in. poprzez dobrowolne wydanie przez właściciela portfela, kluczy prywatnych, haseł czy PIN-ów. Jeśli to nie następuje, organ prowadzący postępowanie przygotowawcze może przeprowadzić przeszukanie w celu ujawnienia kluczowych danych dostępowych. Istnieje również możliwość skierowania żądania wydania rzeczy do giełd kryptowalut, zarówno krajowych, jak i zagranicznych, m.in. poprzez skorzystanie z instrumentów międzynarodowej pomocy prawnej.

Przed podjęciem właściwych czynności procesowych konieczne jest odpowiednie przygotowanie, w tym zaangażowanie specjalisty z zakresu informatyki śledczej lub funkcjonariusza Centralnego Biura Zwalczania Cyberprzestępczości. Podczas przeszukania należy zwracać szczególną uwagę na wszelkie dokumenty, zapiski i urządzenia, które mogą zawierać informacje o kluczach publicznych, kluczach prywatnych, seed lub historii transakcji. Wytyczne wskazują, iż jeśli to możliwe, waluty wirtualne powinny zostać natychmiast przetransferowane na portfel prokuratury, co pozwoli uniknąć ich utraty lub nieautoryzowanego wyprowadzenia przez osoby trzecie. Każdy etap czynności musi być szczegółowo udokumentowany, w tym w protokołach i za pomocą zrzutów ekranu.

Prokuratura zaleca stosowanie zewnętrznych portfeli sprzętowych lub papierowych do przechowywania zabezpieczonych walut wirtualnych. Portfele giełdowe powinny być wykorzystywane jedynie w szczególnie uzasadnionych przypadkach, takich jak brak możliwości przechowywania niskich walut na portfelach zewnętrznych. Proces zakładania portfela powinien być przeprowadzany komisyjnie i udokumentowany protokołem. Administrator portfela, najczęściej wskazany przez kierownika jednostki, odpowiada za jego bieżącą obsługę i zarządzanie. Klucze prywatne i seed należy przechowywać w osobnych kopertach zdeponowanych w Narodowym Banku Polskim. Obsługa portfeli powinna odbywać się na dedykowanych komputerach, odseparowanych od sieci prokuratury.

Zalecenia wskazują, że zabezpieczone waluty wirtualne, z uwagi na ich zmienną wartość, powinny być w miarę możliwości niezwłocznie sprzedawane. Decyzja o sprzedaży podejmowana jest w formie postanowienia, a proces realizuje komornik lub naczelnik urzędu skarbowego. Wszelkie czynności związane z transferem walut wirtualnych, w tym ich sprzedaż, powinny być szczegółowo dokumentowane, aby zapewnić pełną rozliczalność. Po sprzedaży niezbędna jest zmiana postanowienia o zabezpieczeniu majątkowym, która wskazywać będzie na zabezpieczenie uzyskanej kwoty w walucie fiducjarnej.

Co warte podkreślenia, wytyczne wskazują, że „podstawową formę przechowywania kryptowalut, stanowiących przedmiot zabezpieczenia majątkowego bądź stanowiących dowody rzeczowe, a jednocześnie stanowiących depozyt wartościowy, jest ich przetransferowanie na portfel zewnętrzny, przy czym rekomenduje się stosowanie portfela papierowego, bądź sprzętowego marki Ledger”. Oznacza to, że w sytuacjach pozyskiwania walut wirtualnych w toku postępowania, domyślnym modelem działania jest tworzenie indywidualnych portfeli sprzętowych (ok. 600 zł/szt. - Ledger Nano X) dedykowanych konkretnej sprawie. Sam proces konfiguracji portfela sprzętowego powinien zostać przeprowadzony komisyjnie przy udziale kierownika jednostki, wyznaczonego administratora portfela oraz w razie potrzeby specjalisty. Warto dodać w tym momencie, że zdecydowana większość kierowników jednostek prokuratur, ani samych prokuratorów nie miała nigdy styczności z aktywami wirtualnymi. Co za tym idzie obowiązek konfigurowania portfeli oraz generowania kluczy i adresów, na których potencjalnie zabezpieczane mają być warte miliony waluty wirtualne, nakładany na osoby, które z powodów braku wiedzy technicznej (oczywiście zrozumiałej – niepodobna wymagać od każdego prokuratora, że będzie rozumiał zależności pomiędzy kluczem prywatnym, publicznym czy adresem) mogą nie mieć pełnej świadomości jakimi danymi operują, wydaje się być nie do końca adekwatny.

Prokuratura Krajowa rekomenduje tworzenie tzw. portfeli ogólnych na poziomie regionalnym i okręgowym, tylko w wyjątkowych i nagłych przypadkach. Każdy transfer środków na portfel ogólny musi być zgłaszany prokuratorowi regionalnemu lub okręgowemu, wraz z podaniem szczegółów transakcji, takich jak sygnatura sprawy, ilość przelanych walut wirtualnych i data operacji.

Całość procesu zabezpieczania walut wirtualnych wymaga ścisłej współpracy z ekspertami technicznymi oraz bieżącego monitorowania przez wyznaczone jednostki. Kluczowe jest także przestrzeganie wysokich standardów bezpieczeństwa i zapewnienie rozliczalności wszystkich działań związanych z obsługą walut wirtualnych.

Ogólny model przedstawiony powyżej, podlega rzecz jasna w omawianych wytycznych głębszemu uszczegółowieniu, które w bardzo wielu miejscach należy poddać głębszej krytyce z uwagi na fundamentalne błędy natury technicznej i nieoptymalny model postępowania w procesie zabezpieczania walut wirtualnych.

### **Portfele a adresy**

Szczegółową analizę wytycznych rozpocząć należy od następującego fragmentu: „*podejmowane w toku postępowania czynności, mogą w praktyce prowadzić do ujawnienia podlegających zajęciu kryptowalut: na portfelu zewnętrznym, będącym w dyspozycji sprawcy bądź innej osoby objętej zakresem ustaleń śledztwa, np. sprzętowym, papierowym, desktopowym czy webowym lub też na kontach założonych na giełdzie lub w kantorze kryptowalut*”.

Mając na względzie wysoce specjalistyczny charakter omawianej materii oraz konieczność zachowania maksymalnej precyzji w zakresie nazewnictwa mogą pojawić się przypuszczenia, że autorzy wytycznych nie rozróżniają pojęcia adresów walut wirtualnych od portfeli. Należy przypomnieć, że:

*„Przez „portfel kryptowalutowy” rozumieć trzeba program, urządzenie czy inny fizyczny nośnik, na którym przechowywać będziemy pary kluczy umożliwiających skorzystanie ze zgromadzonych środków. Celem klaryfikacji dodać należy, że sam portfel (wbrew potocznemu znaczeniu tego słowa) nie przechowuje żadnych środków, a wyłącznie klucze prywatne (tj. swoiste dane dostępne do adresów). Oczywiście jest, że ograniczone możliwości percepcyjne uniemożliwią zdecydowanej większości użytkowników zapamiętanie wielu par kluczy publiczny–prywatny i korespondujących z nimi adresów, dlatego pojawiło się wiele sposobów przechowywania owych kluczy.(...) Dla jasności trzeba dodać, że jakkolwiek często poruszane w kontekście kryptowalut są pojęcia paper wallet czy brain wallet, to należy mieć świadomość, że zapisujemy tam (na owej kartce papieru czy w naszej pamięci) wyłącznie klucz prywatny, który możemy porównać do hasła umożliwiającego dostęp do systemu bankowości elektronicznej. Zapis wartości naszej waluty wirtualnej jest bowiem zawsze w jakiejś strukturze danych (najczęściej w blockchainie), gdzie owe wartości są zapisywane”<sup>4</sup>.*

Za kategoriycznie błędne należy więc uznać utożsamianie ze sobą obu terminów. Adres w żadnym wypadku nie może być uznany za portfel, tzn. nie służy do przechowywania par kluczy warunkujących możliwość korzystania ze środków, a stanowi on unikalny identyfikator alfanumeryczny używany do odbierania i wysyłania kryptowalut w sieci blockchain<sup>5</sup>. Umożliwia użytkownikowi aktywne uczestnictwo w sieci poprzez dokonywanie transferów. Jest generowany z klucza publicznego (a ten z klucza prywatnego) za pomocą funkcji kryptograficznych (SHA-256, RIPEMD-160, kodowanie Base58Check<sup>6</sup>). Ponadto, wydaje się, że zupełnie zbędnym jest używanie w tym kontekście sformułowania „adres publiczny”<sup>7</sup>, gdyż nie istnieją adresy niepubliczne

---

<sup>4</sup> A. Behan, *Waluty wirtualne jako przedmiot przestępstwa*, Krakowski Instytut Prawa Karnego Fundacja, Kraków 2022, s. 165.

<sup>5</sup> Celem zilustrowania można go przyrównać do quasi numeru rachunku bankowego, z którego i na który dokonywane być mogą transfery.

<sup>6</sup> Zob. dokładnie opisany proces tworzenia adresów – *Ibidem*, s. 147 i n.

<sup>7</sup> Z drugiej strony w wytycznych znajduje się sformułowanie, że *podczas przeszukania zasadne jest zwracanie uwagi na wszelkie zapiski, mogące stanowić adres klucza publicznego bądź prywatnego, hasła, loginy*”, co rodzi podejrzenie, że nie do końca poprawnie rozróżniane są pojęcia kluczy i adresu.

a transparentność tychże danych jest zdeterminowana specyfiką działania samego systemu zdecydowanej większości walut wirtualnych<sup>8</sup>.

Dalsza analiza zaleceń wydanych przez Prokuraturę Krajową wskazuje jednak, że ich autorzy traktują oba pojęcia jako synonimy bądź używają terminologii niewłaściwej z punktu widzenia technicznego, co ilustrują następujące fragmenty wytycznych:

*„W przypadku ujawnienia w sprawie **adresu publicznego portfela**, czy to przez biegłego w toku badania zabezpieczonych nośników elektronicznych, czy to w toku przeszukania miejsca lub urzędnika zawierającego dane informatyczne, w pierwszej kolejności należy podjąć próbę zidentyfikowania, czy adres ten jest **portfelem zewnętrznym** (sprzętowym, papierowym, desktopowym), czy też mamy do czynienia z **portfelem giełdowym**. (...) Ponadto ujawnienie jednocześnie klucza prywatnego może wskazywać, że mamy do czynienia z portfelem zewnętrznym”.*

Lektura wytycznych sugeruje, że „portfel zewnętrzny” odnosi się do sytuacji, w której kluczami prywatnymi, a tym samym zgromadzonymi na adresie środkami samodzielnie zarządza użytkownik bez korzystania z usług zewnętrznego podmiotu (np. giełdy). Znacznie bardziej przystającą i powszechnie uznawaną klasyfikacją portfeli w tym aspekcie jest podział na model typu custodial oraz non-custodial. Rozróżnienie to oparte jest na ocenie, czy uczestnik sieci sprawuje wyłączną kontrolę nad środkami czy potencjalnie dysponować nimi może jeszcze inny podmiot, ze względu na przekazanie mu kluczy prywatnych, celem ich przechowywania oraz zarządzania w imieniu usługobiorcy<sup>9</sup>. Należy, wszakże wyraźnie rozróżniać samo pojęcie portfela od modelu, w jakim on funkcjonuje (tzn. metody przechowywania za jego pomocą kluczy) oraz od pojęcia samego adresu, na którym zgromadzone zostały środki. Fundamentalna różnica pomiędzy nimi (tj. portfelami custodial i non-custodial) sprowadza się do sposobu zarządzania kluczami prywatnymi umożliwiającymi dysponowanie zgromadzonymi na danym adresie w sieci środkami. W przypadku samodzielnie tworzonych przez użytkowników adresów, założyć można, że dysponują oni także kluczami prywatnymi umożliwiającym podpisywanie transakcji<sup>10</sup>. Co do zasady odmiennie przedstawia się sytuacja w modelu custodial, a w szczególności gdy użytkownik zgromadzone środki przechowuje na giełdzie kryptowalutowej. W takim przypadku bowiem środki wielu użytkowników są zazwyczaj wspólnie przechowywane w puli, a adresy te widoczne są w blockchainie giełdy, która prowadzi **wewnętrzną ewidencję** (własną bazę danych/księgę rachunkową) określającą, jaki udział w tej puli przypada konkretnemu użytkownikowi. A zatem „stan konta” widoczny na krypto-giełdowym koncie określonego klienta to tak naprawdę wyłącznie informacja z tej wewnętrznej bazy danych.

---

<sup>8</sup> Odmiennie wygląda kwestia jawności w „anonimowych” systemach walut wirtualnych – np. Monero gdzie wykorzystywane są zaawansowane techniki kryptograficzne (m.in. ring signatures, stealth addresses, RingCT) a przesłedzenie dokonywanych na blockchainie transakcji i ustalenie powiązanych z nimi adresów jest bardzo trudne (lub niemożliwe).

<sup>9</sup> A. Behan, *Waluty wirtualne jako przedmiot przestępstwa*, Krakowski Instytut Prawa Karnego Fundacja, Kraków 2022, s. 169 i n.

<sup>10</sup> O ile ich np. nie utracili.

Należy wskazać na kolejny przykład nierozróżniania między sobą adresu oraz portfela oraz braku zrozumienia modelu działania giełd kryptowalutowych. W części wytycznych pt. „*Zabezpieczanie kryptowalut ujawnionych na portfelu giełdowym*”, podano błędnie, że „*stan środków na każdym portfelu jest jawny i dostępny dla każdego. W celu jego sprawdzenia należy skorzystać z jednego z dostępnych narzędzi, np. wpisując ujawniony adres publiczny na stronie www.blockchain.com*”. Pominąwszy fakt, że w blockchainie nie widać UTXO portfela, ale poszczególnych adresów, to analiza nawet takiego adresu giełdowego, ujawnić może, że należy on do giełdy, ale w żaden sposób nie ujawni stanu posiadania konkretnego użytkownika, analogicznie jak w przypadku rachunku zbiorczego<sup>11</sup> (ang. omnibus account), na którym widoczna jest jedna wspólna pula aktywów, zaś szczegółowe saldo poszczególnych klientów jest odnotowywane wyłącznie w wewnętrznej ewidencji tego podmiotu. Na danym adresie mogą znajdować się bowiem, jednostki walut wirtualnych należące do tysięcy klientów danej giełdy. Innymi słowy, za pomocą wskazanych narzędzi nie da się ustalić, jaka część kryptowalut widocznych na adresie przypisanym do giełdy należy do określonego klienta korzystającego z jej usług, ponieważ informacje te są dostępne w ramach wewnętrznego systemu rozliczeniowego giełdy, o czym już wcześniej wspomniano.

Dodać tylko należy, że portfel custodial jest charakterystycznym rodzajem usług świadczonych przez giełdy kryptowalut i stanowi jednocześnie najczęściej spotykany sposób zarządzania zgromadzonymi środkami przez ich dysponentów z uwagi na łatwość dokonywania transakcji kupna/sprzedaży. Pojęcie „*custodian wallet provider*” wprowadzone zostało po raz pierwszy do europejskiego porządku prawnego w dyrektywie (UE) 2018/843 (tzw. AML V)<sup>12</sup>, a zdefiniowane w art. 3 pkt. 19 dyrektywy (UE) 2015/849 jako „*entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies*”<sup>13</sup>. Przytoczona definicja „dostawcy usług w zakresie kryptoaktywów” uległa zmianie z dniem 30 grudnia 2024 r. na podstawie art. 38 pkt 2 lit. c rozporządzenia (UE) 2023/1113<sup>14</sup>, który celem jej zrekonstruowania odsyła do art. 3 ust. 1 pkt. 15, 16 rozporządzenia (UE) 2023/1114<sup>15</sup> (tzw. MiCA).

---

<sup>11</sup> Jest to rodzaj rachunku bankowego lub rachunku papierów wartościowych, na którym zgromadzone są środki (pieniądze lub aktywa inwestycyjne) należące do wielu różnych klientów.

<sup>12</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dn. 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE; Dz.U. UE L 156/43 z 2018 r.

<sup>13</sup> W polskiej wersji znalazło się sformułowanie „podmiot świadczący usługi polegające na przechowywaniu prywatnych danych uwierzytelniających w imieniu swoich klientów na potrzeby posiadania, przechowywania i przekazywania walut wirtualnych”.

<sup>14</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849 (Dz. U. UE. L. z 2023 r. Nr 150, str. 1).

<sup>15</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektywy 2013/36/UE i (UE) 2019/1937 (Dz. U. UE. L. z 2023 r. Nr 150, str. 40 z późn. zm.).

Oczywiście powzięcie informacji czy dany adres, jest związany z jakąś giełdą, ma niebagatelne znaczenie dla dalszych czynności podejmowanych przez prokuraturę. Wynika z niej bowiem dla prowadzącego postępowanie konieczność włączenia w proces dokonywania czynności procesowych i ich efektywnej realizacji dodatkowy podmiot, z którym współpraca jest niezbędna i bezpośrednio warunkuje legalność i skuteczność zastosowanych instytucji procesowych.

Każde to podnieść daleko idące wątpliwości względem modelu postępowania przedstawionego w wytycznych, który „w przypadku dobrowolnego wydania loginów i haseł do konta giełdowego”, nakazuje „dokonać logowania i przetransferowania jednostek cyfrowych z portfela sprawy, na portfel prokuratury”. Przypominać to może sytuację, w której policjant / prokurator samodzielnie wykonałby przelew środków zgromadzonych na rachunku bankowym podejrzanego za pomocą pozyskanych danych logowania do systemu bankowości internetowej. Takie działanie należałoby uznać za skrajnie naruszające obowiązujące przepisy. Co więcej, nieprawdą jest, że podanie loginu i hasła do giełdy równoznaczne jest z udzieleniem uprawnień do zlecenia transferu środków. Operacja, jaką sugerują wytyczne, jest w istocie wydaniem polecenia giełdzie (bez udzielenia jej informacji, że zlecenia nie dokonuje jej klient uprawniony na mocy umowy łączącej go z giełdą, ale prokurator albo inna osoba wskazana przez niego), aby ze swojego adresu dokonała transferu środków na podany adres odbiorcy, z pominięciem formalnej ścieżki wyznaczonej przez obowiązujące przepisy.

Autorzy wytycznych częściowo trafnie dostrzegają okoliczność, że w toku „czynności podejmowanych w miejscu zamieszkania sprawy może również dojść do ujawnienia na pozór **nic nie znaczącego ciągu od 12 do 24 słów w języku angielskim. Słowa te stanowią mogą tzw. seed, czyli rodzaj klucza prywatnego, służącego do odzyskania dostępu do środków, zgromadzonych na portfelu kryptowalutowym**”. Problematyka tzw. frazy odzyskiwania została wstępnie zasygnalizowana w kontekście brain wallet natomiast wymaga na tym etapie rozważań szczegółowego odniesienia.

Pojęcie „seed” jest immanentnie związane ze sposobem generowania kluczy w tzw. portfelach deterministycznych<sup>16</sup>, które umożliwiają, m.in. tworzenie dowolnie wielu adresów z wykorzystaniem jednego seed<sup>17</sup>. Dla zachowania spójności wywodu należy przypomnieć, że do wygenerowania tzw. ziarna/nasiona/seed wykorzystujemy „zestaw zrozumiałych dla człowieka słów, umożliwiającym odzyskanie kluczy do adresów w razie utracenia tych danych. Idea opiera się na wybraniu zestawu 12, 18 lub 24 słów, z których każde ma odpowiadający numer na liście. BIP-39 zuniifikował 2048 słów w 9 językach –

---

<sup>16</sup> Jakkolwiek jest możliwe wygenerowanie z niego pojedynczego adresu to co do zasady wykorzystuje się w przypadkach tworzenia portfeli HD.

<sup>17</sup> Zob. szerzej na temat portfeli HD – BIP-32 (Bitcoin Improvement Proposal). <https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki>, zarchiwizowany na <https://perma.cc/3PT9-XKZJ>; BIP-44 <https://github.com/bitcoin/bips/blob/master/bip-0044.mediawiki>, zarchiwizowany na <https://perma.cc/U9DM-V3H4>; BIP-49 <https://github.com/bitcoin/bips/blob/master/bip-0049.mediawiki>, zarchiwizowany na <https://perma.cc/7D4V-WSDG>; BIP-84 <https://github.com/bitcoin/bips/blob/master/bip-0084.mediawiki>, zarchiwizowany na <https://perma.cc/69VT-LCYJ>.

z tego można standardowo wybrać określoną przez siebie liczbę słów, za czym stoi – rzecz jasna – liczba możliwych kombinacji”<sup>18</sup>. Słowa te, np. drop away bridge romance cargo glow coach lizard remove entire noble very nie są samym seed, ale tzw. „seed phrase” czy „seed words” – i pozwolą dopiero wygenerować ziarno “239c3d46605381e7b5812aa521892473b3868a02914ca88793926d95fe2a2ecb3ea5d4e2be342a813855d8fd125f81e39cf947574a4154ca51195cb0705b99d8”, a następnie obliczyć korespondujący z nim „Account Extended Private Key” xprv9yXex9UP9dqfjCJiAt31Qz1Pq8ZM72uGfUugMoDFR34TdLbBnmLXEHBcfYhWoWVGZoYTpFPMiVoxkALFWS5ZsMJRfhcKgvWruWFwvE3HSpC.<sup>19</sup>

Wartości te<sup>20</sup> pozwolą następnie wygenerować dowolnie wiele kluczy prywatnych (następco kluczy publicznych i adresów). Umożliwiłoby to, o czym szerzej w dalszej części opracowania, wygenerowanie i przydzielenie przez Prokuraturę Krajową adresu każdej prokuraturze, bez konieczności przekazywania komukolwiek kluczy prywatnych do konkretnego adresu.

Same słowa nie są „rodzajem klucza prywatnego”, tj. nie umożliwiają bezpośrednio dysponowania środkami, lecz stanowią tzw. zdanie mnemoniczne, które służy jako podstawa do wygenerowania ziarna, a to z kolei, co do zasady, do deterministycznego wyliczenia konkretnych kluczy i korespondujących z nimi adresów. Co do zasady, gdyż wytyczne nie wskazują, że Standard BIP-39, wprowadza możliwość zdefiniowania dodatkowego „passphrase”, czyli quasi hasła bez znajomości którego, sam seed nie będzie miał żadnej wartości. W BIP-39 do obliczenia właściwego seedu używana jest funkcja PBKDF2-HMAC-SHA512, gdzie oprócz seed phrase wprowadzić można dodatkową sól w postaci ciągu: „mnemonic” + „passphrase”. Należy sfalsyfikować twierdzenie z wytycznych, iż „samo-posiadanie powyższego klucza umożliwia dokonanie zajęcia kryptowalut, bez konieczności pozyskania nośnika portfela sprzętowego, hasła czy PIN-u.” Ten „*nic nie znaczący ciąg od 12 do 24 słów w języku angielskim*” nie stanowi samodzielnej gwarancji pozyskania informacji niezbędnych do dokonywania transferów środków zgromadzonych na adresach. Dodać należy także, że standard BIP-39 posiada słowniki w 9 językach, które mogą stanowić „seed phrase”<sup>21</sup>, o czym zalecenia także powinny wspominać – gdyż ograniczenie czujności jednostek

<sup>18</sup> A. Behan, Waluty wirtualne jako przedmiot przestępstwa, Krakowski Instytut Prawa Karnego Fundacja, Kraków 2022, s. 177 – 178.

<sup>19</sup> W przypadku BIP-49 ciąg ten wygeneruje Account Private Key: yprvAJgpR8KVSAeMf5pkxwpZeVMc9rkFRzyzA2pFww22MSgY6vXog6ffphcy3PihWbUm2idGFSvsoGYZsPkm6xBqN9HDx2TVnYTLxw8AnUR9qyE, natomiast w przypadku BIP-84: zprvAeD431cqM6NPqfuKNaFWeCX2M1Bte15qUCMDCxgQZ8ATD4KLbgPTJV9EtiEKCEdzjQejqE1R4bsNZSsWkqCLPAw3HXy4uXNm4riNWCyhhK.

<sup>20</sup> Zob. szczegółowo opisany proces tworzenia: G. Walker, Mnemonic Seed. Encoding a Random Number in to Words And Using Them to Create a Seed, <https://perma.cc/2GDX-EZSA>.

<sup>21</sup> Te języki to angielski, japoński, koreański, hiszpański, chiński (uproszczony/tradycyjny), francuski, włoski, czeski, portugalski. Zob. <https://github.com/bitcoin/bips/blob/master/bip-0039/bip-0039-wordlists.md>, zarchiwizowany na <https://perma.cc/MXZ4-WV42>.

policii/prokuratury wyłącznie do słów angielskich jest absolutnie wadliwe i nieuzasadnione.

## **ZAKŁADANIE PORTFELA PROKURATURY**

Wytyczne wskazują także procedurę w jakiej portfele prokuratorów winny być tworzone i konfigurowane, jako nadrzędną zasadę ustanawiając, że *„podstawową formę przechowywania kryptowalut jest ich przetransferowanie na portfel zewnętrzny, przy czym rekomenduje się stosowanie portfela papierowego, bądź sprzętowego marki Ledger”*.

W tym momencie należy skupić się na fragmencie dotyczącym portfeli papierowych, wskazanych jako jeden ze sposobów „bezpiecznego” przechowywania jednostek walut wirtualnych. Wytyczne bowiem doprecyzowują w dalszej ich części, iż *„wygenerowanie portfela papierowego jest możliwe przy użyciu, np. strony <https://www.bitaddress.org>”* oraz, że *„na jednym portfelu papierowym możliwe jest przechowywanie tylko jednej waluty wirtualnej, przy czym na portfelach papierowych można przechowywać tylko niektóre rodzaje kryptowalut”*.

Nie sposób zgodzić się z powyższymi twierdzeniami z wielu powodów. Po pierwsze, „portfel papierowy” to kartka papieru, na której zapisany jest klucz prywatny (ewentualnie też klucz publiczny i adres). Na owej kartce nie ma rzecz jasna żadnych walut wirtualnych, więc nie można przetransferować na nią jakichkolwiek środków. Jednocześnie każda osoba, która ów klucz prywatny zobaczy/zapamięta/skopiuje będzie mogła dokonać transferu owych wartości. Z tego powodu, od wielu już lat zasadnie wskazuje się, że portfele papierowe zastąpione być powinny przez portfele sprzętowe, które oferują znacznie większe możliwości i nieproporcjonalnie wyższy poziom bezpieczeństwa, co nie oznacza jednak, że można je uznać za w pełni bezpieczne.

Za całkowicie niedopuszczalne i sprzeczne z fundamentalnymi standardami bezpieczeństwa należy uznać generowanie kluczy lub adresów za pomocą publicznie dostępnych serwisów, takich jak ten wskazywany przez autorów, ze względu na to, że osoba tworząca pary kluczy w takich warunkach nie ma jakichkolwiek możliwości weryfikacji, czy administrator tego serwisu nie rejestruje generowanych wartości. To, że dotychczas nikt nie zaraportował takiego ataku w kontekście tej witryny nie jest absolutnie usprawiedliwieniem takiego działania. Zalecane postępowanie wiąże się z ogromnym ryzykiem kompromitacji kluczy prywatnych i potencjalnym przejęciem środków przez osoby trzecie, które mogłyby uzyskać dostęp do generowanych przez użytkownika na stronie kluczy.

Z perspektywy bezpieczeństwa informacyjnego minimalnym standardem w generowaniu kluczy kryptograficznych powinno być ich tworzenie w środowisku lokalnym (offline) z wykorzystaniem zweryfikowanego oprogramowania open source. Przykładami takich narzędzi są skrypt JavaScript dostępny na [bitaddress.org](https://www.bitaddress.org) (wersja

uruchamiana po stronie klienta)<sup>22</sup>, Electrum lub MyCrypto. Oprogramowanie tego typu umożliwia generowanie par kluczy kryptograficznych oraz odpowiadających im adresów bez konieczności połączenia z siecią Internet, co redukuje potencjalne wektory ataku.

Należy jednakże podkreślić, że żadne narzędzie do generowania kluczy nie zapewnia absolutnego bezpieczeństwa. Nawet w przypadku uznawanej za stosunkowo bezpieczną wersji offline skryptu bitaddress.org zidentyfikowano podatności związane z modelem generowania entropii, który determinuje wartość początkową  $k$ , mieszczącą się w zakresie  $1 \leq k \leq 2^{256}-1$ .<sup>23</sup> Tego rodzaju niedoskonałość nie umożliwia bezpośredniego wyprowadzenia klucza prywatnego na podstawie klucza publicznego, jednak znacząco zwiększa efektywność i szybkość ataków typu brute force, co stanowi istotne zagrożenie dla środków. Rzeczywiste konsekwencje takiej podatności, zaobserwowano w przypadku algorytmu entropii używanego w Libbitcoin Explorer 3.0.0 do 3.6.0, która umożliwiła atakującym uzyskanie kluczy do stworzonych adresów, na których przechowywane były środki. W kontekście „bezpiecznego” tworzenia kluczy/adresów i konfigurowania portfeli, przygotowana przez Distrust analiza<sup>24</sup> wskazała, iż:

„Generowanie i korzystanie z portfela było niezwykle rygorystycznie nadzorowane:

- Wygenerowano go na laptopie „air-gapped” z systemem Linux i samodzielnie skompilowanym oprogramowaniem.

- Użyta została 24 wyrazowa fraza mnemoniczna zgodnie BIP-39.

- Frazę mnemoniczną została bezpiecznie wprowadzona do portfeli sprzętowych Ledger i Trezor.

- Nadano bezpieczne kody PIN i fizycznie zabezpieczono portfele sprzętowe.

- Frazę mnemoniczną nigdy nie została wprowadzona do komputera.

- Kopia zapasowa frazy mnemonicznej została dobrze zabezpieczona.”

Badacze, analizując tę podatność<sup>25</sup>, wskazali, że proces generowania seed phrase, który powinien być oparty co najmniej na Cryptographically Secure Pseudo Random Number Generator (CSPRNG)<sup>26</sup>, w rzeczywistości wykorzystywał pseudo-random number generator (PRNG) oparty na algorytmie Mersenne Twister (MT19937). Co gorsza, w procesie inicjalizacji tego generatora zastosowano jedynie 32-bitową wartość czasu systemowego jako ziarno. Taki sposób generowania losowości znacząco obniża poziom entropii seed i czyni go podatnym na ataki brute force.

Algorytm MT19937, będący implementacją generatora liczb pseudolosowych Mersenne Twister, nie spełnia wymagań stawianych kryptograficznie bezpiecznym

---

<sup>22</sup> Zob. <https://github.com/pointbiz/bitaddress.org>, zarchiwizowany na <https://perma.cc/E4LD-SBFP>.

<sup>23</sup> Zob. <https://github.com/pointbiz/bitaddress.org/issues/291>, zarchiwizowany na <https://perma.cc/9X TL-6YRA>. Podnosi się w tym kontekście zasadnie, że jednym z najbezpieczniejszym i najbardziej losowym sposobem jest rzut monetą 256 razy przydając, np. dla reszki wartość 1, a dla orła 0 oraz zapisanie tej liczby binarnie.

<sup>24</sup> Zob. <https://perma.cc/FR95-RMMP>.

<sup>25</sup> Nazwaną „Milk Sad”. Były to pierwsze dwa słowa z pierwszej frazy seed w procesie generowania złamanego klucza.

<sup>26</sup> Kryptograficznie bezpiecznego generatora liczb pseudolosowych.

generatorom liczb pseudolosowych (CSPRNG), ponieważ jego wewnętrzny stan może zostać odtworzony przez osobę trzecią, o ile pozna ona dostateczną liczbę wyjściowych wartości generowanych przez algorytm. Kluczowym ograniczeniem MT19937 w kontekście bezpieczeństwa kryptograficznego jest sposób inicjalizacji. Standardowo wykorzystuje on 32-bitowe ziarno, co daje  $2^{32}$  możliwych stanów początkowych. Taka niewielka liczba stanów początkowych znacząco obniża entropię procesu generowania, co w praktyce umożliwia przeprowadzenie skutecznego ataku brute force, nawet przy użyciu „domowego” sprzętu komputerowego.

Ze względu na te ograniczenia, MT19937 nie jest zalecany do zastosowań kryptograficznych, gdzie wymagana jest wysoka nieprzewidywalność i odporność na analizy statystyczne. W takich przypadkach należy stosować kryptograficznie bezpieczne generatory liczb pseudolosowych (CSPRNG), które zapewniają wyższy poziom bezpieczeństwa.

Zastosowanie MT19937 w kontekście wymagającym wysokiego poziomu bezpieczeństwa, takim jak generowanie kryptowalutowych kluczy prywatnych, stanowi poważne naruszenie zasad bezpieczeństwa kryptograficznego<sup>27</sup>. Jego deterministyczny charakter oraz podatność na odtworzenie stanu wewnętrznego na podstawie wyjściowych wartości sprawiają, że algorytm ten nie gwarantuje właściwego poziomu ochrony przed nieautoryzowanym dostępem do kluczy prywatnych i w konsekwencji do środków.

Analiza tego przypadku ujawniła analogiczny problem z portfelem „Cake Wallet”<sup>28</sup> i równoległe zgłoszoną w „Trust Wallet”<sup>29</sup> podatność CVE-2023-31290<sup>30</sup>, które pozwoliły przestępcom wytransferować z adresów ofiar kryptowaluty o wartości milionów dolarów<sup>31</sup>.

Z tego względu kluczowe jest stosowanie oprogramowania, które gwarantuje wysoki poziom transparentności w zakresie generowania entropii, weryfikacja źródeł stosowanych algorytmów oraz regularna aktualizacja narzędzi kryptograficznych. W sytuacjach krytycznych zaleca się również stosowanie sprzętowych generatorów liczb losowych (HWRNG) jako dodatkowego zabezpieczenia zapewniającego właściwy poziom entropii.

---

<sup>27</sup> Zob. <https://github.com/intel/pailliercryptolib/issues/2>, zarchiwizowany na <https://perma.cc/KJ8H-C5WD>.

<sup>28</sup> Zob. ogłoszenie twórców Cake Wallet na Reddit z fragmentem: „Prosimy o NATYCHMIASTOWE utworzenie nowych portfeli Bitcoin w wersji 4.1.7, a następnie przeniesienie środków ze starego portfela seed z 12 słowami do nowo utworzonego portfela seed z 24 słowami.” Zob. <https://perma.cc/R96G-UANC>.

<sup>29</sup> Ujawnioną przez Ledger Donjon. Zob. więcej na <https://www.ledger.com/blog/Funds-of-every-wallet-created-with-the-Trust-Wallet-browser-extension-could-have-been-stolen>, zarchiwizowany na <https://perma.cc/AHE8-RRSJ>.

<sup>30</sup> Zob. <https://nvd.nist.gov/vuln/detail/CVE-2023-31290>, zarchiwizowany na <https://perma.cc/C2VB-ELCP>.

<sup>31</sup> Zob. <https://www.investing.com/news/cryptocurrency-news/libbitcoin-vulnerability-leads-to-900k-theft-from-bitcoin-wallets-3152533>, zarchiwizowany na <https://perma.cc/ZBZ3-6XE9>; [https://www.reddit.com/r/Bitcoin/comments/158nyuo/mass\\_hacking\\_of\\_over\\_1000\\_bitcoin\\_accounts/](https://www.reddit.com/r/Bitcoin/comments/158nyuo/mass_hacking_of_over_1000_bitcoin_accounts/) (dostęp: 2025-01-12 21:00); <https://community.trustwallet.com/t/browser-extension-wasm-vulnerability-postmortem/750787>, zarchiwizowany na <https://perma.cc/XJ2Y-V46M>.

Powyższe uwagi i zagrożenia zestawień należy z alternatywnym do „papierowych portfeli” modelem „przechowywania” walut wirtualnych, jakim jest zgodnie z wytycznymi portfel sprzętowy (wytyczne wskazują tu urządzenia marki Ledger - Ledger Nano S Plus<sup>32</sup> i Ledger Nano X<sup>33</sup>). Wytyczne wskazują, że „Po nabyciu stosownego nośnika zajdzie konieczność wyznaczenia osoby, do zakresu obowiązków której należeć będzie administrowanie portfelem. (...) zasadne jest powierzenie powyższych obowiązków właściwemu dyrektorowi finansowemu lub głównemu księgowemu” oraz „należy dokonać jego konfiguracji oraz zainstalować aplikację Ledger Live, niezbędną do obsługi urzędnika, dostępną na oficjalnej stronie producenta”. Zalecane zarazem jest, aby „konfiguracja portfela sprzętowego powinna zostać przeprowadzona komisyjnie przy udziale kierownika jednostki, wyznaczonego administratora portfela oraz **w razie potrzeby specjalisty**. Przy czym należy uniemożliwić zapoznanie się z ustanowionymi kodami dostępowymi specjalistcie, jeśli będzie nim osoba spoza prokuratury. Cały przebieg procesu zakładania portfela zewnętrznego należy udokumentować stosownym protokołem konfiguracji nośnika”.

Zestawienie opisanego przez Distrust modelu tworzenia portfeli dokonywanego przez specjalistów w niemalże podręcznikowy sposób, który okazał się mimo wszystko podatny na atak, z modelem, w którym to liniowy prokurator, który niekoniecznie musi być ekspertem od technicznych meandrów systemów aktywów wirtualnych, ma podejmować odpowiednie czynności wraz z kierownikiem jednostki (także co do zasady nie informatykiem) i „w razie potrzeby” z pomocą specjalisty, uznać należy za skrajnie niewłaściwy. Niepodobna wskazać w jaki sposób osoby, które nie mają żadnego realnego przygotowania z zakresu funkcjonowania kryptoaktywów, w bezpieczny sposób mają tworzyć i konfigurować portfele kryptowalutowe, opierając się jedynie na „instrukcji”. Warty wskazania jest także fakt, że wytyczne raz jako domyślnego administratora portfela wskazują właściwego dyrektora finansowego lub głównego księgowego, a w innym miejscu stanowią, że w sytuacji „planowanego pozyskiwania waluty wirtualnej w toku prowadzonych postępowań, należy utworzyć indywidualny portfel zewnętrzny, w zależności od potrzeb papierowy bądź sprzętowy, służący do przetransferowania skonkretyzowanych środków i administrowany następnie w ramach danego śledztwa przez prokuratora - referenta”. Z kolei w dalszej części zasygnalizowane jest, że „jakkolwiek wyznaczenie osoby administrującej portfelem leży w gestii kierownika jednostki, zasadne jest powierzenie powyższych obowiązków właściwemu dyrektorowi finansowemu lub głównemu księgowemu”.

Wskazywany model poleca, bez żadnych dodatkowych zastrzeżeń, po skonfigurowaniu portfela „zainstalować aplikację Ledger Live, niezbędną do obsługi urzędnika, dostępną na oficjalnej stronie producenta”. Należy zwrócić uwagę na to, że

---

<sup>32</sup> Na dzień 26.12.2024 r. cena ok. 350 zł.

<sup>33</sup> Na dzień 26.12.2024 r. cena ok. 700 zł.

w aplikacji tej znajduwane były już podatności – o czym informował sam producent<sup>34</sup>. Także same urządzenia podatne były na ataki fizyczne wykorzystujące ekran OLED<sup>35</sup> czy Bluetooth<sup>36</sup>.

Za oczywiście wadliwe należy uznać twierdzenie dotyczące portfeli papierowych, iż „na jednym portfelu papierowym możliwe jest przechowywanie tylko jednej waluty wirtualnej, przy czym na portfelach papierowych można przechowywać tylko niektóre rodzaje kryptowalut”. Według jego autorów na tej samej kartce nie można zapisać np. ciągów:

KzDdstTA8jkM4GTRk8nRhYKu9XPDo7Yq1nbK6tT8khQZsJo5ueNy (klucz prywatny BTC<sup>37</sup>)

oraz

0x5716e8f57a37900ca0ec1f32a56525f8e28cee2a150434ab5f7e196b5e9452db (klucz prywatny ETH<sup>38</sup>).

Co więcej, w świetle wytycznych nie jest możliwym zapisanie na kartce klucza do większości kryptowalut, skoro „na portfelach papierowych można przechowywać tylko niektóre rodzaje kryptowalut”. Jest to oczywiście nieprawda a parafrazując znane powiedzenie, że papier wszystko przyjmie, z całą stanowczością stwierdzić trzeba, że na kartce można zapisać klucz/klucze/adresy dowolnych kryptowalut.

Interesujący w kontekście prowadzonych rozważań jest następujący fragment:

*„Podkreślenia wymaga również fakt, iż w przypadku ewentualnej konieczności przekazania dowodów lub zabezpieczenia majątkowego w postaci kryptowalut z aktem oskarżenia do Sądu, bez ich uprzedniej sprzedaży, prostsze i bardziej zasadne będzie przekazanie do Sądu całego portfela zewnętrznego.”*

Przez przekazanie portfela zewnętrznego do sądu, wytyczne rozumieją tu przekazanie portfela sprzętowego. Choć nie jest to sprecyzowane, to należy założyć, że takie przekazanie należałoby dokonać najpewniej z kluczami/PIN – ami, które będą warunkować dostęp do urządzenia. Z drugiej strony, zalecenia wskazują, iż po konfiguracji „zapisany PIN oraz seed należy niezwłocznie umieścić w osobnych kopertach, a następnie zdeponować wraz z Ledgerem w NBP jako depozyt wartościowy”, co sugeruje, że do sądu przekazane zostanie samo urządzenie, które realnie nie będzie miało jakiegokolwiek wartości, gdyż nie będzie można go nawet uruchomić.

---

<sup>34</sup> „Ledger wykrył exploit wykorzystujący Ledger Connect Kit w czwartek 14 grudnia 2023 roku. Ten exploit wstrzyknął złośliwy kod do DApps, które korzystały z Ledger Connect Kit, nakłaniając użytkowników EVM DApp do podpisywania transakcji, które drenują ich portfele”. Zob. <https://www.ledger.com/blog/security-incident-report>, zarchiwizowany na <https://perma.cc/66LJ-RSTC>. Celem wyjaśnienia dodać należy, że Ledger Connect Kit zapewnia fizyczne połączenie urządzenia Ledger z komputerem lub smartfonem, co umożliwia korzystanie z aplikacji Ledger Live.

<sup>35</sup> Zob. <https://support.ledger.com/article/360033473414-zd>, zarchiwizowany na <https://perma.cc/A7P3-QFY7?type=image>.

<sup>36</sup> Zob. <https://support.ledger.com/article/360034576433-zd>, zarchiwizowany na <https://perma.cc/R9BW-6RBV?type=image>.

<sup>37</sup> Dla adresu 1PhmDbukKsFqhN6ZtSsVWUsmteLU2Qt9zJ.

<sup>38</sup> Dla adresu 0x58c7bB5dcD2Fdc4e5cAc190E0384D6f953dE95E6.

Należy zauważyć, że wydanie organowi procesowemu portfela sprzętowego nie eliminuje ryzyka dokonania transferu środków przez osobę posiadającą dostęp do frazy odzyskiwania (seed phrase) lub klucza prywatnego. W konsekwencji sąd nie będzie miał technicznych możliwości zablokowania ewentualnego transferu środków zdeponowanych na adresie lub adresach powiązanych z przekazanym urządzeniem. Sfalsyfikować tym samym należy tezę dotyczącą złożonych w depozycie NBP portfeli sprzętowych i kopert, że *„pobranie nośnika z depozytu oraz jego fizyczne użycie konieczne będzie jedynie w momencie transferowania z niego środków”*. W przypadku, gdyby osoba zaangażowana w konfigurację portfela – na przykład nieuczciwy specjalista IT – zapamiętała frazę odzyskiwania lub przechowywała jej kopię, możliwe jest odtworzenie zawartości portfela na innym urządzeniu i przeprowadzenie nieautoryzowanych transakcji. Co więcej, nie istnieją narzędzia pozwalające jednoznacznie ustalić, czy dana transakcja została podpisana za pomocą oryginalnego klucza sprzętowego czy jego kopii.

Tym samym, przekazanie portfela sprzętowego do sądu jako formy zabezpieczenia majątkowego lub dowodu rzeczowego może być oceniane jako wysoce ryzykowne z punktu widzenia skuteczności ochrony samych środków. Może doprowadzić to do sytuacji, w której środki de facto pozostaną poza skuteczną kontrolą instytucji sądowej, co podważa sens i bezpieczeństwo tego rodzaju praktyki i czyni ją dla sądu niezwykle ryzykowną.

Wytyczne wskazują również, iż za *„dopuszczalną sytuację przechowywania zabezpieczonych dowodów w postaci kryptowalut na portfelu giełdowym wskazać można okoliczność, kiedy w toku postępowania zabezpieczono niszowe waluty wirtualne, których przechowywanie na portfelu zewnętrznym nie jest możliwe, ponieważ dostępne na rynku nośniki nie dają możliwości założenia odpowiedniego konta do przechowywania danego typu krypto waluty”*.

W tym kontekście warto jednak zauważyć, że oba polecane przez prokuraturę portfele sprzętowe, obsługują ponad 5500 monet i tokenów<sup>39</sup>. Zasadne jest zatem stwierdzenie, że w przypadku braku obsługi danego altcoina przez te urządzenia, istnieje wysokie prawdopodobieństwo, że kryptowaluta ta nie będzie również dostępna do przechowywania za pośrednictwem giełdy kryptowalut<sup>40</sup>.

Ponadto, uwzględniając potencjalne spektakularne wzrosty wartości niszowych kryptowalut, wyłączenie ich a priori ze strefy zainteresowania organów ścigania wydaje się nieuzasadnione z perspektywy celów postępowania karnego oraz skuteczności podejmowanych w jego ramach działań.

Za całkowicie niezrozumiałe uznać należy model, zgodnie z którym *„w zależności od ustalonego stanu faktycznego, należy rozważyć ewentualną zasadność założenia kilku portfeli papierowych czy nawet sprzętowych w jednej sprawie, np. osobno dla każdego z*

---

<sup>39</sup> Zob. <https://www.ledger.com/supported-crypto-assets> (dostęp: 2025-01-12 21:00).

<sup>40</sup> Największa giełda kryptowalut na świecie Binance ma w swojej ofercie ok. 350 kryptowalut.

*podejrzanych. Rozwiązanie to pozwoli na łatwiejsze procedowanie z każdym z dowodów z osobna, w tym na przekazywanie zabezpieczonych dowodów do sądu, bądź do postępowania wyłącznego itd.”.*

Tego rodzaju podejście, polegające na zakupie i konfiguracji osobnego portfela sprzętowego dla każdego z podejrzanych, wydaje się być nieuzasadnione z kilku powodów. Po pierwsze, jest to rozwiązanie nieoptymalne ekonomicznie, gdyż wiąże się z ponoszeniem wysokich kosztów zakupu urządzeń, których koszty oscylują na około kilkaset złotych za jednostkę. Po drugie, konfigurowanie wielu portfeli jest niezwykle czasochłonne i zwiększa ryzyko pomyłek podczas ich konfiguracji, zwłaszcza w przypadku generowania kilku, kilkunastu lub nawet kilkudziesięciu portfeli w ramach jednego postępowania. Po trzecie, model ten nie uwzględnia technologicznych możliwości oferowanych przez współczesne portfele sprzętowe, takie jak Ledger Nano X, które umożliwiają utworzenie wielu niezależnych portfeli w ramach jednego urządzenia. Ponadto, zastosowanie jednej z opcji oferowanych przez te urządzenia, tj. generowanie portfela deterministycznego (Hierarchical Deterministic Wallet, HD Wallet) pozwala na generowanie nieograniczonej liczby adresów, co eliminuje konieczność stosowania wielu fizycznych urządzeń.

Wytyczne w tym kontekście wskazują, iż „*co do zasady utworzone w prokuraturach regionalnych i okręgowych portfele „ogólne”, służyć powinny jedynie do czasowego przechowywania kryptowalut, zabezpieczonych w nagłych sytuacjach procesowych. W przypadku planowanego pozyskiwania waluty wirtualnej w toku prowadzonych postępowań, należy utworzyć indywidualny portfel zewnętrzny, w zależności od potrzeb papierowy bądź sprzętowy, służący do przetransferowania skonkretyzowanych środków i administrowany następnie w ramach danego śledztwa przez prokuratora - referenta, na co wskazano powyżej”.* Same transfery zaleca się przeprowadzać na komputerach, które „*powinny służyć wyłącznie do obsługi portfela sprzętowego i dokonywania transferu waluty wirtualnej. Niedopuszczalne jest dokonywanie na tych jednostkach jakichkolwiek innych operacji, jak również podpinanie do nich innych nośników czy instalowanie innego oprogramowania”.* Oznacza to, że mając na uwadze, iż w Polsce funkcjonuje obecnie 342 prokuratury rejonowe, 45 prokuratur okręgowych, 11 prokuratur regionalnych, to potencjalnie w każdej z nich powinien być dedykowany komputer przeznaczony wyłącznie na dokonywanie transferów kryptowalutowych, co także uznać należy za wysoce nieoptymalne.

Za całkowicie niezrozumiałe uznać należy twierdzenie, iż „*w toku dotychczas przeprowadzonych czynności testowych i weryfikacyjnych, nie potwierdzono bezpieczeństwa aplikacji Monero GUI<sup>41</sup>, niezbędnej do wygenerowania na Ledgerze adresu publicznego dla kryptowaluty Monero, a zatem nie jest zalecane tworzenie kont dla tej waluty cyfrowej”.*

---

<sup>41</sup> Zob. <https://github.com/monero-ecosystem/monero-GUI-guide/blob/master/monero-GUI-guide.md> zarchiwizowany na <https://perma.cc/8Z3Y-BRHS>.

Portfele Monero GUI oraz CLI<sup>42</sup> stanowią dwa oficjalne rozwiązania do zarządzania kryptowalutą Monero (XMR), różniące się interfejsem użytkownika i zakresem zastosowania. Portfel Monero GUI (Graphical User Interface) został zaprojektowany z myślą o użytkownikach preferujących graficzny interfejs, co czyni go bardziej przystępnym dla osób mniej zaawansowanych technicznie. Portfel Monero CLI (Command Line Interface) jest natomiast narzędziem dedykowanym bardziej doświadczonym użytkownikom, umożliwiającym pełną kontrolę nad operacjami w środowisku tekstowym. CLI ze względu na większą elastyczność pozwala na uruchamianie pełnego węzła Monero oraz konfigurację związanych z prywatnością i bezpieczeństwem. Trudno wyjaśnić, czemu wytyczne nie zalecają tworzenia portfeli akurat dla tej kryptowaluty, która z uwagi na swoje techniczne właściwości często bywa używana w działalności przestępczej, tj. handlu na rynkach darknetowych, wymuszenia z użyciem ransomware oraz unikania regulacji finansowych. Zwłaszcza, że Ledger posiada dedykowane rozwiązanie<sup>43</sup> umożliwiające powiązanie GUI Wallet z portfelem, uznając to oprogramowanie za bezpieczne. Oczywiście, podobnie jak w przypadku każdego oprogramowania, możliwe jest znalezienie podatności, jednak dotyczy się to każdego z opisywanych tu rozwiązań programowych, włącznie z Ledger Live, które wykorzystywane będzie do każdej transakcji<sup>44</sup>.

## PROPOZYCJE ZMIAN

- 1) Wytyczne błędnie utożsamiają adresy i portfele kryptowalutowe. Konieczne jest precyzyjne rozróżnienie tych pojęć: portfel przechowuje klucze prywatne, podczas gdy adres jest alfanumerycznym identyfikatorem w blockchain. Zaleca się użycie klasyfikacji custodial i non-custodial, by dokładnie określić model zarządzania środkami, oraz unikania terminu „adres publiczny”.
- 2) Wytyczne dopuszczają generowanie kluczy za pomocą serwisów internetowych, co jest poważnym błędem. Generowanie kluczy musi odbywać się w środowisku offline, w nadzorowany sposób z wykorzystaniem zweryfikowanego oprogramowania, by minimalizować ryzyko kompromitacji danych.
- 3) Wytyczne muszą uwzględnić możliwość dodania frazy „passphrase” jako dodatkowego zabezpieczenia przy tworzeniu seed phrase.
- 4) Wytyczne krytykują oprogramowanie Monero GUI, nie podając alternatyw dla obsługi tej niezwykle popularnej wśród przestępców waluty wirtualnej, nie wskazując też na wyższy stopień zagrożeń względem oprogramowań

---

<sup>42</sup> Zob. <https://www.getmonero.org/resources/user-guides/monero-wallet-cli.html>, zarchiwizowany na <https://perma.cc/YGP8-DPXJ>.

<sup>43</sup> Monero (XMR) Wallet App.

<sup>44</sup> Możliwym jest także wygenerowanie adresu Monero, bez użycia oprogramowania GUI lub CLI, korzystając z bibliotek lub narzędzi dostępnych w różnych programowania, które obsługują protokół Monero, jakkolwiek repozytoria te nie zostały zweryfikowane przez główny zespół Monero. Zob. <https://www.getmonero.org/resources/developer-guides/>, zarchiwizowany na <https://perma.cc/B7TM-KZ94>.

stosowanych względem innych walut wirtualnych. Należy wprowadzić procedury obsługi także niszowych kryptowalut.

- 5) Wytyczne proponują przeprowadzenie transferu środków z konta giełdowego podejrzanego przez prokuratora przy użyciu danych logowania, jeśli takowe otrzyma. Działanie takie jako naruszające obowiązujące przepisy, powinno zostać zastąpione wystosowaniem formalnego żądania do giełd celem zrealizowania zlecenia przelewu zgodnie z obowiązującymi przepisami.

Najważniejszą zmianą, jaka winna zostać dokonana w omawianym modelu działania, jest przemodelowanie koncepcji tworzenia samych portfeli (kluczy i adresów). W celu zapewnienia skutecznego, bezpiecznego pod względem informatycznym zabezpieczania kryptowalut w ramach postępowań karnych<sup>45</sup>, konieczne jest opracowanie ustandaryzowanego modelu zarządzania kluczami kryptograficznymi, który uwzględni specyfikę tych aktywów oraz wymagania organizacyjne i prawne prokuratury.

Prokuratura Krajowa powinna utworzyć zespół ds. zarządzania aktywami wirtualnymi, który będzie odpowiedzialny za wszelkie czynności związane z generowaniem kluczy kryptograficznych, konfigurację portfeli, zarządzanie aktywami oraz monitorowanie transakcji związanych z kryptowalutami w toku prowadzonych postępowań. Taki model organizacyjny minimalizuje ryzyko błędów technicznych wynikających z braku specjalistycznej wiedzy wśród prokuratorów liniowych i umożliwia ujednoczenie procedur na poziomie ogólnokrajowym. Generowanie kluczy kryptograficznych oraz zarządzanie portfelami powinno odbywać się wyłącznie w środowisku fizycznie odizolowanym (ang. air-gapped environment), a wszelkie transfery środków dokonywane muszą być ściśle audytowane i odbywać się na dedykowanym do tego komputerze połączonym z Internetem.

Proponowany model opiera się na centralizacji procesu generowania i zarządzania kluczami w wyspecjalizowanej jednostce Prokuratury Krajowej, przy jednoczesnym zastosowaniu portfeli deterministycznych (HD Wallets) oraz wielopodpisowych (multi-signature). Portfele deterministyczne (HD Wallets), umożliwiają bowiem generowanie nieskończenie wielu unikalnych adresów z jednego klucza nadrzędnego. Każdy adres mógłby być przypisywany do konkretnej sprawy, co zapewnia przejrzystość i kontrolę nad przepływem środków.

W przypadku zabezpieczania znacznych środków lub w sytuacjach szczególnego ryzyka zaleca się stosowanie portfeli wielopodpisowych (multi-signature) w modelu np. „3 z 5” czy „4 z 6”. Oznacza to, że do autoryzacji transakcji (np. sprzedaży czy zwrotu) wymagane będzie zaangażowanie co najmniej, np. trzech z pięciu/czterech z sześciu<sup>46</sup> osób posiadających klucze podpisowe<sup>47</sup>, co minimalizuje ryzyko nieautoryzowanego dostępu i zapewnia transparentność podejmowanych działań.

---

<sup>45</sup> Raz jeszcze podkreślić należy że sama dopuszczalność stosowania instytucji zabezpieczenia majątkowego względem kryptowalut rodzi bardzo poważne wątpliwości natury prawnej.

<sup>46</sup> Lub dowolnie innej konfiguracji.

<sup>47</sup> Którymi mogą być rzecz jasna portfele sprzętowe Ledger.

Wyeliminowanie konieczności zarządzania kryptowalutami przez prokuratorów liniowych, minimalizuje ryzyka, związane z błędami technicznymi, stosowanie portfeli multi-signature oraz redundancji w przechowywaniu fraz odzyskiwania chroni w zdecydowanie lepszy sposób przed utratą danych, a zaangażowanie kilku osób w autoryzację transakcji zapewnia nieporównywalnie wyższy poziom bezpieczeństwa samych środków.

W analogiczny sposób należałoby zmodyfikować sposób transferu środków, a punktem wyjścia do dalszych rozważań uczynić można model następujący:

**1. Zgłoszenie potrzeby zabezpieczenia**

Prokurator prowadzący sprawę składa telefonicznie/mailowo wniosek do zespołu o wygenerowanie dedykowanego adresu kryptowalutowego/adresów kryptowalutowych.

**2. Generowanie adresów i kluczy**

Zespół generuje adres w ramach portfela HD i przekazuje go prokuratorowi prowadzącemu. Adres ten jest przypisany wyłącznie do konkretnej sprawy/podejrzanego.

**3. Przechowywanie środków**

Po uzyskaniu kluczy prywatnych od podejrzanego lub z innego źródła, i przekazaniu ich bezpiecznym kanałem do zespołu, dokonuje on transferu środków na wygenerowany adres, eliminując konieczność angażowania prokuratorów liniowych w techniczne aspekty operacji.

**4. Przechowywanie fraz odzyskiwania**

Kopie zapasowe fraz odzyskiwania (seed phrase) lub same klucze prywatne powinny być przechowywane w bezpiecznych lokalizacjach, takich jak sejf Narodowego Banku Polskiego, lub Prokuratury Krajowej. W celu zapewnienia najwyższego poziomu bezpieczeństwa redundancji zalecane byłoby zastosowanie algorytmu Shamir's Secret Sharing, dzielącego frazę na kilka części, z których tylko część jest wymagana do ich odtworzenia<sup>48</sup>.

---

<sup>48</sup> Np. na 5 udziałów z których 3 są wymagane aby odtworzyć frazę. Nie chodzi tu bynajmniej o to aby np. w 2 lokalizacjach zabezpieczyć po 12 słów w każdej. Podział frazy odzyskiwania na części (np. 12/12 słów) jest ryzykowny, ponieważ każda część zawiera istotną część informacji o całej frazie, co zwiększa podatność na ataki *brute force*, a utrata jednej części uniemożliwia odzyskanie klucza. W przeciwieństwie do tego, Shamir's Secret Sharing (SSS) dzieli frazę na udziały, z których każdy jest matematycznie niezależny i nie ujawnia żadnych informacji o frazie, zapewniając jednocześnie redundancję dzięki możliwości odtworzenia klucza przy zgromadzeniu minimalnej liczby udziałów. SSS eliminuje ryzyko utraty dostępu do klucza w przypadku awarii jednego miejsca przechowywania i oferuje znacznie wyższy poziom bezpieczeństwa kryptograficznego.

## BIBLIOGRAFIA

1. Behan A., Waluty wirtualne jako przedmiot przestępstwa, Krakowski Instytut Prawa Karnego Fundacja, Kraków 2022
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dn. 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE; Dz.U. UE L 156/43 z 2018 r.
3. <https://community.trustwallet.com/t/browser-extension-wasm-vulnerability-postmortem/750787>
4. <https://github.com/intel/pailliercryptolib>
5. <https://github.com/monero-ecosystem/monero-GUI-guide/blob/master/monero-GUI-guide.md>
6. <https://github.com/pointbiz/bitaddress.org>
7. <https://nvd.nist.gov/vuln/detail/CVE-2023-31290>
8. <https://perma.cc/R96G-UANC>
9. <https://support.ledger.com/article/360033473414-zd>
10. <https://support.ledger.com/article/360034576433-zd>
11. <https://www.getmonero.org/resources/developer-guides/>
12. <https://www.getmonero.org/resources/user-guides/monero-wallet-cli.html>
13. <https://www.investing.com/news/cryptocurrency-news/libbitcoin-vulnerability-leads-to-900k-theft-from-bitcoin-wallets-3152533>
14. <https://www.ledger.com/blog/Funds-of-every-wallet-created-with-the-Trust-Wallet-browser-extension-could-have-been-stolen>
15. <https://www.ledger.com/blog/security-incident-report>
16. <https://www.ledger.com/supported-crypto-assets>
17. [https://www.reddit.com/r/Bitcoin/comments/158nyuo/mass\\_hacking\\_of\\_over\\_1000\\_bitcoin\\_accounts/](https://www.reddit.com/r/Bitcoin/comments/158nyuo/mass_hacking_of_over_1000_bitcoin_accounts/)
18. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów oraz zmiany dyrektywy (UE) 2015/849 (Dz. U. UE. L. z 2023 r. Nr 150, str. 1)
19. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (Dz. U. UE. L. z 2023 r. Nr 150, str. 40 z późn. zm.)
20. Walker G., Mnemonic Seed. Encoding a Random Number in to Words And Using Them to Create a Seed, <https://perma.cc/2GDX-EZSA>
21. Wytyczne Prokuratury Krajowej 1001-12.024.4.2023 z dnia 25 maja 2023 r.

# OSZUSTWA Z WYKORZYSTANIEM TOKENÓW PODSZYWAJĄCYCH SIĘ POD POPULARNE KRYPTOAKTYWA

SCAMS INVOLVING TOKENS IMITATING POPULAR CRYPTO-ASSETS

Aleksandra SZYNCZEWSKA <sup>1</sup>, Szymon JASIŃSKI <sup>2</sup>

**Streszczenie:** Stosunkowo nowym zjawiskiem w kontekście cyberprzestępstw są oszustwa z wykorzystaniem tokenów podszywających się pod popularne kryptoaktywa. W niniejszej publikacji autorzy skupili się na przedstawieniu tego rodzaju zagrożenia, w szczególności mając na uwadze łatwość stworzenia fałszywego tokena przy wykorzystaniu darmowych instrukcji i narzędzi dostępnych w Internecie. Autorzy podjęli próbę opisanego trzech konkretnych przypadków oszustw, w których tokeny podszywające się pod inne autentyczne projekty kryptowalutowe odegrały kluczową rolę. W pracy wskazano także praktyczne wskazówki dotyczące tego, jak zidentyfikować fałszywy token.

**Słowa kluczowe:** podszywanie się pod kryptoaktywa, fałszywy token, cyberprzestępczość, kryptoaktywa.

**Summary:** A relatively new phenomenon in the context of cybercrime are scams involving tokens impersonating popular crypto-assets. In this publication, the authors focused on presenting this type of threat, particularly bearing in mind the ease of creating a fake token using free instructions and tools available on the Internet. The authors attempted to describe three specific fraud cases in which tokens impersonating other authentic cryptocurrency projects played a crucial role. The article also provides practical guidelines on how to identify a fake token.

**Keywords:** crypto-assets, crypto-asset impersonation, fake token, cybercrime.

## WPROWADZENIE

Zjawisko „podszywania się” jest powszechnie znane w kontekście różnego rodzaju oszustw, w tym tych z wykorzystaniem kryptoaktywów. Jest to technika stosowana przez sprawców, która może przybierać rozmaite formy. Jak wskazano w „2023 Cryptocurrency Fraud Report”, który opublikowany został przez Internet Crime Compliant Center (IC3), działające jako oddział Federalnego Biura Śledczego, w 2023 r. „oszustwa związane z call

---

<sup>1</sup> zondacrypto, aszynczewska@gmail.com.

<sup>2</sup> zondacrypto, szymon.jasinski.kontakt@gmail.com.

center, w tym te związane z obsługą techniczną/klientów i z podszywaniem się pod rząd, stanowiły około 10 procent strat związanych z kryptowalutami<sup>3</sup>”. Choć termin ten, według „Słownika języka polskiego PWN”, odnosi się do „podawania się fałszywie za kogoś”<sup>4</sup>, to niniejsza praca koncentruje się na relatywnie nowym zjawisku, jakim jest podszywanie się pod kryptoaktywa. Oszustwo to, w ogólnym ujęciu, polega na stworzeniu tokena, który z pozoru przypomina istniejący, dobrze znany projekt, jak na przykład Tether (USDT), ale który w rzeczywistości nie reprezentuje żadnej wartości. Takie tokeny mogą być następnie wykorzystywane przez sprawców w celach osiągnięcia korzyści majątkowych, przykładowo poprzez ich sprzedaż nieświadomym inwestorom, którzy są przekonani co do tego, że mają do czynienia z autentycznym kryptoaktywem.

Obecnie nie istnieje wiele analiz czy opracowań poświęconych oszustwom z wykorzystaniem tokenów podszywających się pod popularne kryptoaktywa, jednak jest to zjawisko, które stopniowo zaczyna przyciągać coraz większą uwagę. Warto zauważyć, że przed tzw. *Cryptocurrency Token Impersonation Scam* w kwietniu 2024 r. przestrzegало Federalne Biuro Śledcze (FBI). FBI wydało wówczas ostrzeżenie dotyczące tego zagrożenia, opisując przypadek ofiary, która w jego wyniku straciła środki o wartości 2,1 mln USD<sup>5</sup>. Publikacja stanowi dowód na to, że proceder wykorzystywania fałszywych kryptoaktywów, przede wszystkim stablecoinów (których wartość ma być ściśle powiązana np. z konkretną walutą fiducjarną), staje się coraz większym problemem. Wybór stabilnych monet do tego celu może być podyktowany ich rosnącą popularnością. Jak wskazują dane, Tether odgrywa kluczową rolę w ekosystemie kryptoaktywów, zajmując trzecie miejsce, jeśli chodzi o dominację rynkową, zaraz po BTC oraz ETH<sup>6</sup>. Stablecoiny coraz częściej są przedmiotem zainteresowania uczestników rynku kryptoaktywów, w tym także cyberprzestępców. Według „The 2024 Crypto Crime Report” opublikowanego przez firmę Chainalysis, do 2021 r. to Bitcoin pozostawał preferowaną kryptowalutą wśród przestępców, co wynikało najprawdopodobniej z jego wysokiej płynności. Sytuacja uległa jednak zmianie i w ostatnich latach to stablecoiny stanowiły większość całkowitego wolumenu nielegalnych transakcji<sup>7</sup>. Należy podkreślić, że zmiana ta idzie w parze ze wzrostem udziału stabilnych monet w całkowitej aktywności kryptowalutowej na świecie, obejmującej także działania legalne. Niemniej, krajobraz ten może ulegać zmianom w najbliższym czasie z uwagi na wejście w życie europejskiego rozporządzenia MiCA (*Markets in Crypto-Assets*). Wspomniany akt prawny reguluje rynek m.in. w zakresie tokenów będących e-pieniądzem, czyli kryptoaktywów, które mają utrzymywać stabilną wartość dzięki temu, że są powiązane z jedną walutą

---

<sup>3</sup> 2023 Cryptocurrency Fraud Report, Internet Crime Compliant Center (IC3), FBI, s. 3

<sup>4</sup> <https://sjp.pwn.pl/slowniki/podszywac%20sie.html>, dostęp: 28.10.2024

<sup>5</sup> <https://www.fbi.gov/contact-us/field-offices/denver/news/fbi-warns-of-cryptocurrency-token-impersonation-scam>, dostęp: 19.10.2024

<sup>6</sup> <https://coinmarketcap.com/charts/#bitcoin-dominance>, dostęp: 20.10.2024

<sup>7</sup> The 2024 Crypto Crime Report, Chainalysis, s. 7

urzędową<sup>8</sup> (jak przykładowo USDC<sup>9</sup> powiązane z ceną dolara amerykańskiego). Zgodnie z przepisami rozporządzenia emitenci tego typu tokenów, by móc dopuszczać je do obrotu w Unii Europejskiej, muszą posiadać zezwolenie na prowadzenie działalności jako instytucja kredytowa lub instytucja pieniądza elektronicznego oraz zgłosić dokument informacyjny dotyczący danego kryptoaktywa i opublikować go zgodnie z niniejszym rozporządzeniem<sup>10</sup>. Powyższe może znacząco wpłynąć na liczbę użytkowników stablecoinów w UE, ponieważ kryptoaktywa niespełniające wymagań określonych w MiCA, nie będą mogły być udostępniane do obrotu dla klientów z Europejskiego Obszaru Gospodarczego.

Prostota tworzenia tokenów kryptowalutowych może być dużym ułatwieniem dla cyberprzestępców w kontekście podszywania się pod istniejące, popularne kryptoaktywa. Warto jednak zaznaczyć, że tego typu fałszywe tokeny są możliwe do zidentyfikowania poprzez zwrócenie uwagi na kilka kluczowych aspektów, które zostały przedstawione przez autorów w dalszej części artykułu.

## MONETA KRYPTOWALUTOWA A TOKEN

Kryptoaktywo, według definicji zawartej w rozporządzeniu MiCA, „oznacza cyfrowe odzwierciedlenie wartości lub prawa, które da się przemieścić i przechowywać w formie elektronicznej z wykorzystaniem technologii rozproszonego rejestru lub podobnej technologii”<sup>11</sup>. W zakres owej definicji wchodzi zatem zarówno różnego rodzaju tokeny, jaki i monety kryptowalutowe. Aby jednak rozwiać ewentualne niejasności co do znaczenia terminu „token” w kontekście kryptoaktywów, który jest przedmiotem niniejszej publikacji, zasadnym jest podjęcie próby jego zdefiniowania. W tym celu jako najbardziej trafne jawi się porównanie go z monetą kryptowalutową. Bazując na dostępnych źródłach wydaje się, że w pierwszej kolejności należy zwrócić uwagę na takie kwestie jak sieć blockchain, na której budowane są rzeczony aktywa cyfrowe oraz ich funkcjonalność.

Jeśli chodzi o monetę kryptowalutową, to jest ona zbudowana na własnym i niezależnym łańcuchu bloków. Przykładami takich monet są Bitcoin (BTC) - zbudowany na sieci Bitcoin, Ether (ETH) - funkcjonujący w sieci Ethereum, czy Litecoin (LTC) - działający w sieci Litecoin. Są to kryptoaktywa natywne dla konkretnego blockchaina, będące integralną częścią i główną walutą określonej sieci. Jeżeli zaś mowa o zastosowaniu monety kryptowalutowej, stanowi ona przede wszystkim środek płatniczy, jednostkę rozliczeniową we własnym łańcuchu bloków lub środek przechowywania wartości<sup>12</sup>.

---

<sup>8</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektywy 2013/36/UE i (UE) 2019/1937, s. 24 (art. 3, pkt 1)

<sup>9</sup> <https://www.circle.com/usdc>, dostęp: 28.10.2024

<sup>10</sup> Tamże, str. 68 (art. 48, pkt 1)

<sup>11</sup> Tamże, s. 24 (art. 3, pkt 1)

<sup>12</sup> <https://coinmarketcap.com/academy/article/coin-vs-token:-what-is-the-difference>, dostęp: 16.10.2024

Z kolei odnosząc się do tokena należy podkreślić, że jest on zbudowany na istniejącym już blockchainie i nie stanowi monety natywnej danej sieci<sup>13</sup>. Jako przykład może posłużyć Tether (USDT), który jest emitowany na różnych łańcuchach bloków, takich jak Ethereum czy Tron<sup>14</sup> lub Basic Attention Token (BAT), mogący działać w sieci Ethereum albo Solana<sup>15</sup>.

Tokeny, w zależności od ich funkcjonalności, rozróżnić można na kilka głównych rodzajów:

- użytkowe (*utility tokens*) - oferują określoną użyteczność. Służą one, m.in. do korzystania z usług lub funkcji w ramach konkretnego projektu. Takim tokenem jest wspomniany wyżej BAT, a posiadanie go daje prawo do używania go „jako środka do uzyskiwania dostępu do usług na platformie BAT oraz do umożliwienia korzystania z platformy i interakcji z nią”<sup>16</sup>;
- zarządzania (*governance tokens*) - zapewniają posiadaczom możliwość brania udziału w podejmowaniu kluczowych decyzji związanych m.in. ze zdecentralizowaną aplikacją (*dApp*). Na przykład UNI - token zarządzania dla zdecentralizowanej giełdy Uniswap, działającej na blockchainie Ethereum, pozwala posiadaczom na uczestnictwo w głosowaniach dotyczących przyszłych aktualizacji związanych ze sposobem jej działania<sup>17</sup>, a siła głosu jest rozłożona proporcjonalnie do salda tokenów UNI;
- bezpieczeństwa (*security tokens*): reprezentują udziały własnościowe, m.in. w konkretnych firmach<sup>18</sup>. Przykładem może być RealToken powiązany z branżą nieruchomości, dający możliwość inwestowania w nie. Jest to aktywo będące reprezentacją udziałów w spółce, która jest właścicielem aktu własności danej nieruchomości<sup>19</sup>;
- niezamienne tokeny (*non-fungible tokens - NFT*): mogą być traktowane jako poświadczenie autentyczności i własności konkretnego aktywa, jak na przykład cyfrowa treść czy dzieło sztuki, które jest unikalne. Takim NFT są CryptoPunks, czyli 10 000 unikalnych, wygenerowanych postaci z dowodem własności zarejestrowanym w blockchainie Ethereum<sup>20</sup>;
- stablecoiny: „to unikalna kategoria tokenów zaprojektowanych w celu utrzymania stabilnej wartości w stosunku do określonego aktywa lub zestawu

---

<sup>13</sup> <https://www.ledger.com/academy/crypto/what-is-the-difference-between-coins-and-tokens>, dostęp: 16.10.2024

<sup>14</sup> <https://tether.to/en/supported-protocols/>, dostęp: 15.10.2024

<sup>15</sup> <https://basicattentiontoken.org/faq/>, dostęp: 15.10.2024

<sup>16</sup> Tamże, dostęp: 18.10.2024

<sup>17</sup> <https://app.uniswap.org/explore/tokens/ethereum/0x1f9840a85d5af5bf1d1762f925bdaddc4201f984> dostęp: 17.10.2024

<sup>18</sup> <https://www.ledger.com/academy/fungible-token-categories-explained>, dostęp: 20.10.2024

<sup>19</sup> <https://faq.realt.co/en/article/what-is-realt-who-can-invest-how-do-i-invest-1yyc5h5/>, dostęp: 18.10.2024

<sup>20</sup> <https://cryptopunks.app/>, dostęp: 18.10.2024

*aktywów, takich jak waluty fiducjarne, surowce lub inne kryptoaktywa”<sup>21</sup>.  
Przykładem może być wspomniany wcześniej Tether czy USD Coin.*

## **LATWOŚĆ TWORZENIA TOKENÓW I ZAGROŻENIA Z TYM ZWIĄZANE**

Możliwość i łatwość tworzenia tokenów przyczynia się do rozwoju ekosystemów blockchain i walut wirtualnych oraz umożliwia innowacje. Niemniej, wiąże się ona również z pewnymi zagrożeniami z tym związanymi. Warto zwrócić uwagę na oszustwo typu *rug pull*, możliwe do przeprowadzenia przy stosunkowo małym nakładzie pracy w kontekście stworzenia tokena będącego przedmiotem oszustwa. Polega ono na zainicjowaniu projektu kryptowalutowego przez dewelopera, pozyskaniu inwestorów poprzez obietnicę dużego wzrostu jego wartości, a następnie porzuceniu przedsięwzięcia przez twórcę i zniknięciu wraz z zebranymi środkami, jednocześnie pozostawiając użytkowników z pozbawionym wartości cyfrowym aktywem<sup>22</sup>.

Tokeny działają w większości sieci kryptowalutowych, takich jak Bitcoin, Ethereum, Binance Smart Chain, Arbitrum, Solana, stąd też przy ich tworzeniu nie ma potrzeby koncentrowania się wyłącznie na jednej konkretnej. Do tej pory najczęściej wybieraną siecią było Ethereum z racji swojej popularności. Jednak z uwagi na wysokie opłaty sieciowe coraz częściej korzysta się z rozwiązań warstwy drugiej, takich jak Polygon czy Arbitrum, oferujących znacznie niższe opłaty. Jako że są one zbudowane na bazie sieci Ethereum, to ich działanie, standardy tokenów i eksploratory bloków są jednakowe lub bardzo podobne.

Samodzielne tworzenie tokenów w najbardziej popularnym standardzie ERC-20<sup>23</sup> wymaga jedynie podstawowych umiejętności programistycznych. Poniżej przedstawiony został kod, który z wykorzystaniem ogólnodostępnej biblioteki OpenZeppelin, zawierającej gotowe implementacje standardów tokenów, generuje kontrakt o nazwie „TetherUSD\_token”. Wraz z utworzeniem kontraktu, wytwarzane są tokeny o nazwie TetherUSD oraz skrócie USDT w ilości 10 milionów jednostek i wysyłane na portfel twórcy kontraktu.

---

<sup>21</sup> <https://medium.com/@mayuko.kondo/emurgo-africa-2023-q1-report-ch-2-1-types-of-tokens-on-blockchain-998e0ad4a979#b9e4>, dostęp: 26.10.2024

<sup>22</sup> <https://www.chainalysis.com/blog/2021-crypto-scam-revenues/>, dostęp: 19.10.2024

<sup>23</sup> <https://eips.ethereum.org/EIPS/eip-20>, dostęp: 23.10.2024

```
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract TetherUSD_token is ERC20 {
    constructor(address owner) ERC20("TetherUSD", "USDT") {
        uint256 ownerSupply = 10000000 * (10 ** decimals());
        _mint(owner, ownerSupply);
    }
}
```

Rys. 1. Zrzut ekranu z środowiska programistycznego wraz z kodem tokena ERC20.  
Źródło: opracowanie własne

Istnieją również generatory online, z pomocą których tworzenie tokenów ERC-20 nie wymaga żadnej wiedzy technicznej, a same narzędzia zapewniają użytkownikowi bardzo prosty i przejrzysty interfejs. Co więcej, takie rozwiązania nie stosują żadnej walidacji nazw czy skrótów. Korzystając z nich, można zatem bez trudu stworzyć token o takiej samej nazwie, jak inny powszechnie znany projekt. Kluczową różnicą między korzystaniem z generatorów a narzędzi programistycznych jest cena. Te pierwsze często pobierają dodatkową opłatę, co zwiększa ostateczny koszt utworzenia tokena.

## Token Details

Enter token details and choose a network

**Token Type and Network**

Token Type \*  
StandardERC20

Choose a Token Type.

Network \*  
Ethereum - Mainnet

Choose a Network.

**Token details required fields**

Token Name \*  
Ether

A custom name for the token.

Token Symbol \*  
ETH

A custom symbol for the token (usually 3-5 chars).

Token Decimals \*  
18

The decimal precision for the token (usually 18).

**Token supply required fields**

Initial Supply \*  
10000

The initial number of available tokens that will be created in your wallet.

Max Supply \*  
10000

The maximum number of tokens available.

**Token features**

- ERC20 Compliant
- Verified Source Code
- Remove Credits
- Customizable Decimals
- Supply Type  Fixed
- Access Type  None
- Burnable
- Mintable
- Reflection
- Taxable
- Permit
- Anti Whale Protection
- Liquidity Pool Setup
- Deflationary
- ERC1363
- Token Recover
- Transfer Type  Unstoppable

**Network** Mainnet

**Total** 0.07 ETH

I have read, understood and agreed to Token Generator's [Terms of Use](#).

**NEXT**

Rys. 2. Internetowy generator tokenów. Źródło: opracowanie własne, na podstawie [smartcontracts.tools/token-generator/](https://smartcontracts.tools/token-generator/)

Prostota tego procesu może stanowić zagrożenie związane z powstawaniem tokenów, które podszywają się pod istniejące, autentyczne wirtualne aktywa, jak przykładowo USDT czy ETH. Takie tokeny z pozoru mogą być łudząco podobne do prawdziwych aktywów cyfrowych, bowiem mogą występować pod tą samą nazwą - na przykład Tether (USDT). Jednakże w rzeczywistości nie będą one miały żadnej wartości, w przeciwieństwie do swoich oryginalnych odpowiedników. Samo oszustwo z użyciem fałszywych tokenów kryptowalutowych przyjmuje różne formy. Mogą one być wykorzystywane przez oszustów na wiele sposobów i do rozmaitych celów przestępczych, na przykład do phishingu, oszustw inwestycyjnych czy zatruwania adresów kryptowalutowych (tzw. *address poisoning*). W dalszej części niniejszego

artykułu zostaną opisane przykłady wszystkich trzech wyszczególnionych wyżej metod oszustw, przy jednoczesnym bliższym przyjrzeniu się sposobom działania sprawców.

## PHISHING Z WYKORZYSTANIEM PORTFELA ATOMIC WALLET

Jednym z przykładów ataku phishingowego w obszarze kryptowalut jest kampania wymierzona w użytkowników Atomic Wallet. Oszustwo ukierunkowane jest na osoby korzystające z tego portfela kryptowalutowego przy wykorzystaniu jego specyficznej właściwości. Polega ona na tym, że jeśli nazwa tokena pokrywa się z nazwą innego, bardziej popularnego wirtualnego aktywa, portfel automatycznie przyjmuje wartość rynkową tego oryginalnego.

Mechanizm tego oszustwa można opisać w kilku krokach. Pierwszym z nich jest rozsyłanie przez oszustów fałszywych wiadomości e-mail, w których podszywają się pod instytucje zaufania publicznego lub wsparcie techniczne Atomic Wallet. W treści wiadomości informują ofiarę o rzekomym uzyskaniu znacznej kwoty w tokenach kryptowalutowych, co ma na celu wzbudzenie zainteresowania i „złowienie” potencjalnej ofiary.

From: Atomic Finance <teamsupport@atomicwallet.org>  
Date: Thu, Feb 23, 2023 at 7:22 PM  
Subject: Wallet Activation!  
To: [REDACTED]

Hello [REDACTED],

### Congratulations!

Your wallet has been successfully created under your name, due to that - an amount of **123.25 ETH (\$205,942.59)** will be linked to your wallet address once you complete the wallet activation.  
**0x666df8911Cd94504C5FA2FB310F87d2498fBf124**

Please complete an authorization of **1.455 ETH** in order to authorize your wallet - and in order to link between the accounts.

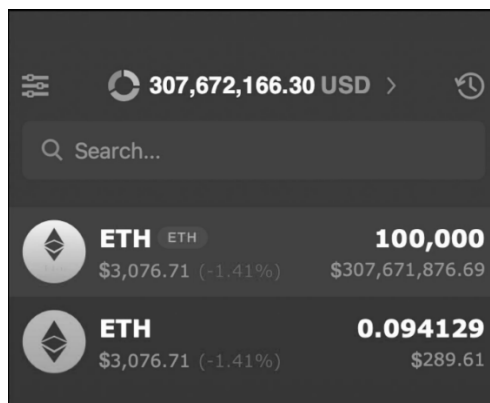
PS

The authorization process is imminent for the funds to be cleared to your account, only once the authorization is complete the ownership of the funds will be set to your name and you will be able to withdraw the entire amount, including the funds you have authorized.

Rys. 3. Wiadomość e-mail od oszustów.

Źródło: <https://support.atomicwallet.io/article/342-wallet-setup-scam>

W kolejnym kroku, po złapaniu ofiary, przestępcy przekazują jej dostęp do portfela kryptowalutowego, poprzez udostępnienie jej tzw. *seed phrase* (czyli zestawu 12-24 wyrazów, umożliwiających odtworzenie kluczy prywatnych do portfela). Zdarzają się również sytuacje, w których oszuści zakładają portfel wspólnie z pokrzywdzonym. W tym celu używają oprogramowania umożliwiającego zdalny dostęp do urządzenia pokrzywdzonego, dzięki czemu mają bezpośredni wgląd we frazy *seed* nadawane podczas konfiguracji, a co za tym idzie - pełny dostęp do portfela. Na portfelu, który można odtworzyć z przesłanej przez oszustów frazy *seed*, znajdują się już przedstawione w mailu tokeny. W przypadku tworzenia go wspólnie z ofiarą, środki są często przesyłane zaraz po skonfigurowaniu go. Należy zaznaczyć, że nie są to środki w oryginalnej monecie kryptowalutowej, jaką jest Ether, lecz w tokenie, który podszywa się pod nią. Mimo tego, że jest to fałszywy token, aplikacja Atomic Wallet wyświetla obok niego rzeczywistą cenę realnego aktywa ETH i podsumowanie całkowitej wartości.



Rys. 4. Widok fałszywego tokena EHT oraz prawdziwego ETH w aplikacji portfela. Źródło: opracowanie własne na podstawie aplikacji mobilnej portfela Atomic Wallet

Na powyższym rysunku zobaczyć można porównanie sposobu wyświetlania fałszywego oraz prawdziwego ETH na portfelu Atomic Wallet. Od góry, widoczny jest token podszywający się pod Ether, a poniżej - oryginalna moneta kryptowalutowa o tej samej nazwie. Po uzyskaniu przez ofiarę dostępu do portfela zawierającego bezwartościowe tokeny podszywające się pod prawdziwe ETH, ofiara nie jest w stanie ich wypłacić. Wynika to z faktu, że w sieci Ethereum do opłacania kosztów transakcji wykorzystywana jest moneta natywna, czyli Ether, której nie ma na saldzie portfela. Z tego powodu, w kolejnym kroku, oszuści zwracają się do ofiary z prośbą o dokonanie wpłaty - tzw. opłaty weryfikacyjnej w ETH. Po zdeponowaniu środków przez ofiarę, oszuści natychmiast je wypłacają. Nierzadko w portfelu pozostawiana jest jedynie niewielka ilość ETH, która ma pozwolić na pokrycie kosztu ewentualnego transferu fałszywych tokenów. Pozostawienie tej kwoty na saldzie ma na celu zminimalizowanie podejrzeń ofiary, co może skutkować wydłużeniem czasu wykrycia i zgłoszenia oszustwa<sup>24</sup>.

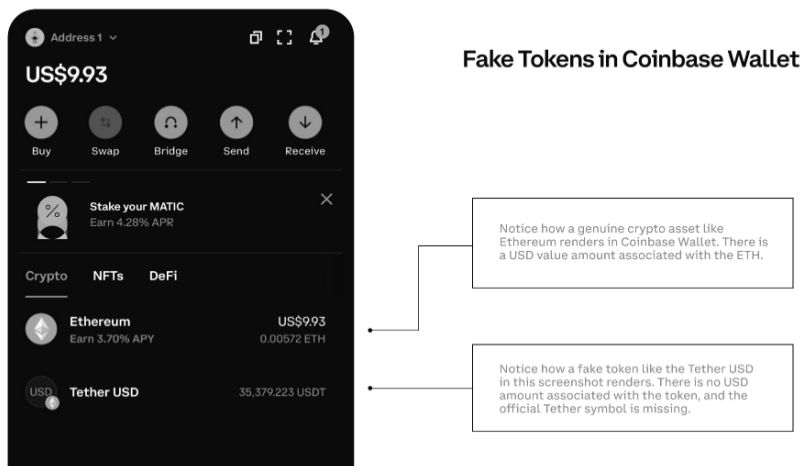
## OSZUSTWO INWESTYCYJNE Z WYKORZYSTANIEM PORTFELA COINBASE WALLET

Oszustwa inwestycyjne z wykorzystaniem kryptoaktywów są obecnie zjawiskiem powszechnym. W analizowanym przypadku schemat działania sprawców nie był jednak typowy, bowiem polegał na rzekomej zamianie środków zdeponowanych przez ofiarę na fałszywe tokeny, mające imitować te powiązane z autentycznym projektem. W celu zobrazowania mechanizmów i coraz bardziej wyrafinowanych metod stosowanych przez przestępców w przypadku, wydawać by się mogło, klasycznych oszustw inwestycyjnych,

<sup>24</sup> <https://support.atomicwallet.io/article/342-wallet-setup-scam/>, dostęp: 23.10.2024

poniżej przedstawiono przykład użytkownika, który padł ofiarą fałszywej platformy inwestycyjnej oraz wykorzystania tokena podszywającego się pod stablecoina.

Początek wyglądał dość standardowo - ofiara samodzielnie poszukiwała platformy, na której mogłaby zainwestować swoje środki. Gdy takową znalazła, udostępniła swoje dane kontaktowe w formularzu, a niedługo potem zadzwonił do niej „doradca”. Rzeczony doradca przekonał rozmówcę do zdeponowania środków na platformie, początkowo o równowartości 250 USD, a następnie większej kwoty. Osoba podająca się za brokera skontaktował się z użytkownikiem, informując o zyskach osiągniętych z obrotu wpłaconymi przez niego środkami. Jednocześnie przedstawiła kolejną niezwykłą okazję inwestycyjną, wymagającą jednak większego wkładu finansowego. Ofiara nie chcąc dokonywać kolejnych wpłat, zgodziła się na ofertę pożyczki ze strony doradcy, który wykorzystując techniki manipulacyjne, zapewniał o wysokich zwrotach z inwestycji. Warto zaznaczyć, że sprawcy udostępnił użytkownikowi podgląd rzekomo wygenerowanych zysków na fałszywej platformie. Kiedy użytkownik zdecydował się zakończyć inwestycję i zadeklarował zamiar przelania zarobionych środków na zewnętrzny portfel, oszuści zarekomendowali skorzystanie z Coinbase Wallet, na który, jak twierdzili, przenieśli zarobione środki i do którego udostępnił mu frazy *seed*. Istotne jest, aby podkreślić, że posiadając *seed phrase* przypisany do portfela kryptowalutowego, zyskuje się możliwość dowolnego dysponowania znajdującymi się na nim środkami. Użytkownik, nie mając tego świadomości, otworzył portfel i został poinformowany, że aby odblokować USDT widniejące na saldzie, konieczna jest spłata pozornie pożyczonych mu wcześniej środków o wartości 20 tys. dolarów. Dokonał transferu na rzecz oszustów, lecz podczas jego realizacji doszło do rzekomego błędu. W rezultacie, według sprawców, środki nie mogły zostać prawidłowo zaksięgowane na saldzie docelowym i konieczne było wykonanie drugiego przelewu na tę samą kwotę, co pokrzywdzony uczynił. W rzeczywistości była to udana próba wyłudzenia od niego większej ilości pieniędzy. Ostatecznie pozornie zarobione środki pojawiły się w portfelu, do którego użytkownik posiadał dostęp. Warto wspomnieć, że jeśli chodzi o Coinbase Wallet, w przeciwieństwie do opisywanego wcześniej Atomic Wallet, po dodaniu fałszywego tokena do portfela brak jest przy nim przeliczenia na walutę fiducyjną (jak jest to widoczne w przypadku kryptowaluty ETH, która przeliczona jest na dolary), a także brakuje oficjalnego logo Tethera (zob. Rys. 4). Są to elementy, na które należy zwrócić szczególną uwagę, aby zweryfikować, czy posiadane kryptoaktywo jest rzeczywiście tym, na które wstępnie wygląda.



Rys. 5. Fałszywy token w Coinbase Wallet.

Źródło: <https://help.coinbase.com/en/wallet/security/fake-stablecoins>

Ostatecznie ofiara zdecydowała się dokonać ich wypłaty na giełdę kryptowalutową, zaczynając od testowego przelewu 10 (fałszywych) USDT. Depozyt, z oczywistych względów, nie mógł zostać zaksięgowany na saldzie giełdowym, a po skontaktowaniu się z obsługą klienta użytkownik dowiedział się, że posiadane przez niego kryptoaktywa nie są prawdziwym Tetherem i nie mają żadnej realnej wartości. Oszustwo to doprowadziło do utraty całości zainwestowanych przez ofiarę środków, pozostawiając ją z ponad 50 tys. jednostek fałszywego tokena USDT. Opisany powyżej przypadek obrazuje powszechną praktykę tworzenia fałszywych platform inwestycyjnych wykorzystujących kryptoaktywa, jednakże z pewną modyfikacją działania sprawców. Nieoczywistym elementem było posłużenie się portfelem Coinbase Wallet do zapewnienia ofierze dostępu do rzekomo wygenerowanych zysków, które w rzeczywistości okazały się być tokenami podszywającymi się pod Tether.

## ZATRUVANIE ADRESU KRYPTOWALUTOWEGO

Zatrucie adresu (*address poisoning*) to rodzaj oszustwa wykorzystującego jawność danych transakcyjnych zawartych w blockchainie. Jego mechanizm jest stosunkowo prosty i zakłada chwilowy brak uwagi i czujności ze strony ofiary, a zaczyna się on od monitoringu łańcucha bloków przez sprawców. Skanując transakcje kryptowalutowe poszukują adresów, pomiędzy którymi dochodzi do regularnych transferów środków. Po ich wytypowaniu, oszuści najczęściej dokonują transferu z adresu przypominającego adres rzeczywistego odbiorcy z historii transakcji. W rezultacie, użytkownicy mogą nieświadomie skopiować fałszywy adres (tj. przypominający taki, z

którym wcześniej wchodził w interakcje) z historii, nie sprawdzając jego poprawności, przelewając środki bezpośrednio do portfela sprawcy<sup>25</sup>.

W najprostszych przykładach tego typu działań oszuści wykorzystywali losowo wygenerowane adresy do przeprowadzenia ataku. Z czasem, gdy realizowane przez nich operacje stawały się coraz bardziej zaawansowane, zaczęli używać tzw. *vanity generator*, który służy do tworzenia adresów zawierających konkretne znaki w określonych miejscach.



Rys. 6. Zrzut ekranu strony internetowej udostępniającej narzędzie *vanity generator*. Źródło: <https://vanity-eth.tk/>

Powyższy rysunek (Rys. 6) obrazuje, że możliwe jest stworzenie adresu zawierającego dowolny z zadeklarowanych znaków. Należy jednak zauważyć, że wraz ze wzrostem ich liczby rośnie stopień trudności wygenerowania takiego adresu, a zatem wydłuża się czas potrzebny na uzyskanie go. Stworzenie adresu, którego pierwsze i ostatnie znaki powtarzają się z tymi z portfela ofiary, zwiększa szanse oszustów, ponieważ większość eksploratorów blockchain domyślnie pokazuje tylko kilka pierwszych i kilka ostatnich znaków adresu, ukrywając jego środkową część.

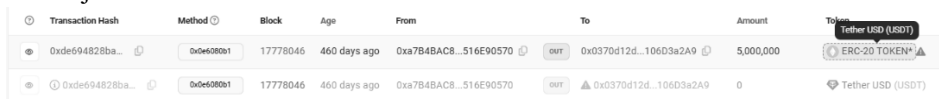
Transaction Hash	Method	Block	Age	From	To	Amount	Token
0x19a2e15547...	Transfer	19824906	172 days ago	0x1E227979...a6f538FD5	out 0xd9a1c378...244853a91	1,155.28802767	ERC-20: Wra...BTC
0x3374abc5a9...	Transfer	19789009	177 days ago	0x1E227979...a6f538FD5	out 0xD9A19256...e58853a91	1,155.28802767	Wrapped BTC (WBTC)

Rys. 7. Zrzut widoku transakcji pochodzącej z adresu wygenerowanego przy pomocy narzędzia *vanity generator* w eksploratorze bloków Etherscan. Źródło: <https://etherscan.io/>

Po utworzeniu adresu podobnego do tego, z którym wcześniej ofiara wchodziła w interakcje, oszuści dokonują transakcji o wartości zerowej lub bliskiej zeru. Głównym celem jest to, by adres stał się widoczny jako adres kontrahenta lub, w przypadku niektórych portfeli, został dodany do książki adresowej. Z biegiem czasu proces ten

<sup>25</sup> <https://www.chainalysis.com/blog/address-poisoning-scam/>, dostęp: 27.10.2024

ewoluował ze względu na fakt, że eksploratory bloków zaczęły ukrywać transakcje o zerowej wartości<sup>26</sup>.



Transaction Hash	Method	Block	Age	From	To	Amount	To
0xde694828ba...	0xde6080e1	17778046	460 days ago	0xa784BAC8...516E90570	out	0x0370d12d...106D3a2A9	5,000,000
0xde694828ba...	0xde6080e1	17778046	460 days ago	0xa784BAC8...516E90570	out	0x0370d12d...106D3a2A9	0

Rys. 8. Zrzut widoku transakcji o wartości zerowej oraz transakcją z wykorzystaniem fałszywego tokena w eksploratorze bloków Etherscan. Źródło: <https://etherscan.io/>

Z uwagi na powyższe, aby transakcja była widoczna w eksploratorze łańcucha bloków, sprawcy zaczęli tworzyć tokeny naśladujące inne popularne, jak na przykład w przypadku zobrazowanym na Rys. 7, podszywające się pod USDT. Pozwoliło im to na przesyłanie większych ilości tokenów, przez co transakcje nie są ukrywane w eksploratorze<sup>27</sup>. Po przesłaniu na adres ofiary kryptoaktywów imitujących te prawdziwe, oszuści liczą na moment nieuwagi użytkownika, w którym ten przypadkowo prześle swoje rzeczywiste środki na adres kontrolowany przez sprawców, kopiując go z historii transakcji.

## JAK ROZPOZNAĆ FAŁSZYWY TOKEN?

Różnice pomiędzy podszywającym się a oryginalnym tokenem zostały zaprezentowane na przykładzie sieci Etehreum i domyślnego eksploratora tego łańcucha bloków, jakim jest Etherscan. Warto podkreślić, że kilka z wymienionych różnic dotyczy również innych sieci. Kluczowe aspekty, na które należy zwrócić uwagę podczas weryfikacji tokena, zaznaczono na rysunku (zob. Rys. 8) i opisano poniżej.

Na Rys. 9 oryginalny token USDT pokazany został jako pierwszy od góry, a jego fałszywa wersja znajduje się niżej.

1. Najważniejszą informacją w przypadku tokenów jest adres kontraktu. Jest to 42-znakowy heksadecymalny ciąg znaków, który jest niepowtarzalny i wygląda podobnie do zwykłego adresu portfela<sup>28</sup>. Dokonując samodzielnej analizy można porównać go z adresem zawartym w dokumentacji projektu lub z adresem kontraktu podanym w agregatorach danych o kryptoaktywach, takich jak Coinpaprika czy Coingecko, które weryfikują te informacje.
2. Kolejnym ważnym punktem jest logo projektu oraz niebieski *checkmark* - w ten sposób oznaczane są projekty zweryfikowane przez eksplorator bloków i te o „dobrej reputacji”, co oznacza, że m.in. cele projektu są jasne i klarowne, dostępne są informacje o jego twórcach czy to, że token jest przedmiotem obrotu

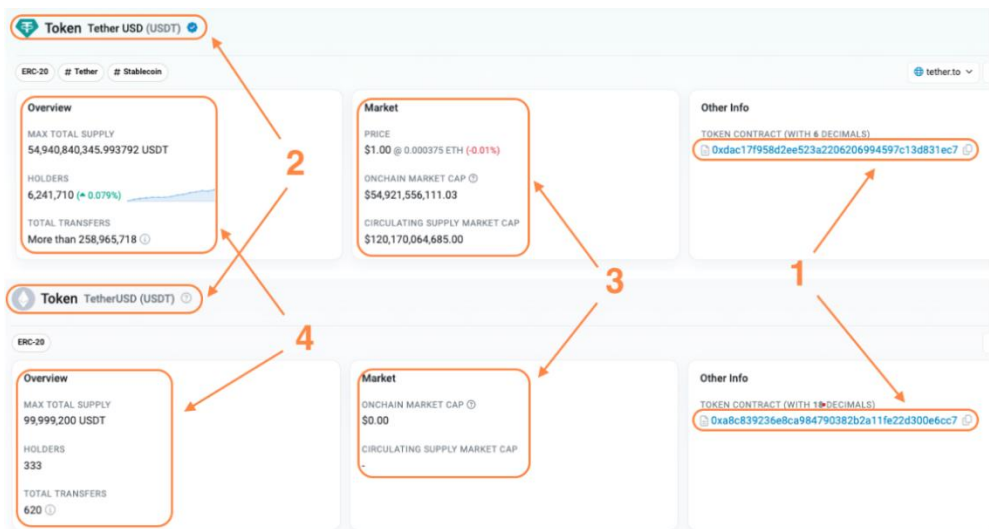
<sup>26</sup> <https://cointelegraph.com/news/etherscan-hides-zero-value-token-transfers-to-deter-address-poisoning-attacks>, dostęp: 28.10.2024

<sup>27</sup> <https://www.chainalysis.com/blog/address-poisoning-scam/>, dostęp: 23.10.2024

<sup>28</sup> <https://info.etherscan.com/what-is-an-ethereum-address/>, dostęp: 28.10.2024

na giełdach przeprowadzających weryfikację KYC<sup>29</sup>.

3. Warto również zwrócić uwagę na dane rynkowe, które wyświetlane są wówczas, gdy token jest przedmiotem obrotu na giełdzie kryptowalutowej. W przypadku fałszywych tokenów takich informacji nie będzie.
4. Ostatnim aspektem jest liczba transakcji związanych z danym tokenem oraz liczba posiadaczy - wartości te są zazwyczaj wysokie w przypadku tokenów istniejących na rynku od dłuższego czasu i cieszących się dużą popularnością. Niskie wartości tych wskaźników mogą natomiast wskazać na fałszywe tokeny lub projekty we wczesnych fazach rozwoju.



Rys. 9. Podgląd danych z eksploratora bloków Etherscan dotyczących tokena działającego w sieci Etehreum.

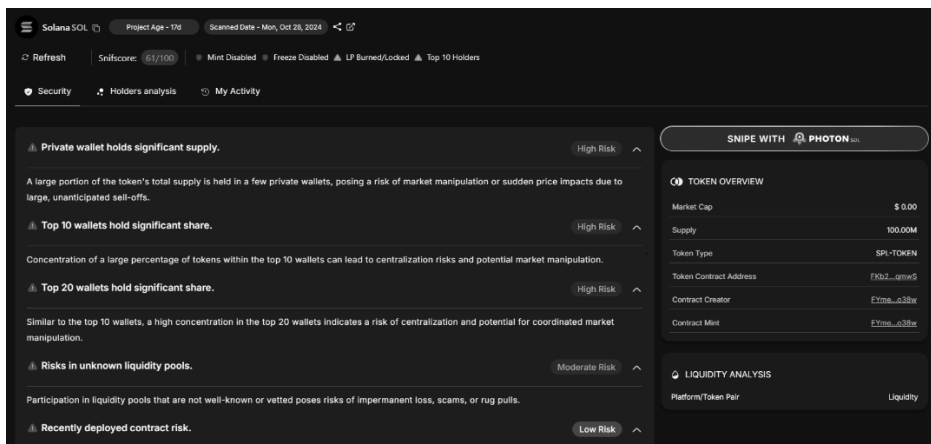
Źródło: opracowanie własne, na podstawie strony etherscan.io

Warto wspomnieć także o istnieniu narzędzi do badania i analizowania tokenów. Tak zwane „sniffery” to narzędzia, które analizują dane sieciowe, rynkowe i transfery. Dzięki zebranim danym są one w stanie ocenić, czy token jest autentyczny, czy też stanowi próbę oszustwa. Przykładem takiego narzędzia może być Solana Token Sniffer<sup>30</sup> lub Token Sniffer<sup>31</sup>.

<sup>29</sup> <https://info.etherscan.com/etherscan-token-reputation/>, dostęp: 27.10.2024

<sup>30</sup> <https://www.solsniffer.com/sniftokens>, dostęp: 28.10.2024

<sup>31</sup> <https://tokensniffer.com/>, dostęp 29.10.2024

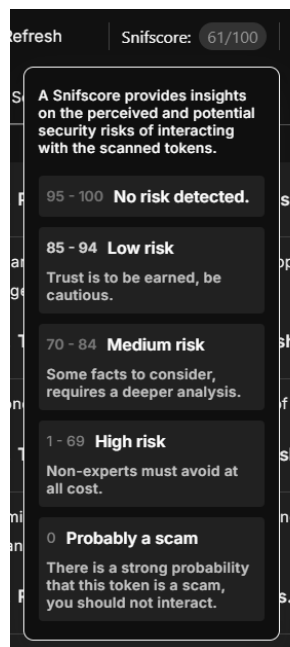


Rys. 10. Zrzut ekranu ukazujący analizę tokena w Solana Token Sniffer.

Źródło: opracowanie własne, na podstawie strony [solsniffer.com](https://solsniffer.com)

Narzędzie to zostało zaprojektowane przede wszystkim z myślą o analizie projektów kryptowalutowych i ich jakości w celu ułatwienia podjęcia decyzji dotyczących ewentualnych inwestycji w dany projekt. Ze względu na szeroki zakres przetwarzanych informacji, znajduje ono również zastosowanie w wykrywaniu oszustw. Rysunek 9 ilustruje przykład tokena o adresie `FKb27DJaTLkNBbC7vp9K02PZa3BA1on5mzLNZta7qmwS`, powstałego w sieci Solana i noszącego tę samą nazwę (SOL), którego celem jest naśladowanie natywnej monety tej sieci. Zgodnie z dokumentacją, narzędzie sprawdziło co najmniej 22 wskaźniki dla tego tokena, między innymi datę jego utworzenia, liczbę adresów, na których się znajduje oraz jego płynność. W związku z otrzymanymi wynikami, token uzyskał ocenę 61 na 100 punktów<sup>32</sup> (zob. Rys. 10), która wskazuje na to, że niedoświadczone osoby nie powinny wchodzić z nim w interakcje.

<sup>32</sup> <https://solsniffer.gitbook.io/solsniffer-user-guide/product-snif-tokens>, dostęp: 28.10.2024



Rys. 11. Zrzut ekranu ukazujący wynik analizy wraz ze skalą w Solana Token Sniffer. Źródło: opracowanie własne, na podstawie strony solsniffer.com

## PODSUMOWANIE

Celem niniejszego artykułu było przybliżenie stosunkowo nowego zjawiska wykorzystania tokenów podszywających się pod popularne kryptoaktywa do różnego rodzaju działań przestępczych. Każdy z opisanych w pracy przypadków obrazuje, jak metody stosowane przez cyberprzestępców, nawet w klasycznych schematach oszustw, takich jak phishing czy oszustwa inwestycyjne stale ewoluują. W publikacji zwrócono uwagę na to, że sprawcy potrafią wykorzystywać znajomość nowych rozwiązań technologicznych, a jednocześnie nieświadomość swoich ofiar, co umożliwia im uzyskanie znacznej przewagi. Dodatkowo, prostota tworzenia tokenów kryptowalutowych może być dużym ułatwieniem dla cyberprzestępców w kontekście podszywania się pod istniejące, popularne kryptoaktywa.

Należy jednak zaznaczyć, że takie fałszywe tokeny mogą zostać zidentyfikowane na podstawie kilku istotnych szczegółów, na które autorzy zwrócili uwagę. Opisywane w artykule przypadki podkreślają również znaczenie podejmowania świadomych i rozważnych decyzji inwestycyjnych związanych z kryptoaktywami, a także potrzebę ciągłego pogłębiania wiedzy w zakresie oszustw z nimi związanych.

## BIBLIOGRAFIA

1. Atomic Wallet, Wallet setup scam, <https://support.atomicwallet.io/article/342-wallet-setup-scam>
2. Atomic Wallet, Fake tokens: common questions, <https://support.atomicwallet.io/article/288-fake-tokens-common-questions#tokensniffer>
3. Buterin V., Vogelsteller F., ERC-20: Token Standard, <https://eips.ethereum.org/EIPS/eip-20>
4. Chainalysis, The Biggest Threat to Trust in Cryptocurrency: Rug Pulls Put 2021 Cryptocurrency Scam Revenue Close to All-time Highs, <https://www.chainalysis.com/blog/2021-crypto-scam-revenues/>
5. Chainalysis, Anatomy of an Address Poisoning Scam, <https://www.chainalysis.com/blog/address-poisoning-scam/>
6. Chainalysis, The 2024 Crypto Crime Report
7. Circle, MiCA USDC White Paper, <https://www.circle.com/legal/mica-usdc-whitepaper>
8. Coinbase Wallet, *Protect against fake stablecoins*, <https://help.coinbase.com/en/wallet/security/fake-stablecoins>
9. Cryptoslav I., *Coin vs Token: What Is the Difference?*, <https://coinmarketcap.com/academy/article/coin-vs-token-what-is-the-difference>
10. Etherscan, *Etherscan Token Reputation*, <https://info.etherscan.com/etherscan-token-reputation/>
11. Etherscan, *What is an Ethereum Address?*, <https://info.etherscan.com/what-is-an-ethereum-address/>
12. Federal Bureau of Investigation (Internet Crime Compliant Center), 2023 Cryptocurrency Fraud Report
13. <https://app.uniswap.org/explore/tokens/ethereum/0x1f9840a85d5af5b1d1762f925bdaddc4201f984>
14. <https://basicattentiontoken.org/faq/>
15. <https://coinmarketcap.com/charts/#bitcoin-dominance>
16. <https://cryptopunks.app/>
17. <https://faq.realt.co/en/article/what-is-realt-who-can-invest-how-do-i-invest-1yyc5h5/>
18. <https://sjp.pwn.pl/slowniki/podczywa%C4%87%20si%C4%99.html>
19. <https://www.circle.com/usdc>
20. Kondo M., *Types of Tokens on Blockchain*, <https://medium.com/@mayuko.kondo/emu-rgo-africa-2023-q1-report-ch-2-1-types-of-tokens-on-blockchain-998e0ad4a979#b9e4>
21. Ledger, *Crypto Coins and Tokens: Their Use-Cases Explained*,

- <https://www.ledger.com/academy/crypto/what-is-the-difference-between-coins-and-tokens>
22. Ledger, *Crypto Tokens: Utility, Governance and Security Tokens Explained*, <https://www.ledger.com/academy/fungible-token-categories-explained>
  23. Migoya V., *FBI Warns of Cryptocurrency Token Impersonation Scam*, <https://www.fbi.gov/contact-us/field-offices/denver/news/fbi-warns-of-cryptocurrency-token-impersonation-scam>
  24. OpenZeppelin, *openzeppelin-contracts*, v5.0.2, <https://github.com/OpenZeppelin/openzeppelin-contracts>
  25. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937
  26. Sun Z., *Etherscan hides zero-value token transfers to deter address-poisoning attacks*, <https://cointelegraph.com/news/etherscan-hides-zero-value-token-transfers-to-deter-address-poisoning-attacks>
  27. Tether, *Fiat currencies on the Bitcoin blockchain*, <https://assets.ctfassets.net/vyse88cgw-fbl5UWgHMvz071t2Cq5yTw5vi/c9798ea8db99311bf90ebe0810938b01/TetherWhitePaper.pdf>
  28. Tether, *Supported Protocols and Integration Guidelines*, <https://tether.to/en/supported-protocols/>

# RADIO FORENSICS - NETWORK ANALYSIS USING (IN)EXPENSIVE HARDWARE AND WIFI 6/6E/7 REVOLUTION

dr Zbigniew JAKUBOWSKI<sup>1</sup>, Grzegorz MARCZAK<sup>2</sup>  
Compendium Educational Center

**Streszczenie:** W poprzednim wystąpieniu skoncentrowaliśmy się na możliwościach wykorzystania (nie)tanich technologii do analizy sieci radiowych i sposobami użycia ich w ich do analizy śledczej. W niniejszym artykule postaramy się pokazać możliwości analizy nieznanymi protokołami radiowymi przy pomocy analizatorów spektrum wspierających technikę SDR (ang. „Software Defined Radio”). W czasie tej konferencji praktycznie nie było wystąpienia związanego z rewolucją w sieciach radiowych. W artykule omówimy analizę ruchu z „pluskwy” bezprzewodowej oraz dzwonka radiowego jako przykładu komunikacji urządzenia IoT (ang. „Internet of Things”) o nieznanym protokole.

Sieci WiFi5, tj. sieci zgodne z rozszerzeniem standardu 802.11ac, nie spełniły pokładanych w nich nadziei. Wzrost wydajności tych sieci nie był zbyt duży, a ponadto standard nie rozwiązywał problemów komunikacji bezprzewodowej w środowiskach o dużym zagęszczeniu użytkowników. Kolejne wersje WiFi6/6e/7 adresują ten właśnie problem wprowadzając równocześnie nowoczesne kryptograficzne zabezpieczenia.

Dodatkowo poświęcimy trochę uwagi urządzeniom „noobs” zadając pytanie czy rzeczywiście są warte swojej ceny i sprawdzając czy możemy sami niewielkimi kosztami zrealizować podobne funkcjonalności. Mam nadzieję, że uda nam się Państwa przekonać, że nawet przy niskim budżecie można wiele osiągnąć, wykorzystując posiadane już zasoby.

**Słowa kluczowe:** IoT, (Internet of Things), hacking, analiza śledcza, analiza transmisji radiowych, SDR, WiFi

## WSTĘP

Naszą publikację w zeszłym roku rozpoczęliśmy od stwierdzenia, że sprzęt i oprogramowanie, o którym mowa w tym wykładzie, mogą zostać użyte do ataku, mogą stać się ofiarą i/lub mogą zawierać użyteczne dowody pomagające nam rozwiązać zagadkę. To twierdzenie będzie nam przyświecać i w tegorocznej publikacji.

Miniony rok był rewolucją w komputerach jednopłytkowych. Naszym zdaniem takim wydarzeniem jest najpierw pojawienie się Raspberry Pi-5, a potem wersji z 16GB pamięci RAM. Dotychczasowy problem w profesjonalnym wykorzystaniu Raspberry Pi, jakim były karty micro SD, może być rozwiązany poprzez podłączenie regularnego dysku SSD poprzez magistralę PCI. Dodatkowo pojawiły się nakładki umożliwiające

---

<sup>1</sup> zbigniew.jakubowski@compendium.pl

<sup>2</sup> grzegorz.marczak@radioforensics.org

podłączenie procesora AI Hailo-8L. Są też rozwiązania pozwalające na zastosowanie małego dysku NVME oraz procesora AI. Otwiera to zupełnie nowe perspektywy wykorzystania komputerów jednopłytkowych. Problemem może stać się zasilanie, gdyż sam Raspberry Pi 5 wymaga zasilacza 5A!

Sieci WiFi przeżywają rewolucję. O ile popularne WiFi5 znane jako 802.11ac postawiło na przepustowość klasycznymi metodami tj. poprzez zwiększenie ilości strumieni przestrzennych, zastosowania głębszych modulacji oraz zwiększenia szerokości kanału radiowego, o tyle WiFi6 koncentruje się na efektywności przesyłania danych w środowiskach o dużej koncentracji użytkowników. Ograniczenie WiFi5 praktycznie do transmisji danych do 1 użytkownika w jednym pakiecie radiowym stanowi poważne ograniczenie. WiFi5 działa również tylko w paśmie 5 GHZ.

W artykule postaramy się ujawnić wady i zalety poszczególnych rozwiązań.

Często słyszymy pytanie czy warto jest kupować urządzenia typu PwnGotchi, Flipper Zero, Deauther Watch etc. Pokażemy kilka przykładów, gdzie podobne funkcjonalności można osiągnąć za znacznie mniejsze pieniądze. Należy pamiętać również, że podatności nie są wieczne i już w przypadku wdrożenia ich na wspomnianych urządzeniach są już częściowo usunięte. Niestety wymiana sprzętu na przykład kart radiowych to wymiana laptopa i systemów operacyjnych co trwa w praktyce 5 do 6 lat.

## ŚRODOWISKO PRACY

W niniejszych materiałach wykorzystamy narzędzia z legendarnego systemu Kali Linux, zaimplementowanego na Windows 11 pod kontrolą WSL2. Dla chętnych naśladowania warto wspomnieć, że nie jest to proces prosty. Kali Linux pracujący pod kontrolą WSL2 oferuje jądro systemu bez wsparcia dla urządzeń bezprzewodowych – nie działa Bluetooth ani WiFi. Instalacja pakietów bezprzewodowych jest bezcelowa, bo brak jest wsparcia sprzętowego na poziomie jądra systemu. Proponowanym wyjściem z sytuacji jest kompilacja własnego jądra systemu z repozytorium GitHub. Dla osób niewtajemniczonych to trochę czarna magia. Dodatkowo w ostatnich wersjach wymagane były zmiany serwisów systemowych, aby bez instalacji zewnętrznego serwera X11 można było używać WSLG. Microsoft również nie rozpiera się stabilnością poprawek, po których czasem wymagana jest działalność badawcza.

Z powyższych uwag wynika, że rozwiązanie ma sporo wad. Jednak biorąc pod uwagę jego elastyczność i mimo wszystko długoterminowe wsparcie Microsoft jest to rozwiązanie bardzo funkcjonalne. W czasie prezentacji nie musimy przełączać się pomiędzy różnymi systemami, grafika jest lepiej zintegrowana niż na emulatorach, a czas startu WSL2 to kilka sekund.

Na komputerach z MAC OS można wykorzystywać wirtualizatory, takie jak na przykład Parallels. Należy jednak mieć świadomość, nowe urządzenia MacBook wykorzystują architekturę ARM, co implikuje, że musimy mieć wersję systemu pod tą architekturę. Dystrybucje, które oferują tylko wersję Intel x64 nie będą działać. Także uaktualnienia Kali mogą spowodować, że urządzenia lub/i oprogramowanie przestanie

działać. Warto więc zrobić kopię stanu maszyny wirtualnej, aby nie stracić dotychczasowej funkcjonalności. Czy w przyszłości możemy się spodziewać dużych problemów? Zdecydowanie tak, bo na przykład wchodzi do jądra Linux'a wsparcie dla WiFi7 czyli generalnie duże zmiany stosu radiowego.

### **ANALIZA PROTOKOŁÓW Z WYKORZYSTANIEM SDR**

Mam nadzieję, że poprzednie wystąpienie pokazało konieczność analizy spektrum radiowego. Karty WiFi „widzą” tylko pakiety 802.11 ale na tej samej częstotliwości pracują przecież inne protokoły takie jak na przykład Bluetooth, ZigBee, działają myszy i klawiatury bezprzewodowe. Brak zrozumienia transmisji radiowych w naszej sieci może doprowadzić na przykład do wycieku danych Z kolei zbyt późno wykryta kradzież danych może mieć katastrofalne skutki.



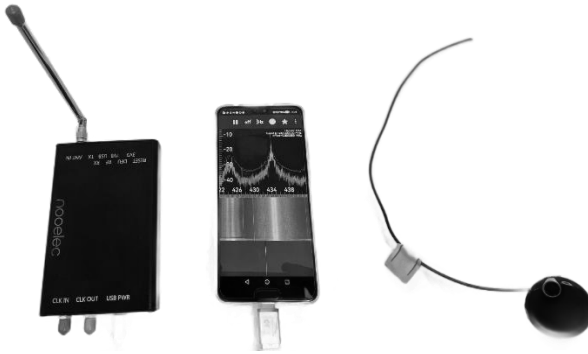
*Rysunek 2 Analizatory spektrum radiowego*

Na rysunku 1 widzimy w kolejności:

- prosty analizator spektrum 2.4 GHz,
- interfejs DVB-T ze specjalnym chipsetem pozwalający na analizę spektrum do 1.8-1.9 GHz i częstotścią próbkowania około 2MHz,
- profesjonalny analizator spektrum dla WiFi 2.4 i 5 GHz,
- urządzenie HackRF One pozwalające na pracę do 6 GHz, 8bit/próbkę i częstotść próbkowania do 20MHz.

Urządzenie DVB-T z układem RTL2832U Realtek i HackRF ma możliwość nie tylko analizy spektrum, ale również cyfrowania analizowanego sygnału. Sygnał cyfrowy możemy przetwarzać poprzez oprogramowanie SDR na bieżąco lub nagrywać i poddawać go analizie już w laboratorium.

Przykład tego znajdziecie Państwo na rysunku 2.



*Rysunek 2 Urządzenie podsluchowe widoczne na analizatorze spektrum*

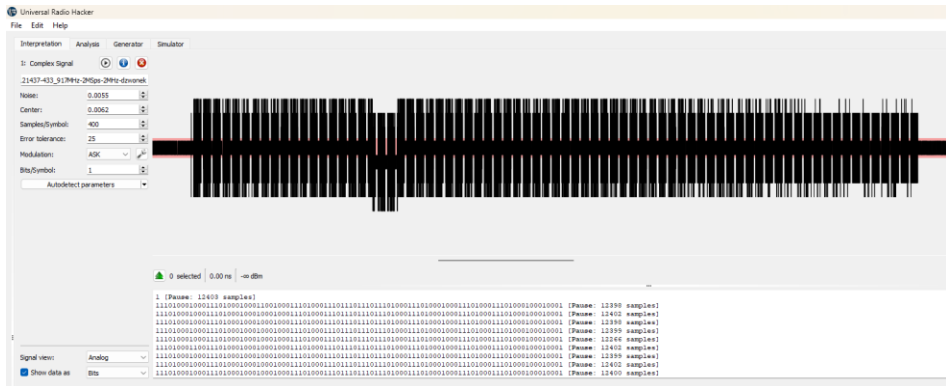
Pokazywaliśmy to już wcześniej. Sygnał radiowy z urządzenia podsluchowego został zdekodowany i nagrany poprzez oprogramowanie SDR. W tym przypadku urządzenie podsluchowe korzysta ze standardowej modulacji takiej jaką znamy z radia FM. Skąd można zdobyć taką informację? Tutaj sprawa była prosta, wystarczyła wizyta na stronie firmy oferującej sprzęt dla detektywów. Generalnie jednak nie jest to trywialne i wymaga pewnego procesu badawczego. Na przykład modulację można odgadnąć ze spektrometru, a sygnał FM ma specyficzny kształt, przy czym bardzo często profesjonalne analizatory spektrum oferują sygnatury widmowe różnych urządzeń. Urządzenia posiadające amerykański certyfikat FCC mają szczegółową dokumentację, łącznie z tym, że możemy znaleźć widok płytki drukowanej i układów.

Mając częstotliwość i sposób modulacji możemy wykorzystać oprogramowanie SDR do zdekodowania i nagrania transmisji, co demonstrowaliśmy w czasie wykładu.

Zaprezentowaliśmy również analizę transmisji pomiędzy komponentami dzwonka bezprzewodowego. Wykorzystaliśmy do tego celu urządzenie HackRF One oraz oprogramowanie Universal Radio Hacker. Analizę przeprowadziliśmy w następujących krokach

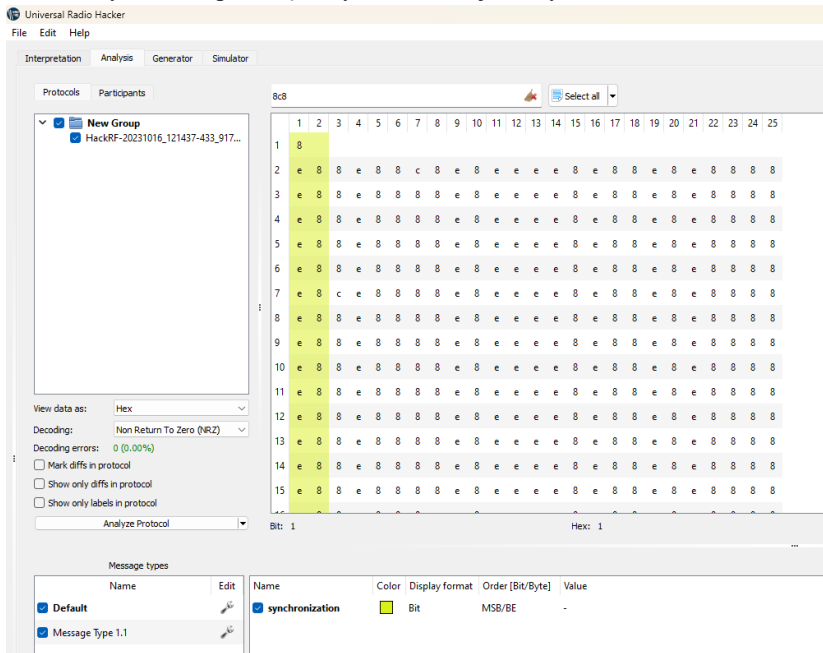
1. Wykrycie częstotliwości pracy urządzenia
2. Akwizycja danych przy pomocy HackRF One
3. Analiza ruchu pod kątem stosowanych modulacji – w naszym przypadku była to prosta modulacja amplitudowa

4. Korekta błędów transmisji uzyskanego sygnału cyfrowego poprzez ręczną edycję
5. Odtworzenie poprawionego sygnału

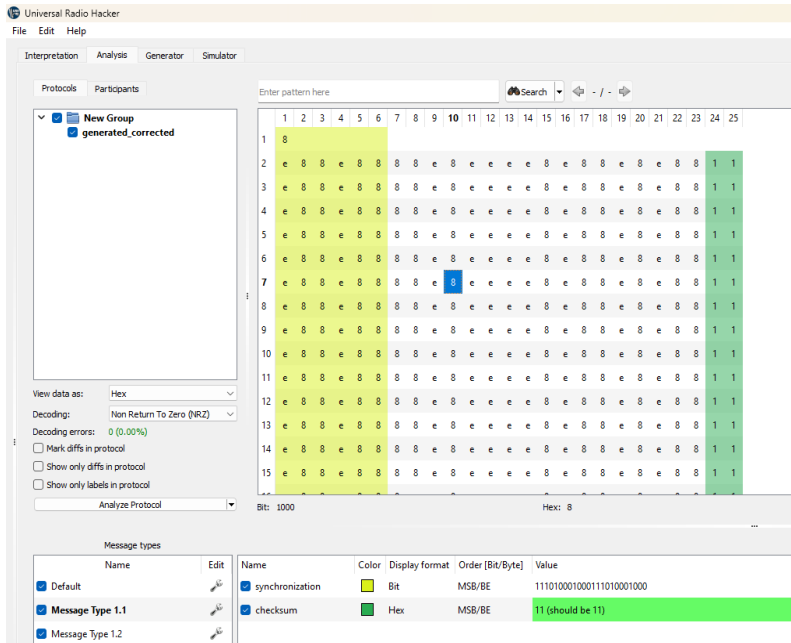


Rysunek 3 Zdigitalizowany sygnał analogowy

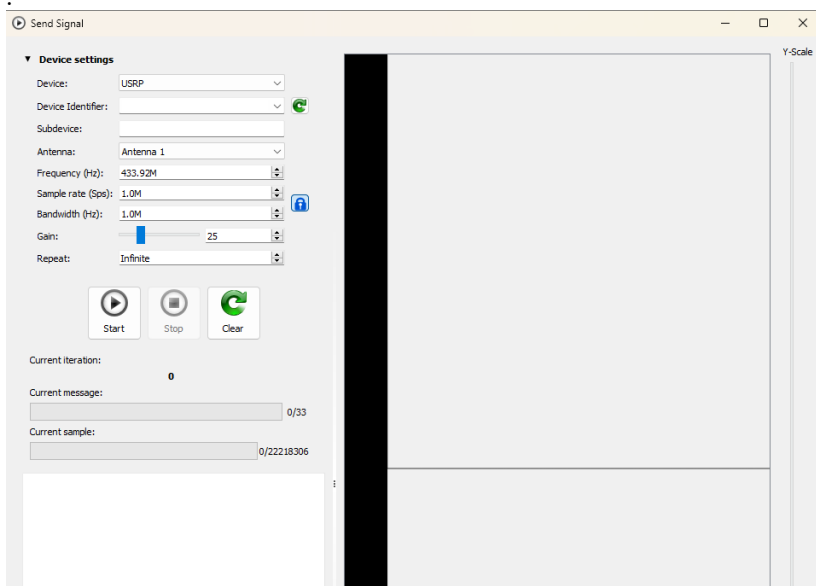
Na rysunkach pominięliśmy kroki 1 i 2 jako trywialne



Rysunek 4 Sygnał poprawiony - usunięto błędy transmisji



Rysunek 5 Powtórna analiza - widoczna synchronizacja i sumy kontrolne



Rysunek 6 Retransmisja sygnału

Koncepcja SDR jest bardzo poważnie traktowana przez wojsko. Część nadawczo/odbiorcza jest realizowana przez sprzęt, możemy natomiast całkowicie zmienić to, co robi radio, wymieniając oprogramowanie. W chwili obecnej kompromitacja systemu łączności wojskowej powoduje konieczność wymiany skompromitowanych urządzeń, a więc całkowity paraliż łączności. W przypadku sprzętu radiowego wykorzystującemu SDR w takiej sytuacji musimy jedynie wymienić oprogramowanie.

## **REWOLUCJA WIFI**

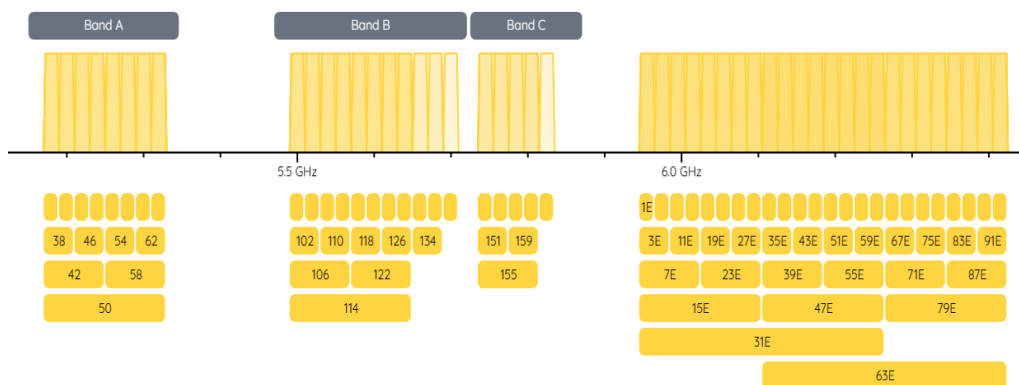
Zacznijmy od objaśnienia terminów stosowanych powszechnie w opisach produktów sieci bezprzewodowych. Zgodnie z konwencją IEEE norma bezprzewodowa jest tylko jedna - IEEE 802.11. Jest ona uzupełniana i modyfikowana poprzez mechanizm „amendments” czyli poprawek. Rzekoma norma 802.11n to w rzeczywistości poprawka „High Throughput”. Poprawki te są integrowane i raz na jakiś czas pojawia się norma IEEE 802.11-yyyy, gdzie „yyyy” to rok jej publikacji. Ostatnia modyfikacja to 802.11-2020. Skąd więc nazwa WiFi? W początkowym okresie rozwoju technologii 802.11 okazało się bardzo szybko, że normy nie są wystarczająco precyzyjne, aby zapewnić współpracę urządzeń od różnych producentów. W szczególności pojawienie się komputerów notebook z Intel Centrino w których, aby umieścić logo Centrino należało również zamontować kartę bezprzewodową Intel. Powołano konsorcjum Wireless Fidelity czyli właśnie WiFi. Jest to dobrowolne stowarzyszenie producentów sprzętu bezprzewodowego mające na celu zapewnienie właściwej współpracy urządzeń różnych producentów. W sieciach IoT taki ruch jest ciągle niestety oczekiwany... Wbrew pozorom tego typu ruch spowodował eksplozję rozwoju urządzeń mobilnych, a brak takiej organizacji upadek sieci WiMax.

WiFi5 czyli 802.11ac (ang. „Very High Throughput 6GHz”) nie rozwiązało problemów z wielodostępem użytkowników do usług sieciowych. Mechanizmy wielodostępu oferowane przez WiFi5 sprawdzają się tylko w określonych warunkach to znaczy, kiedy na przykład separacja kątowa pomiędzy klientami jest wystarczająco duża i możemy stosować MU-MIMO (ang. „Multi User MIMO”). Poszerzenie szerokości kanałów do 160 MHz również było problematyczne, specjalnie w Europie, gdzie obowiązuje DFS i obowiązek wykrywania radarów. Nie zmieniono również mechanizmów zabezpieczeń kryptograficznych. Praktyka wskazuje również, że ze względu na pobór mocy karty USB czy telefony wykorzystują tylko jeden lub dwa strumienie przestrzenne, ponieważ każdy strumień przestrzenny wymaga osobnego kanału radiowego, a tym samym oznacza to wzrost zapotrzebowania na moc zasilania. Mechanizm również może być stosowany tylko w paśmie powyżej 5 GHz. Należy również zaznaczyć, że mechanizmy typu MU-MIMO były nieobecne w pierwszych urządzeniach, które pojawiały się na rynku. Marketingowo przykryto to nazwą „Wave 1”.

Dopiero WiFi 6 802.11ax czyli „High-Efficiency WLAN” dało nam szansę na rzeczywiste rozwiązanie wielodostępu za pomocą modulacji OFDMA. Oznacza to, że w

przypadku przesyłania informacji możemy przesłać informację do wielu użytkowników równocześnie wykorzystując różne grupy nośnych w tej samej ramce radiowej. Po tym wydarzeniu nastąpiły istotne zmiany technologiczne — wprowadzenie WiFi 6E, czyli standardu 802.11ax z dostępnością pasma 6 GHz, co praktycznie podwaja przestrzeń dostępnych częstotliwości, a następnie rozwój WiFi 7.

Porównanie najważniejszych cech poszczególnych technologii znajdziemy w tabeli. WiFi 7. Tu zwróćmy uwagę na nowości, takie MLO (ang. „Multi Link Operation”) oraz zwiększenie głębokości modulacji do 4096 QAM. Nowy plan częstotliwości możecie państwo zobaczyć na rysunku.



Rysunek 6 Plan częstotliwości dla WiFi 6E i WiFi 7

Bezpieczeństwo sieci zostało dramatycznie podniesione. Obowiązkowe jest stosowanie MFP (ang. „Management Frame Protection”) czyli rozszerzenia 802.11w uniemożliwiającego ataki na uwierzytelnianie 802.11. Zastosowanie MFP powoduje, że sprzęt typu „deauther” przestaje działać, o ile zarówno punkt dostępu bezprzewodowego, jak i klient wspierają MFP.

Zabezpieczenia kryptograficzne zostały również ulepszone. WPA-3 jest obowiązkowe. Przynosi to wiele zmian, które przenoszą nas w obszar funkcji eliptycznych. Tu mamy dobrą wiadomość. Komputery kwantowe do złamania algorytmu RSA czy Diffie-Hellmann opartego o grupy modulo z kluczem o długości  $n$  bitów wymagają  $2n+3$  qbitów, jeśli stosujemy algorytm Shora. Dla funkcji eliptycznych te liczby sięgają milionów qbitów co jest poza zasięgiem tego, czego możemy się spodziewać w ciągu lat najbliższych. Dodatkowym utrudnieniem jest to, że komputery kwantowe stosowane do łamania kryptografii muszą zapewniać specyficzną funkcjonalność CRQC (ang. „Cryptographically Relevant Quantum Computers”). W przypadku RSA jest to funkcja QFT (ang. „Quantum Fourier Transform”).

Właściwości	Wi-Fi 6	Wi-Fi 6E	Wi-Fi 7
IEEE Standard	802.11ax	802.11ax (Extended)	802.11be
Pasmo	2.4 GHz, 5 GHz	2.4 GHz, 5 GHz, 6 GHz	2.4 GHz, 5 GHz, 6 GHz
Przepustowość	do 9.6 Gbps	do 9.6 Gbps	do 46 Gbps
Szerokość Kanału	do 160 MHz	do 160 MHz	do 320 MHz
Modulacja	1024-QAM	1024-QAM	4096-QAM
Opóźnienia	Niskie	Niskie z powodu pasma 6 GHz	Bardzo niskie z MLO
MLO (Multi Link Operation)	Brak wsparcia	Brak wsparcia	Dostępne
OFDMA	Wsparcie	Wsparcie	Wsparcie
MU-MIMO	do 8x8 MU-MIMO	do 8x8 MU-MIMO	rozszerzone MU-MIMO
Wsparcie dla 6 GHz	Brak wsparcia	Dostępne	Dostępne
TWT (Target Wake Time)	Wsparcie	Wsparcie	Wsparcie
Wdrożenie	Szeroka dostępność	Wzrost dostępności	Mało wdrożeń
Key use cases or applications	Streaming, IoT, środowiska o dużej gęstości	Aplikacje wymagającej małych opóźnień, mniej zakłóceń	8K video, AR/VR, wsparcie dla gier z b. niskimi opóźnieniami

Rysunek 7 Porównanie technologii WiFi

Należy z przyjemnością zauważyć, że nasze siły zbrojne dostrzegły potencjał komputerów kwantowych. Ruszył właśnie polski projekt budowy komputera kwantowego. O tym, że zagrożenie jest poważne świadczą na przykład działania firmy Cisco. Podnoszonym przez nią problemem jest stara zasada wywiadu HNDL (ang. „Harvest Now, Decrypt Later”).

Najważniejsze zmiany w algorytmach kryptograficznych to:

- Uwierzytelnianie SAE
- OWE (ang. „Wireless Opportunistic Wireless Encryption”) czyli szyfrowanie ruchu w otwartych hot spotach
- Nowe metody zabezpieczania transmisji o wysokiej wydajności – GCM-AES i tu panuje pewien chaos.

Obiecane metody szybkiej transmisji danych z szyfrowaniem na razie są dostępne tylko w trybie Enterprise. Tryb domowy/SOHO/OWE musi zadowolić się CCMP z AES 128 bit. Na przykład dla Windows 11 i karty Intel AX200 dostajemy następujące informacje:

```
> netsh wlan show driver
```

```
Interface name: Wi-Fi
```

```
Driver           : Intel(R) Wi-Fi 6 AX200 160MHz
```

```
Vendor           : Intel Corporation
```

```
Provider         : Intel
```

```
...
```

```
Radio types supported   : 802.11b 802.11g 802.11n 802.11a 802.11ac 802.11ax
```

```
FIPS 140 mode supported : Yes
```

```
802.11w Management Frame Protection supported : Yes
```

```
Hosted network supported : No
```

```
Authentication and cipher supported in infrastructure mode:
```

```
Open           None
```

```
Open           WEP-40bit
```

```
Open           WEP-104bit
```

```
Open           WEP
```

```
WPA-Enterprise TKIP
```

```
WPA-Enterprise CCMP
```

```
WPA-Personal   TKIP
```

```
WPA-Personal   CCMP
```

```
WPA2-Enterprise TKIP
```

```
WPA2-Enterprise CCMP
```

```
WPA2-Personal  TKIP
```

```
WPA2-Personal  CCMP
```

```
Open           Vendor defined
```

```
WPA3-Personal  CCMP
```

```
Vendor defined Vendor defined
```

```
WPA3-Enterprise 192 Bits GCMP-256
```

```
OWE            CCMP
```

## WPA3-Enterprise CCMP

Zwróćmy uwagę na to, że wszystkie mody personalne mają najwyżej szyfrowanie AES-128 czyli CCMP! Również obiecany AES-GCM-256 jest nieobecny. Tendencja ta pozostaje również w nowszych wersjach sprzętu i oprogramowania. Karty WiFi7 Intel AX 211. AES-GCM-256 jest dostępny tylko dla wersji Enterprise.

Ciekawą rzeczą jest również wsparcie dla oszczędzania energii. Mikrokontrolery z reguły wspierają sieci standardu zgodne z 802.11n. Do nowych rozwiązań wkrada się już 802.11ax ze względu na oszczędzanie energii.

Pojawienie się nowych częstotliwości radiowych, głębokości modulacji, MLO etc. powoduje poważne konsekwencje dla analizy śledczej. Dotychczasowe sposoby analizy śledczej, sprzęt i oprogramowanie wymagają poważnych zmian. Mamy nadzieję opowiedzieć o tym w następnej edycji konferencji.

Ciekawą próbę podjęto w projektowaniu układów scalonych. Okazuje się, że układy zaprojektowane przez AI działają sprawniej niż projektowane konwencjonalnie. Problemem wydaje się to, że AI projektuje układ jako całość, a nie modułowo jak do tego jesteśmy przyzwyczajeni. Jeden z naukowców stwierdził, że badacze nie do końca rozumieją co zrobiła sztuczna inteligencja. I to oprócz optymizmu może być przyczyną niepokoju.

## URZĄDZENIA DLA SNOBÓW

Urządzenia dla snobów są z pewnością ciekawe. Rozwiązania takie jak „Deauther Watch”, „Flipper Zero” czy „Pwnagotchi” niewątpliwie przyciągają uwagę. Pytanie, które trzeba sobie zadać jest proste czy są warte swojej ceny?

Odpowiedź na to pytanie nie jest prosta. Zaczniemy od uwagi, że podatności nie są wieczne. Przykładem są wszystkie urządzenia wykorzystujące pakiety radiowe 802.11 typu „deathentication” – specjalnie podajemy nazwę angielską, gdyż to co my traktujemy jako uwierzytelnienie odbywa się znacznie później. Rozszerzenie standardu 802.11w czyli MFP zapobiegające tego typu atakom zostało wprowadzone już w 2009 roku. Jego stosowanie nie było jednak obowiązkowe. Dopiero WPA-3 wprowadza obowiązek stosowania MFP. Problem jest jednak większy, bo odporność zyskujemy dopiero gdy obie strony stosują to zabezpieczenie. Co gorzej wsparcie musi dotyczyć nie tylko sprzętu, ale również systemów operacyjnych. Wystarczy wydać komendę na MS Windows:

```
> netsh wlan show wirelesscapabilities
```

aby przekonać się co rzeczywiście wspiera nasza karta radiowa w naszym systemie. Zdarzało się, że na decyzje o migracji do kolejnej wersji systemu MS wpływało właśnie wsparcie nowych możliwości sieci radiowych.

Warto również wspomnieć, że jeżeli macie Państwo trochę smykałki do elektroniki te same urządzenia można złożyć przy znacznie mniejszych kosztach. Urządzenie

„Deauther” zrobione 2 lata temu kosztowało około 50 PLN. Często w projektach znajdziecie nawet projekty płytek, których wykonanie można po prostu zlecić. Podobnie oryginalny projekt „Pwnagotchi” proponuje ekran e-paper, który kosztuje około 100 PLN. Urządzenie z wyjątkiem wyświetlania uśmiezków nie używa ich specjalnie, a te same informacje możemy dostać łącząc się przez stronę www urzędnika. Należy również zauważyć, że pomimo, że ekran jest „cool” to zużywa energię, a więc zmniejsza czas pracy urzędnika. W przypadku „Pwnagotchi” musimy wykorzystać power bank, aby zapewnić jego mobilność.

Urządzenia dla snobów są z pewnością ciekawe. Rozwiązania takie jak „Deauther Watch”, „Flipper Zero” czy „Pwnagotchi” niewątpliwie przyciągają uwagę. Pytanie, które trzeba sobie zadać jest proste czy są warte swojej ceny?

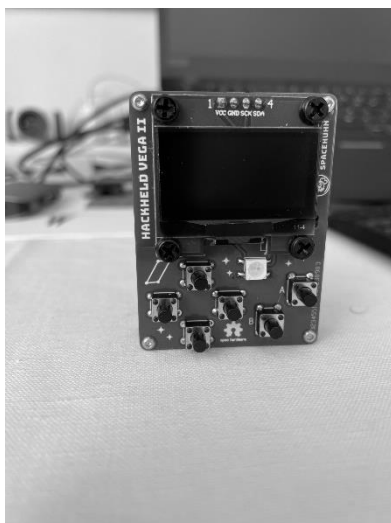
Odpowiedź na to pytanie nie jest prosta. Zaczniemy od prostej uwagi, że podatności nie są wieczne. Przykładem są wszystkie urządzenia wykorzystujące pakiety radiowe 802.11 typu „deathentication” – specjalnie podajemy nazwę angielską, gdyż to co my traktujemy jako uwierzytelnienie odbywa się znacznie później. Rozszerzenie standardu 802.11w czyli MFP zapobiegające tego typu atakom zostało wprowadzone już 2009 roku. Nie było ono jednak obowiązkowe. Dopiero WPA-3 wprowadza obowiązek stosowania MFP. Problem jest jednak większy, bo odporność zyskujemy dopiero gdy obie strony stosują to zabezpieczenie. Co gorzej wsparcie musi dotyczyć nie tylko sprzętu, ale również systemów operacyjnych. Wystarczy wydać komendę na MS Windows:

```
> netsh wlan show wirelesscapabilities
```

aby przekonać się co rzeczywiście wspiera nasza karta radiowa w naszym systemie. Zdarzało się, że na decyzje o migracji do kolejnej wersji systemu MS wpływało właśnie wsparcie nowej możliwości sieci radiowych.

Warto również wspomnieć, że jeżeli macie Państwo trochę smykałki do elektroniki te same urządzenia można złożyć przy znacznie mniejszych kosztach. Często w projektach znajdziecie nawet projekty płytek, których wykonanie można po prostu zlecić. Na rysunku 8 pokazany jest „Deauther” wykonany przez G. Marcza. Podobnie oryginalny projekt „Pwnagotchi” proponuje ekran e-paper, który kosztuje około 100 PLN. Urządzenie z wyjątkiem wyświetlania uśmiezków nie używa ich specjalnie, a te same informacje możemy dostać łącząc się przez stronę www urzędnika. Czy warto łączyć pieniądze w ekran, który, jeśli będziemy robili badania w terenie korzystając z zasilania przez „power bank” zmniejszy nasz czas pracy?

Wspomniane urządzenia to nie jedyne przypadki. Alternatywne rozwiązania oferują projekty takie jak „WiFi Ducky”, czy w przypadku „Rubber Ducky” alternatywne rozwiązania oparte o procesor Digi Spark o czym pisaliśmy w zeszłym roku.



*Rysunek 8 Urządzenie do rozłączania klientów sieci WiFi*

Należy więc zdawać sobie sprawę z tego, że prędzej czy później nasze zabawki przestaną działać. Proces wymiany sprzętu i łatania oprogramowania jest jednak niezwykle wolny, jeśli wymagana jest zarówno wymiana sprzętu jak i systemu operacyjnego. Podobny problem to mechanizmy otwierania bram i szlabanów – jeśli trafimy na podatne na atak urządzenie to możemy założyć, że nie zostanie ono szybko wymienione. Zabawki mogą, ale nie muszą, działać przez długi czas. Na pewno, jeśli możemy warto robić własne projekty – doświadczenia z ich wykonania i uruchomienia są bardzo wartościowe. Warto uzupełnić standardowe testy zabezpieczeń o testy prowadzone naszymi zabawkami.

## **PODSUMOWANIE**

Mikrokontrolery i komputery jednopłytkowe otworzyły przed nami świat IoT. Dzięki niskim cenom i dużej możliwością obliczeniowym urządzenia IoT miały szansę dostać się pod przysłowiowe strzechy. Niepokojącym trendem pozostaje zależność od producenta systemu inteligentnego domu. Nie ma tu zgodności jaką osiągnięto tworząc konsorcjum WiFi co spowodowało, że możemy komunikować się i budować sieci bezprzewodowe w oparciu o urządzenia różnych producentów. Promowane przez Google protokoły takie jak Thread czy Matter przebijają się bardzo powoli. Pozytywną tendencją jest próba integracji bardziej egzotycznych środowisk takich jak na przykład Aqara czy Somfy z bardziej rozpowszechnionymi takimi jak Apple Home. W przypadku wymienionych producentów konfiguruje się po prostu „bridge” na ich bramce do Apple Home. W tym przypadku możemy sterować urządzeniami zarówno poprzez natywne oprogramowanie, jak i Apple Home. Dużo również pisze się o protokole telemetrycznym

MQTT w zastosowaniach IoT. Nie spotkamy go łatwo, bo jest protokół „machine-to-machine”.

Zaprezentowana analiza urządzenia podsłuchowego opartego o transmisję FM oraz dzwonka bezprzewodowego powinno nam uświadomić, że sama analiza sieci WiFi nie wystarcza, aby zapewnić sobie bezpieczeństwo. Protokoły takie jak Bluetooth, LoRa, ZigBee czy Z-Wave używają nie tylko innych modulacji, ale również innych zakresów częstotliwości - jak na przykład piloty do bram. Warto więc wykonać analizę spektrum radiowego, aby zrozumieć co rzeczywiście wokół nas się dzieje. Słabo zabezpieczone urządzenia mogą stać się obiektem ataków na przykład ataku na nasz dzwonek radiowych. Łatwo sobie wyobrazić w jaki sposób można uprzykrzyć życie domownikom... Przypomnijmy również, że projekt sieci „Meshtastic” opartej o LoRa został oceniony jako bardzo niebezpieczny, bo trudny do jakiegokolwiek kontroli. Z reguły urządzenia sieci Meshtastic są sprzężone do telefonów GSM. Urządzenia w tej sieci mogą komunikować się bez połączenia z siecią GSM wykorzystując właśnie sieć LoRa.

Wprowadzenie sieci WiFi 6 czyli rozszerzenia standardu 802.11ax praktycznie nie spotkało się z dużym odzewem. Bardzo szybko pojawiło się WiFi 6e i WiFi 7. O ile WiFi 6 jest rzeczywiście rewolucyjne, jeśli chodzi o budowę sprawnie działających sieci dużej gęstości, to chyba najważniejszą rewolucją jest WiFi 6e, dublujące szerokość pasma dostępnego powyżej 5 GHz. Wprowadzenie 160 MHz kanałów spowodowało, że pasmo 5GHz też zostało wypełnione co w połączeniu z dodatkowymi restrykcjami dla pasma 5 GHz bardzo silnie ograniczało możliwości działania sieci. Nowe mechanizmy zabezpieczeń choć wyglądają dobrze w teorii w wielu przypadkach nie są praktycznie wdrażane w życie. Moja karta WiFi wspiera na przykład dla WPA3 z PSK tylko CCMP.

Zdajemy sobie sprawę, że to co zaprezentowaliśmy otwiera puszkę Pandory. Możliwości, które przedstawiliśmy, są równie łatwe do wykorzystania zarówno do dobrych, jak i złych celów. Mamy więc nadzieję, że wykorzystane zostaną zgodnie z zasadami etyki.

Świat wokół nas zmienia się w ostatnich latach w szaleńczym pędzie, co jest z pewnością również podyktowane wojną, która toczy się nie tylko na Ukrainie, ale w cyberprzestrzeni wokół nas. Nowe zagrożenia pojawiają się jak grzyby po deszczu. Aby efektywnie wykonywać naszą pracę musimy ciągle doskonalić i rozwijać metody zabezpieczania sieci i wykrywania zagrożeń. Pamiętajmy, że nie ma nic gorszego jak fałszywe poczucie bezpieczeństwa.

## BIBLIOGRAFIA

1. Legendarny "Rubber Ducky" [USB Rubber Ducky - Hak5](#)
2. Repozytorium payloadów do Rubber Ducky [GitHub - hak5/usbrubberducky-payloads: The Official USB Rubber Ducky Payload Repository](#)
3. Alternatywny projekt WiFi Ducky [GitHub - spacehuhn/wifi\\_ducky: Upload, save and run keystroke injection payloads with an ESP8266 + ATMEGA32U4](#)
4. Projekt Poison Tap na Raspberry Pi Zero [Samy Kamkar: PoisonTap - exploiting locked computers over USB](#)
5. [GitHub - htr-tech/ducky: Online USB Rubber Ducky Script Converter \(Arduino, Digispark & pyautogui\)](#)
6. Konwerter skryptów do programów wykonalnych: [GitHub - htr-tech/ducky: Online USB Rubber Ducky Script Converter \(Arduino, Digispark & pyautogui\)](#)
7. RF Analyzer na Adroida [GitHub - demantz/RFAnalyzer: Spectrum Analyzer for Android using the HackRF](#)
8. Bluetooth hacking UberTooth One [HackRF One - Great Scott Gadgets](#)
9. SDR Radio "HackrfOne" [HackRF One - Great Scott Gadgets](#)
10. Projekt Meshtastic [Meshtastic](#)
11. [Understanding the Quantum Threat to Network Security - Cisco](#)
12. [AI-designed chips are so weird that 'humans cannot really understand them' — but they perform better than anything we've created | Live Science](#)

# AGENT ROZLICZENIOWY JAKO ELEMENT SYSTEMU BEZPIECZEŃSTWA INSTRUMENTÓW PŁATNICZYCH

ACQUIRER AS PART OF THE PAYMENT INSTRUMENTS SECURITY SYSTEM

Jędrzej GRODZICKI<sup>1</sup>

**Streszczenie:** Artykuł ma na celu ogólne przedstawienie roli pełnionej przez agenta rozliczeniowego (podmiotu prowadzącego działalność związaną z transakcjami dokonywanymi przy użyciu różnego rodzaju instrumentów płatniczych) jako elementu tworzącego i wpływającego na bezpieczeństwo całego systemu. Zwrócenie uwagi na bezpieczeństwo, ograniczone do kwestii związanych z przeprowadzanymi transakcjami, czyli przeciwdziałaniu oszustwom związanym z transakcjami dokonywanymi przy użyciu instrumentów płatniczych.

**Słowa kluczowe:** instrumenty płatnicze, karta płatnicza, agent rozliczeniowy, oszustwa.

**Summary:** The article aims to give a general overview of the role played by an acquirer (an entity engaged in the business of transactions made with various types of payment instruments) as an element that creates and affects the security of the entire system. Attention to security, limited to issues related to the transactions carried out, i.e. countering fraud related to transactions made with payment instruments.

**Keywords:** payment instruments, payment card, acquirer, fraud.

## WPROWADZENIE

Wykreowanie podmiotów, określanych jako agenci rozliczeniowi, wiąże się nierozdzielnie z powstaniem czterostronnych systemów kart płatniczych. Powstanie tego typu systemów było wynikiem rozrastającego się rynku kart płatniczych, kiedy zaistniała potrzeba uzupełnienia schematu płatności o podmiot wyspecjalizowany, stanowiący ogniwo pośredniczące pomiędzy wydawcami kart, a punktami akceptacji, obsługujący transakcje dokonywane w punktach akceptacji, a jednocześnie prowadzący działania ukierunkowane na pozyskiwanie, a przez to rozwój sieci akceptacji kart płatniczych. W miarę rozwoju rynku oraz pojawiania się na nim innych niż karty instrumentów płatniczych, agenci rozliczeniowi w sposób naturalny stali się elementem zapewniającym ich akceptację w ramach czterostronnych systemów służących dotychczas do dokonywania jedynie płatności kartowych.

W powszechnej świadomości najbardziej widocznymi elementami systemów czterostronnych są posiadacze, akceptanci i wydawcy instrumentów płatniczych. Agenci

---

<sup>1</sup> Polskie e-Płatności, jedrzej.grodzicki@gmail.com, ORCID: 0009-0007-1403-2264.

rozliczeniowi pozostają nieco w cieniu całego systemu. Również, jeżeli chodzi o opracowania dotyczące rynków instrumentów płatniczych, niewielka ich liczba poświęcona jest problematyce agentów rozliczeniowych, czy to pod względem funkcjonalności, podejmowanych aktywności gospodarczych, czy też roli tych podmiotów w zapewnieniu systemowego bezpieczeństwa dokonywania transakcji.

## DEFINICJA AGENTA ROZLICZENIOWEGO

Agent rozliczeniowy definiowany jest obecnie na poziomie ustawodawstwa europejskiego, jak również w przepisach prawa polskiego.

Polska ustawa o usługach płatniczych<sup>2</sup> definiuje agenta rozliczeniowego poprzez wskazanie rodzaju działalności podejmowanej i prowadzonej przez taki podmiot, zakwalifikowanej przez ustawodawcę do kategorii usług płatniczych. Działalność ta, określona w tej ustawie jako „acquiring” jest definiowana jako polegająca na: „(...) umożliwianiu akceptowania instrumentów płatniczych oraz wykonywania transakcji płatniczych, zainicjowanych instrumentem płatniczym płatnika przez akceptanta lub za jego pośrednictwem, polegających w szczególności na obsłudze autoryzacji, przesyłaniu do wydawcy instrumentu płatniczego lub systemów płatności zleceń płatniczych płatnika lub akceptanta, mających na celu przekazanie akceptantowi należnych mu środków, z wyłączeniem czynności polegających na rozliczaniu i rozrachunku tych transakcji w ramach systemu płatności w rozumieniu ustawy o ostateczności rozrachunku (...)”<sup>3</sup>. Przyjęcie tego sposobu definiowania agenta rozliczeniowego stanowi emanację definicji usługi acquiringu umieszczonej w Dyrektywie o usługach płatniczych (PSD II)<sup>4</sup>. Zgodnie z motywem 10 PSD II, wskazującym na rozszerzenie definicji działalności acquiringowej na inne, niż tylko acquiring kart płatniczych, modele biznesowe, wprowadzona definicja zarówno nie ograniczała działalności agenta rozliczeniowego jedynie do transakcji kartowych, jak również, w sposób pośredni włączała obsługę transakcji dokonywanych innymi instrumentami płatniczymi w czterostronny schemat transakcyjny.

Na marginesie należy wspomnieć, iż na potrzeby tzw. Rozporządzenia interchange fee<sup>5</sup> w związku z tym, iż jego postanowienia dotyczą jedynie transakcji kartowych, definicja agenta rozliczeniowego została ograniczona ze względu na rodzaj przetwarzanych transakcji: „(...)„agent rozliczeniowy” oznacza dostawcę usług płatniczych zawierającego z odbiorcą umowę o akceptowanie i obsługę transakcji płatniczych realizowanych w oparciu o kartę, których wynikiem jest transfer środków pieniężnych na rzecz odbiorcy(...)”<sup>6</sup>.

---

<sup>2</sup> Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, Dz. U. z 2024 r. poz. 30, dalej: „UoUP”.

<sup>3</sup> Art. 3 ust. 1 pkt 5 UoUP.

<sup>4</sup> Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, Dz.U.UE.L.337

<sup>5</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751 z dnia 29 kwietnia 2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę, Dz.U.UE.L.123.

<sup>6</sup> Art. 2 pkt 1 Rozporządzenia interchange fee.

Polska UoUP wskazuje *expressis verbis*, iż jej postanowienia dotyczą zarówno agentów definiowanych poprzez wykonywaną działalność, jak również agentów rozliczeniowych, których dotyczy definicja w Rozporządzeniu *interchange fee*. W związku z powyższym wskazać należy, iż rozważania prowadzone w niniejszym artykule dotyczyć będą agentów rozliczeniowych traktowanych w sposób szeroki jako podmioty prowadzące działalność związaną z transakcjami dokonywanymi przy użyciu różnego rodzaju instrumentów płatniczych.

## **CZYM JEST BEZPIECZEŃSTWO?**

Aby rozpocząć dalsze rozważania, konieczne jest określenie jaki będzie, na potrzeby niniejszego artykułu, zakres pojęcia „bezpieczeństwo”.

W zakresie szerokim pojęcie to dotyczy takiego prowadzenia działania przez przedsiębiorcę, jakim jest agent rozliczeniowy, które zapewnia stałe, stabilne i nieprzerwane prowadzenie działalności.

Przy takim, szerokim, określeniu tego pojęcia, w jego zakres będą wchodziły właściwie wszystkie aspekty prowadzenia działalności gospodarczej: od bezpieczeństwa pomieszczeń i pracowników, po bezpieczeństwo finansowe, od zapewnienia personelu o odpowiednich kwalifikacjach, po kwestie związane na przykład z przeciwdziałaniem praniu pieniędzy i finansowaniu terroryzmu, czy też od gwarantowania prowadzenia działalności zgodnie z wymogami stawianymi agentom rozliczeniowym przez przepisy prawa, po zapewnienie pracownikom odpowiednich szkoleń pozwalających na rozwijanie i podnoszenie ich kwalifikacji zawodowych.

W niniejszym artykule skupiono się jednak na znacznie węższym pojęciu bezpieczeństwa, ograniczonym do kwestii związanych z przeprowadzanymi transakcjami, czyli przeciwdziałaniu oszustwom (*fraud*) związanym z transakcjami dokonywanymi przy użyciu instrumentów płatniczych.

W ramach działalności prowadzonej przez agenta rozliczeniowego wyróżnić można dwa główne typy oszustw. Podział ten dokonany jest ze względu na to, czy dokonanie oszustwa następuje w wyniku działania osób/podmiotów znajdujących się poza strukturą organizacyjną agenta rozliczeniowego (*fraudy zewnętrzne*), czy też jest wynikiem aktywności podejmowanej w tej strukturze (*fraudy wewnętrzne*).

W ramach pierwszej z kategorii można dokonać dalszej systematyzacji rodzajów oszustw i ich podziału. Możemy więc mówić o oszustwach związanych z instrumentami płatniczymi, realizowanych przy wykorzystaniu urządzeń służących do przeprowadzania transakcji płatniczych (terminale POS, narzędzia do płatności on-line) oraz związane z działalnością akceptantów.

Oszustwa związane z wykorzystaniem instrumentów płatniczych mogą polegać na próbach pozyskiwania towarów lub usług przez osobę nieuprawnioną<sup>7</sup>, próbach

---

<sup>7</sup> Jako osobę nieuprawnioną przyjmuję osobę, która nie weszła w posiadanie instrumentu płatniczego, czy danych transakcyjnych w sposób niezgodny z powszechnie obowiązującymi przepisami prawa- np. dziecko

dokonywania transakcji za pomocą instrumentów płatniczych, lub danych transakcyjnych umożliwiających dokonanie transakcji, których pozyskanie nastąpiło niezgodnie z przepisami prawa<sup>8</sup> oraz na podejmowaniu działań służących pozyskaniu towarów, usług lub środków pieniężnych poprzez niezgodne z prawem oddziaływanie na uprawnionego posiadacza instrumentu płatniczego<sup>9</sup>.

W przypadku transakcji oszukańczych dokonywanych przy użyciu urządzeń służących do przeprowadzania transakcji wskazać należy na działania podejmowane przez akceptantów lub ich pracowników<sup>10</sup> niezależnie, czy mówimy o akceptantach prowadzących fizyczne sklepy czy punkty usługowe (określanych jako „akceptanci naziemni”), czy też akceptantów świadczących usługi on-line.

Do drugiej z wyodrębnionych ogólnej kategorii oszustw - fraudów wewnętrznych należy zaliczyć oszustwa dokonywane przez osoby pracujące w strukturze agenta rozliczeniowego - w tym zakresie można mówić zarówno o działaniach polegających na nieprawidłowościach w procesie zawierania umów z akceptantami<sup>11</sup> i przez to zawieranie ich z podmiotami, które będą generować transakcje oszukańcze, jak również o działaniach lub zaniechaniach pracowników agenta rozliczeniowego podejmowanych w ramach obsługi transakcji dokonywanych w punktach akceptujących czy też obsługi tych podmiotów<sup>12</sup>.

## **DZIAŁANIA AGENTA ROZLICZENIOWEGO W CELU ZAPEWNIENIA BEZPIECZEŃSTWA SYSTEMU**

Aktywność agentów rozliczeniowych związaną z bezpieczeństwem dokonywania transakcji instrumentami płatniczymi można podzielić na dwie, ogólne kategorie działań:

- prewencyjne – nastawione na zminimalizowanie możliwości wystąpienia transakcji oszukańczych;

---

posługujące się kartą, której uprawnionym posiadaczem jest jeden z rodziców, natomiast podejmującą próbę dokonania transakcji instrumentem płatniczym wbrew postanowieniom umowy z wydawcą instrumentu płatniczego zawartej przez prawowitego posiadacza.

<sup>8</sup> Chodzi tu na przykład o transakcje kartami skradzionymi, czy przy wykorzystaniu skradzionych danych służących do przeprowadzenia transakcji (dane z karty- numer, data ważności, kod CVC/ CVV, kody Blik, dane pozyskane w wyniku skimmingu).

<sup>9</sup> Przykładami tego typu działań mogą być wymuszenia dokonania wpłaty pieniędzy z bankomatu przez uprawnionego posiadacza instrumentu, doprowadzenie posiadacza o ograniczonej świadomości do dokonania transakcji instrumentem płatniczym, zawieranie umów o karty kredytowe przez osoby podsztatwione (tzw. słupy) i dokonywanie transakcji w ciężar udzielonego kredytu bez zamiaru jego spłacenia.

<sup>10</sup> Mogą być to działania polegające na świadomym akceptowaniu transakcji dokonywanych instrumentami skradzionymi, samodzielne dokonywanie transakcji takimi instrumentami, pozyskiwanie danych z instrumentów płatniczych, którymi dokonywane są transakcje, w tym skimming) jak również próby wykorzystania urządzeń przerobionych, przez osoby podszywające się pod serwisantów.

<sup>11</sup> Np. zawieranie umów „po znajomości” bez wymaganej weryfikacji akceptanta, zawieranie umów z pełną świadomością nieprawidłowości mogących powstać w ramach transakcji, które będą dokonywane przez akceptanta.

<sup>12</sup> Będą to np. działania, czy też zaniechania weryfikacji alertów transakcyjnych generowanych przez transakcje u akceptanta, brak weryfikacji wykonywania przez akceptanta postanowień umownych np. w zakresie użytkowania terminala w określonej lokalizacji czy też nie przekazywania go do używania podmiotom trzecim.

- następcze – podejmowane po wystąpieniu transakcji fraudowych.

Do działań prewencyjnych można zaliczyć działania związane z bieżącym monitorowaniem transakcji, weryfikacją ich prawidłowości, jak również reakcje na pojawiające się na rynku zjawiska, czy zachodzące procesy<sup>13</sup>. Do tego typu działań zaliczyć oczywiście należy odpowiednie stosowanie się do ustalonych procedur weryfikacji i autoryzacji transakcji płatniczych. Ich niezmiernie ważnym elementem jest ponadto rzetelna i kompleksowa ocena akceptanta i prowadzonej przez niego działalności zarówno przed nawiązaniem współpracy, jak również w jej trakcie.

Dруга wyodrębniona kategoria działań – następcze - obejmuje czynności i działania podejmowane po wystąpieniu transakcji oszukańczych. Należy jednak zaznaczyć, że będą należały do niej nie tylko aktywności podejmowane przez samego agenta rozliczeniowego, ale również te polegające na współpracy z podmiotami zewnętrznymi w zakresie wykrycia i ujęcia osób dokonujących oszustw. Jednym z najważniejszych aspektów prowadzenia tego typu działań jest współpraca agenta rozliczeniowego zarówno z organami ścigania, jak również z innymi podmiotami, takimi jak wydawcy instrumentów płatniczych, organizacje kart płatniczych czy inni agenci rozliczeniowi<sup>14</sup>.

O ile w zakres działań prewencyjnych wchodzi różnego rodzaju działania zapobiegawcze, czynności podejmowane w ramach działań następczych, związanych z konkretnymi już przeprowadzonymi transakcjami oszukańczymi, polegają znaczącej mierze na współpracy i przekazywaniu informacji.

W działalności agenta rozliczeniowego, związanej z transakcjami płatniczymi, należy wskazać dwa, główne nurty przetwarzanych informacji- informacje transakcyjne oraz dane związane z rozliczaniem transakcji (finansowe).

Danymi transakcyjnymi są dane przekazywane w procesie dokonywania transakcji. Pod pojęciem danych rozliczeniowych należy rozumieć kategorię danych, które tworzone są na podstawie danych transakcyjnych i służą do przeprowadzenia rozliczeń finansowych z tytułu transakcji dokonanych w punkcie akceptanta.

Obydwie wymienione powyżej kategorie informacji wykorzystywane mogą być w ramach podejmowanych czynności następczych. W toku analizy danych transakcyjnych możliwe jest określenie punktu lub punktów, w których zostały dokonane transakcje oszukańcze<sup>15</sup>, określenie czy w ramach zdarzenia doszło do wykorzystania jednego, czy wielu instrumentów płatniczych, określenie czasu dokonania transakcji, jak również kwot

---

<sup>13</sup> M.in. działania stanowiące reakcję na wzmogłą aktywność oszukańczą polegającą na próbach użycia kart podrobionych zaobserwowane w segmencie rynku akceptacji kart płatniczych, które, nawet w sytuacji niewystąpienia takich prób w sieci danego agenta rozliczeniowego, mają za zadanie zminimalizowanie ryzyka ich wystąpienia.

<sup>14</sup> Wymiana i udzielanie informacji o akceptantach, z którymi agent rozliczeniowy rozwiązał umowę z powodu nienależytego wykonania przez akceptanta, jest obowiązkiem ustawowym, określonym w art. 12a pkt 4 i 5, natomiast nie dotyczy ona bezpośrednio transakcji oszukańczych, a stanowi działania podmiotowe prewencyjne mające na celu oszacowanie i ograniczenie ryzyka zawarcia umowy przez kolejnego agenta rozliczeniowego z nierzetelnym akceptantem.

<sup>15</sup> W takiej sytuacji daje to możliwość na przykład pozyskania nagrań z monitoringu w punkcie akceptującym (jeżeli jest to punkt monitorowany) co może pomóc w identyfikacji osób dokonujących transakcji.

na jakie opiewały. Możliwa jest również identyfikacja rodzaju wykorzystanego instrumentu płatniczego oraz określenie czy wykorzystany był w punkcie naziemnym czy bez fizycznej obecności instrumentu i osoby nim posługującej się w punkcie akceptanta. Możliwe jest również określenie (szczególnie w przypadku punktów akceptujących w których następuje rejestrowana zmiana kasjerów) personaliów osoby obsługującej transakcję w imieniu akceptanta.

Posiadane przez agenta rozliczeniowego dane transakcyjne mogą zostać wykorzystane do przeprowadzenia analizy zarówno czasu, jak i zakresu dokonanych w jego sieci działań oszukańczych. Należy jednak zauważyć, że dane tego typu, które posiada dany agent rozliczeniowy, nie w każdym przypadku muszą być wystarczające do określenia skali występujących transakcji oszukańczych w odniesieniu całego rynku<sup>16</sup>.

Dane finansowe mogą zostać wykorzystane do określenia przede wszystkim skali przepływów pieniężnych z tytułu transakcji oszukańczych. Na podstawie tych danych można oszacować skalę transakcji oszukańczych występujących u danego akceptanta. Ich analiza może posłużyć również do formułowania wniosków dotyczących częstotliwości i skali dokonywanych w danym punkcie fraudów. W ten sposób jest możliwe szacowanie ryzyka związanego ze współpracą z danym akceptantem, jak również ewentualne wnioskowania na temat prawidłowości prowadzonych przez niego działań<sup>17</sup>.

Analiza danych zarówno transakcyjnych, jak i finansowych może być również wykorzystana w wewnętrznej działalności agenta rozliczeniowego w celu przygotowania i przeprowadzenia działań naprawczych, których celem jest ograniczenie ekspozycji na ryzyko wystąpienia transakcji oszukańczych w danym punkcie akceptującym, czy w sieci punktów danego akceptanta, lub podjęcie działań mitygujących, w ostateczności zaś decyzji o rozwiązaniu umowy o akceptację instrumentów płatniczych.

Rolę agenta rozliczeniowego w systemie transakcji instrumentami płatniczymi, rozpatrywać należy w dwóch płaszczyznach. Jedną z nich to pełnienie funkcji podmiotu zabezpieczającego system od działań zewnętrznych, drugą to działania podejmowane w ramach współpracy z innymi uczestnikami systemu, jak również z organami ścigania – w ramach zwalczania przestępczości.

Ta druga płaszczyzna współpracy wymaga dokonywania analiz oraz dzielenia się, wymiany, informacjami z innymi uczestnikami rynku. O ile przekazywanie informacji ogólnych na temat zjawisk i tendencji nie podlega wymogom poufności, o tyle

---

<sup>16</sup> Tytułem przykładu można podać sytuację wykorzystania skradzionej karty płatniczej do dokonania transakcji nieuprawnionych w punktach akceptujących, w których znajdują się terminale POS obsługiwane przez różnych agentów rozliczeniowych. Dopiero uzyskanie informacji od wszystkich z nich w efekcie pozwoli na określenie skali oszustwa zarówno co do liczby, jak i wartości transakcji.

<sup>17</sup> Konkluzje wnioskowań mogą stanowić, że akceptant jest eksponowany na ryzyko przy dużej skali transakcji oszukańczych, w tym nie powiązanych ze sobą. Z drugiej strony mogą sugerować, iż sam akceptant dokonuje lub współdziała w dokonywaniu oszustw - dla potwierdzenia lub zaprzeczenia prawidłowości tych wniosków konieczne jest dokonanie pogłębionej analizy konkretnej sytuacji.

przekazywanie konkretnych informacji czy o danych transakcyjnych lub finansowych podlega limitowaniu<sup>18</sup>.

Konieczność otrzymania czy weryfikacji danych transakcyjnych lub rozliczeniowych, powstaje najczęściej po stronie organów ścigania w ramach prowadzonych przez nie postępowań. Możliwość i sposób żądania przekazania przez agentów rozliczeniowych potrzebnych informacji warunkowany jest charakterem podmiotu, który prowadzi działalność agenta rozliczeniowego.

Działalność agenta rozliczeniowego może być prowadzona przez bank w ramach działalności bankowej. Agentem rozliczeniowym może być również podmiot niebankowy, który spełnia przewidziane w UoUP wymagania.

Charakter prowadzonej przez agenta rozliczeniowego działalności (bankowa i niebankowa) wpływa na sposób w jaki organa potrzebujące dostępu do informacji agenta rozliczeniowego mają możliwość ich uzyskania.

W przypadku bankowych agentów rozliczeniowych informacje mogą być uzyskane w trybie dostępu do tajemnicy bankowej<sup>19</sup>. W przypadku agentów rozliczeniowych niebędących bankami - w trybie zwolnienia z tajemnicy służbowej<sup>20</sup>.

Na marginesie powyższych rozważań należy zauważyć, iż informacje, którymi dysponuje agent rozliczeniowy, mogą być użyteczne nie tylko w sytuacjach związanych ze zwalczaniem oszustw dokonywanych przy użyciu instrumentów płatniczych. Informacje te mogą służyć do identyfikacji zarówno miejsca dokonywania transakcji danym instrumentem płatniczym<sup>21</sup>, jak również mogą być pomocne przy ustalaniu tożsamości osób, z którymi mogą być powiązane dane transakcyjne<sup>22</sup>. W procedurze weryfikacji posiadanych danych transakcyjnych nie jest możliwa współpraca czy pozyskiwanie informacji bez zachowania trybów opisanych powyżej, w odpowiednich dla bankowych i niebankowych agentów rozliczeniowych. Podkreślić należy jednak, iż agent rozliczeniowy, oprócz danych transakcyjnych i finansowych nie posiada danych identyfikacyjnych, które bezpośrednio mogłyby zostać wykorzystane do ustalenia tożsamości osoby posługującej się instrumentem płatniczym.

## PODSUMOWANIE

Agent rozliczeniowy jako podmiot będący elementem czterostronnego systemu płatności instrumentami płatniczymi, pomimo nie tak eksponowanej pozycji jak

---

<sup>18</sup> Chodzi tu o przekazywanie np. danych transakcyjnych do podmiotów, które nie są uprawnione do ich otrzymywania w ramach prowadzonych operacji transakcyjnych, czy rozliczeniowych.

<sup>19</sup> Art. 104 ust. 3; art. 105 Ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe Dz. U. 2023 poz. 2488.

<sup>20</sup> Art. 180 § 1 Ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego Dz. U. 204 poz. 37.

<sup>21</sup> Podkreślenia wymaga fakt, iż samo dokonanie transakcji nie jest jednoznacznym wskaźnikiem, że transakcji dokonał uprawniony posiadacz instrumentu płatniczego.

<sup>22</sup> Jednym z przykładów może być sytuacja odnalezienia potwierdzenia transakcji dokonanej instrumentem płatniczym przy osobie o nieustalonej tożsamości. W takim przypadku jest możliwość ustalenia na podstawie danych transakcyjnych miejsca dokonania transakcji, wykorzystania danych z monitoringu do weryfikacji czy dokonujący transakcji to osoba, której tożsamość należy ustalić, a jednocześnie ustalenie wydawcy instrumentu płatniczego i w ten sposób ustalenie poszukiwanej tożsamości osoby.

wydawcy, akceptanci i posiadacze instrumentów płatniczych, stanowi ważny element funkcjonowania tego systemu. Pełniąc dwojaką rolę - podmiotu prowadzącego bezpośrednio działania na rzecz rozwoju rynku akceptacji, poprzez zawieranie umów z nowymi akceptantami oraz obsługującego i rozliczającego dokonywane transakcje - jest równocześnie elementem znacząco wpływającym na bezpieczeństwo funkcjonowania omawianego systemu. Rola ta polega na pewnego rodzaju buforowaniu i kontrolowaniu podmiotów zainteresowanych przystąpieniem, czy potem uczestniczących w sieci akceptacji poprzez ich uprzednią, a po zawarciu umowy, bieżącą kontrolę. Ponadto agent rozliczeniowy, w ramach działalności transakcyjno-rozliczeniowej, podejmuje wszelkie kroki zapewniające bezpieczne przeprowadzanie i rozliczanie transakcji. Przy czym stwierdzenie to obejmuje również działania ukierunkowane na niedopuszczenie do realizacji transakcji oszukańczych.

Dla zapewnienia bezpieczeństwa systemu płatności realizowanych przy wykorzystaniu instrumentów płatniczych konieczne jest również podejmowanie przez agenta rozliczeniowego współpracy zarówno z innymi uczestnikami rynku czy też instytucjami albo organizacjami branżowymi, jak również z organami zajmującymi się ściganiem i zwalczaniem przestępczości. W tym zakresie, w ramach wyznaczonych przepisami prawa, agent rozliczeniowy jest podmiotem mogąącym dostarczyć niezbędnych i wymaganych w toku prowadzonych postępowań informacji, jak również aktywnie wspomagać prowadzone działania. Jednocześnie jako podmiot posiadający najszerszą wiedzę o procesach związanych z akceptacją oraz posiadający doświadczenie praktyczne w odniesieniu do tego wycinka rynku, jest w sposób niezaprzeczalny znaczącym elementem wpływającym i zapewniającym wysoki poziom bezpieczeństwa nie tylko w zakresie akceptacji, ale w skali całego rynku płatności instrumentami płatniczymi.

## **BIBLIOGRAFIA**

1. Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych, Dz. U. z 2024 r. poz. 30.
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE, Dz.U.U.E.L.337.
3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751 z dnia 29 kwietnia 2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę, Dz.U.U.E.L.123.
4. Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe Dz. U. 2023 poz. 2488.
5. Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego Dz. U. 204 poz. 37.

# INFORMACJE PRZECHOWYWANE ELEKTRONICZNIE A OPINIA Z INFORMATYKI ŚLEDCZEJ

## ELECTRONICALLY STORED INFORMATION VS. COMPUTER FORENSICS OPINION

Wojciech PILSZAK<sup>1</sup>

**Streszczenie:** Opracowanie zawiera propozycje rozwiązań oraz zasad postępowania z informacjami przechowywanymi elektronicznie, uzyskiwanymi w wyniku zgromadzenia i przygotowania do dalszej analizy i interpretacji danych zawartych na cyfrowych nośnikach informacji, poddawanych badaniu w ramach opinii z zakresu informatyki śledczej. Omówieniu podlega specyficzny rodzaj opinii, w toku której biegły lub instytucja specjalistyczna zabezpiecza całość danych (w tym usuniętych a możliwych do odtworzenia) na zewnętrznym nośniku, w celu poddania ich dalszej analizie przez organy procesowe. W publikacji zostały zaprezentowane rozwiązania stosowane w amerykańskim systemie prawnym a odnoszące się do informacji przechowywanych w formie elektronicznej, jak również przedstawiona została próba ich praktycznego zaadaptowania w polskim systemie prawnym, w opiniach wykonywanych na zlecenie organów ścigania i instytucji wymiaru sprawiedliwości.

**Słowa kluczowe:** opinia sądowo-kryminalistyczna, zabezpieczanie danych, informatyka śledcza, dane przechowywane cyfrowo.

**Summary:** The study includes proposed solutions and principles for handling electronically stored information obtained as a result of collecting and preparing data from digital media for further analysis and interpretation. It focuses on a specific type of forensic opinion in which an expert or specialized institution secures all data (including deleted but recoverable information) on an external medium for further analysis by judicial authorities. The publication presents solutions applied in the U.S. legal system concerning electronically stored information and attempts to adapt these practices to the Polish legal system in opinions prepared at the request of law enforcement agencies and judicial institutions.

**Keywords:** forensic opinion, data preservation, digital forensics, electronically stored information.

---

<sup>1</sup> e-Detektywi sp. z o.o., Pilszak Consulting; wojciech.pilszak@e-detektywi.pl, ORCID: 0009-0004-4439-6403.

## ZAGADNIENIA OGÓLNE

Inspiracją do napisania niniejszej publikacji stała się korespondencja, którą otrzymałem z jednego z Sądów karnych, dotycząca przygotowanej przez spółkę e-Detektywi opinii z zakresu informatyki śledczej. Pierwotnie przygotowaliśmy ją na zlecenie jednej z Prokuratur,

a obejmowała ona akwizycję, czyli zgromadzenie i przygotowanie do dalszej analizy i interpretacji, danych zawartych na dyskach twardych zabezpieczonych komputerów i dostarczenie ich w takiej formie, aby możliwe było zapoznanie się przez zlecającego, zarówno z treścią dokumentów wytworzonych przez użytkowników, jak i z ich (użytkowników) aktywnością związaną z wykorzystaniem zabezpieczonych urządzeń (lokalnie jak i w sieci Internet). Z uwagi na bardzo dużą liczbę danych, materiały wyjściowe dostarczone zostały na dysku twardym, wraz z narzędziem umożliwiającym przeglądanie, przeszukiwanie i ewentualne wyodrębnianie do dalszych raportów istotnych treści. Takie działanie jest w przypadku badań wykonywanych przez spółkę regulą, ponieważ umożliwia dalsze swobodne przetwarzanie dostarczonych danych. Wykonana opinia nie obejmowała żadnej formy analizy i oceny przydatności przez biegłego ujawnionego materiału gdyż, w ocenie zlecającego, nie było to niezbędne dla zapewnienia prawidłowego toku postępowania. W skrócie - zlecający uznał, że biegłemu nie jest potrzebna wiedza o szczegółowych okolicznościach sprawy, a ma on jedynie przygotować materiał do dalszej analizy przez organy procesowe.

Sytuacja taka, w której biegłemu z zakresu informatyki śledczej zleca się jedynie zabezpieczenie całości danych (w tym usuniętych a możliwych do odtworzenia) na zewnętrznym nośniku, w celu poddania ich dalszej analizie przez organy procesowe jest coraz częstsza. W takim wypadku, w części dyspozytywnej postanowienia znajduje się tylko ogólne żądanie obejmujące zabezpieczenie wszelkich danych, w tym usuniętych, a możliwych do odtworzenia, znajdujących się w przekazanym do badań urządzeniu oraz zapisanie ich na zewnętrznym nośniku w formacie umożliwiającym swobodne zapoznanie się z ich treścią. Nie sposób zgodzić się, w tym przypadku, ze stanowiskiem zaprezentowanym przez A. Gaberle, iż „Niczego dobrego nie zwiastuje także ogólnikowość pytań (...), ponieważ bywa to metodą skrywania braku wiedzy lub wyrazem niedbalstwa organu procesowego.”<sup>2</sup> W przypadku spraw skomplikowanych, wielowątkowych, w których prowadzenie zaangażowane są zarówno po stronie Prokuratury, jak i Policji wieloosobowe zespoły ludzkie, zlecający coraz częściej dochodzą do wniosku, iż łatwiej jest przeprowadzić analizę zabezpieczonego przez biegłego materiału samodzielnie, niż zdawać się na osobę lub osoby ze znacznym doświadczeniem w swojej branży, ale nie dysponujące jakąkolwiek wiedzą procesową i pozap procesową związaną z prowadzeniem postępowania przygotowawczego, czy też z jego przedmiotem. Tego rodzaju sytuacje mają miejsce najczęściej w przypadku

---

<sup>2</sup> A. Gaberle, 3. *Forma i zakres opinii biegłych* [w:] *Dowody w sądowym procesie karnym. Teoria i praktyka*, Warszawa 2010.

przestępstw o charakterze czysto kryminalnym, gdzie urządzenia cyfrowe stanowią jedynie wsparcie procesu komunikacji, czy przetwarzania danych przez sprawcę lub grupę przestępczą, albo pozwalają, np. na przygotowanie określonych dokumentów, a nie są wykorzystywane do popełnienia wysoce wyspecjalizowanych przestępstw w dziedzinie cyfrowej. Wówczas analiza dotyczy najczęściej istniejących procesów komunikacji w grupie przestępczej, struktury i zasad jej funkcjonowania, a nie specyficznych zagadnień technicznych, do których przedstawienia wymagana jest wiedza specjalistyczna, która w omawianym przypadku ogranicza się najczęściej do umiejętności jak najszerzej agregacji danych z uwzględnieniem zasobów zaszyfrowanych i chmurowych.

Nie można zapominać także o bardzo istotnych, a nierzadko dominujących, aspektach finansowych. Każda analiza przeprowadzana na dużych zbiorach danych, to proces zarówno czasochłonny jak i kosztowny, a obserwując mechanizm wyboru wykonawców ekspertyz można odnieść wrażenie, iż na pierwszym miejscu zlecający stawiają koszty, a wszelkie inne kryteria związane ze sporządzaniem opinii znajdują się dopiero na dalszych pozycjach. Przeniesienie ciężaru analizy na stronę organu procesowego, znacząco, w rozumieniu tegoż organu, koszty te redukuje. Inna sprawa, że to właśnie czas i obowiązujące stawki powodują, iż po stronie biegłego łatwiej jest wykonać pewne zautomatyzowane działania przy pomocy wyspecjalizowanych narzędzi, niż angażować się w żmudne i czasochłonne procesy, wymagające zgromadzenia bardzo dużej ilości informacji wstępnych, a w wielu przypadkach także szczegółowego zapoznania się z materiałem dowodowym uzyskanym w trakcie prowadzonego postępowania.

I tutaj zbliżamy się do sedna problemu, czyli sposobu udostępnienia zagregowanych danych do dalszej analizy lub wykorzystania przez organ procesowy. Zgodnie z art. 200 par. 1 Kodeksu postępowania karnego<sup>3</sup>, opinia jest składana przez biegłego ustnie lub na piśmie, w zależności od polecenia organu procesowego. W par. 2 tegoż artykułu znajdziemy natomiast informacje o tym, co każda opinia powinna zawierać. Każda przygotowana w formie pisemnej ekspertyza musi zawierać:

- imię, nazwisko, stopień i tytuł naukowy, specjalność i stanowisko zawodowe biegłego;
- imiona i nazwiska oraz pozostałe dane innych osób, które uczestniczyły w przeprowadzeniu ekspertyzy, ze wskazaniem czynności dokonanych przez każdą z nich;
- w wypadku opinii instytucji - także pełną nazwę i siedzibę instytucji;
- czas przeprowadzonych badań oraz datę wydania opinii;
- sprawozdanie z przeprowadzonych czynności i spostrzeżeń oraz oparte na nich wnioski;
- podpisy wszystkich biegłych, którzy uczestniczyli w wydaniu opinii<sup>4</sup>.

---

<sup>3</sup> Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (t.j. Dz. U. z 2024 r. poz. 37 z późn. zm.).

<sup>4</sup> Tamże.

Zbliżone, chociaż mniej szczegółowe, regulacje znajdziemy także w przypadku opinii przygotowywanych na potrzeby postępowań cywilnych<sup>5</sup>, jednakże w przedmiotowym opracowaniu jako wiodące będą traktowane regulacje dotyczące postępowań karnych.

Zarówno w przywołanym wcześniej artykule Kodeksu postępowania karnego, jak i w całym Rozdziale 22 tej ustawy, dotyczącym biegłych, tłumaczy i specjalistów, nie znajdziemy żadnej informacji jak należy potraktować coś, co będzie efektem wykonania postanowienia o dopuszczeniu dowodu z opinii biegłego, czy też instytucji specjalistycznej, a co w prawodawstwie amerykańskim jest określane jako Electronically Stored Information (ESI), czyli informacje przechowywane elektronicznie. Ustawodawca skupił się na szczegółowym określeniu strony formalnej opinii, nie poświęcając żadnej uwagi materiałom dodatkowym stanowiącym załączniki do niej. Nie znajdziemy także tego rodzaju informacji w orzecznictwie. Tymczasem wyodrębnione z urzędzenia, rozpoznane i odpowiednio skatalogowane dane przechowywane elektronicznie, w przypadku takich opinii, jak omawiane w tej publikacji, stanowią ich część najbardziej istotną. Dane te, być może niesłusznie, nazywane są załącznikami do opinii, gdyż z obiektywnego punktu widzenia należałoby stwierdzić, iż to opinia papierowa stanowi raczej niezbędny z punktu widzenia przestrzegania procedur, załącznik do nich.

Przywiązanie do formatu papierowego, jak również nacisk kładziony na wydruki danych, może wynikać z przypadków niezrozumienia faktu, z jaką ilością informacji możemy mieć do czynienia w przypadku średnio skomplikowanego urzędzenia elektronicznego. Jako drugi, nieco żartobliwy powód, możemy wskazać na pokutujące w społeczeństwie przekonanie, iż waga sprawy oraz powaga Sądu rośnie wprost proporcjonalnie od ilości tomów akt, które zarejestrują kamery stacji telewizyjnych na stole sędziowskim. Bezspornym natomiast pozostaje fakt, iż w przypadku niektórych środków dowodowych (w tym niektórych opinii) wiodącą formą ich prezentacji pozostaje forma papierowa, lecz z pewnością nie możemy do nich zaliczyć przypadków tutaj omawianych.

Na potrzeby niniejszej publikacji, jako jedno z proponowanych rozwiązań, przedstawione zostanie postępowanie z informacjami przechowywanymi elektronicznie opisane w Federal Rules of Civil Procedure<sup>6</sup> (FRCP). Dokument ten zawierający zbiór procedur mających zastosowanie przed sądami w sprawach cywilnych, stanowi odpowiednik polskiego Kodeksu postępowania cywilnego. Istotnym z punktu widzenia niniejszej publikacji jest art. 34 (Rule 34) dotyczący wytwarzania dokumentów, informacji przechowywanych elektronicznie i rzeczy materialnych lub wchodzenie na

---

<sup>5</sup> Oddział 4 – opinia biegłych - Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2024 r. poz. 1568 z późn. zm.).

<sup>6</sup> <https://www.uscourts.gov/rules-policies/current-rules-practice-procedure/federal-rules-civil-procedure> - ostatni dostęp w dniu 20.11.2024 r.

teren w celu przeprowadzenia inspekcji i w innych celach<sup>7</sup>. Co prawda, dotyczy on szczególnego etapu postępowania stron przed sądami cywilnymi, a samo zagadnienie jest dość odległe od problematyki związanej ze sposobem przedstawienia materiałów uzyskanych w trakcie opiniowania, jednakże zawiera rozwiązania, które mogą stanowić istotny przyczynek do dyskusji na temat formy ich prezentacji.

Na marginesie zaznaczyć należy, iż nie udało się zidentyfikować adekwatnych zapisów zarówno w Federal Rules of Criminal Procedure<sup>8</sup>, jak i w Federal Rules of Evidence<sup>9</sup>.

## PROPONOWANE ROZWIĄZANIA

Ponieważ w polskiej procedurze karnej nie znajdziemy regulacji obejmujących zasady postępowania z dołączonymi do opinii danymi przechowywanymi elektronicznie, postaram się nakreślić pewne wstępne wytyczne, korzystając z art. 34 (Rule 34) FRCP, i przedstawiając go w taki sposób, aby mógł być zastosowany w przypadku opinii, w których materiał wynikowy stanowi całość, możliwa do odczytania, zawartość przechowywana na nośniku danych badanego urzędnika.

Zgodnie z art. 34 lit. a pkt 1 lit. A FRCP, wszelkie dokumenty lub informacje przechowywane elektronicznie – w tym pisma, rysunki, wykresy, wykresy, fotografie, nagrania dźwiękowe, obrazy i inne dane lub kompilacje danych – powinny być dostarczone na dowolnym nośniku, z którego można uzyskać informacje bezpośrednio lub, w razie konieczności, po przetworzeniu na racjonalnie nadającą się do użytku formę. W przypadku opinii, której wynikiem jest zbiór danych przetwarzanych cyfrowo, dostarczenie ich w postaci cyfrowej, na nośniku wydaje się rozwiązaniem najbardziej sensownym, nie tylko z ekonomicznego punktu widzenia.

Należy także zwrócić uwagę na pojawiającą się kwestię przetworzenia na racjonalnie użyteczną formę. Stwierdzenie to nie odnosi się do danych czytelnych bez konieczności przeprowadzania jakiegokolwiek dodatkowej konwersji, jak dokumenty w powszechnie używanych formatach, pliki graficzne, audio czy wideo, ale obejmuje sytuacje kiedy zabezpieczone zostają dane w formatach natywnych wykorzystywanych przez aplikację, czy też system operacyjny. Przykładem takich danych może być, np. baza rozmów komunikatora WhatsApp msgstore.db, czy historia przeglądanych w aplikacji Mozilla Firefox stron internetowych (places.sqlite) lub pliki rejestru systemu operacyjnego Windows (evtx). Za wyjątkiem ostatniego przypadku, nie są to formaty natywne w ścisłym rozumieniu tego słowa, jednakże żadnych z tych przykładowych plików nie można traktować jako zapisanych w racjonalnie nadającej się do użytku formie,

---

<sup>7</sup> Rule 34. Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes w: Federal Rules of Civil Procedure.

<sup>8</sup> <https://www.uscourts.gov/rules-policies/current-rules-practice-procedure/federal-rules-criminal-procedure> - ostatni dostęp w dniu 20.11.2024 r.

<sup>9</sup> <https://www.uscourts.gov/rules-policies/current-rules-practice-procedure/federal-rules-evidence> - ostatni dostęp w dniu 20.11.2024 r.

szczególne dla osób, których wiedza z zakresu szeroko rozumianej informatyki jest raczej szczątkowa. Dostarczenie ekspertyzy, której celem było zabezpieczenie wszystkich danych, w postaci zapisu pełnego i ustrukturyzowanego systemu plików lub kopii binarnej, nie spełnia koniecznego dla opinii wymogu kompletności. Dopiero sparsowanie wszystkich tych danych do interpretowalnego formatu i uzupełnienie o narzędzie do ich dalszej analizy, spowoduje usunięcie tego braku.

Ciekawą propozycję, która może być wykorzystana przez organ zlecający ekspertyzę, zawiera zapis znajdujący się w art. 34 lit. b pkt 1 lit. C FRCP stanowiący, iż wniosek o wydanie danych przechowywanych elektronicznie może określać formę lub formy, w jakich mają być sporządzane informacje przechowywane w formie elektronicznej. Przenosząc ten zapis na grunt wydawanych postanowień, stanowiłby on dyspozycję co do ewentualnej formy w jakiej mają być dostarczone wyekstrahowane dane. Należy nadmienić, iż o ile stosunkowo często wskazywany jest rodzaj nośnika na jakim mają być dostarczone dane, o tyle incydentalnie zdarzają się sytuacje, aby wskazany był konkretny format plików, w jakim mają zostać przedstawione odczytane dane, np. xls czy pdf. Analizując tą kwestię z poziomu możliwości narzędzi dołączanych do zagregowanych danych, w typowych przypadkach akwizycji realizowanej z dysków twardych czy też pamięci telefonów komórkowych, wydaje się to dobrą, choć niezamierzoną do końca, praktyką – prawie każde z nich daje możliwość dalszego eksportu do wielu popularnych formatów wyodrębnionych już, istotnych dla postępowania, danych.

Wykorzystując powyższe założenia, wypracowaliśmy rozwiązanie, które wydaje się rozsądnym kompromisem pomiędzy wymaganiami zaprezentowanymi w art. 200 par. 2 kpk a możliwościami analizy i obróbki danych zgromadzonych w formie cyfrowej. Rozwiązanie to zostało wdrożone w ramach wykorzystywanego w spółce e-Detektywi narzędzia wspomagającego opiniowanie – EDS. Kluczowym założeniem projektowanego systemu było odzwierciedlenie dokumentu papierowego spełniającego wymogi formalne, jakim powinna odpowiadać opinia biegłego, w wersji interaktywnej zapisanej na dołączonym nośniku i umożliwiającej nawigowanie po treści dokumentu i zapoznanie się z załącznikami w wersji cyfrowej. Do stworzenia wersji interaktywnej zastosowane zostało rozwiązanie, nie wymagające ze strony użytkownika końcowego instalowania jakichkolwiek wtyczek czy dodatkowych rozszerzeń, czyli zapis w „czystym” języku HTML, który można odtworzyć w każdej ogólnodostępnej przeglądarce internetowej. Nawigując na poziomie wersji interaktywnej można zarówno zapoznać się z samą treścią opinii, odpowiadającej wersji papierowej, jak również z elementami dodatkowymi, takimi jak, np. skan postanowienia o dopuszczeniu dowodu z opinii biegłego, czy dokumentacja fotograficzna obrazująca cały proces przyjęcia materiału dowodowego do badań. Dołączenie tych materiałów pozwala z jednej strony uniknąć poszukiwania postanowienia w aktach postępowania, gdyż całość dokumentacji związanej z opiniowaniem znajduje się w jednym miejscu, z drugiej zaś umożliwia

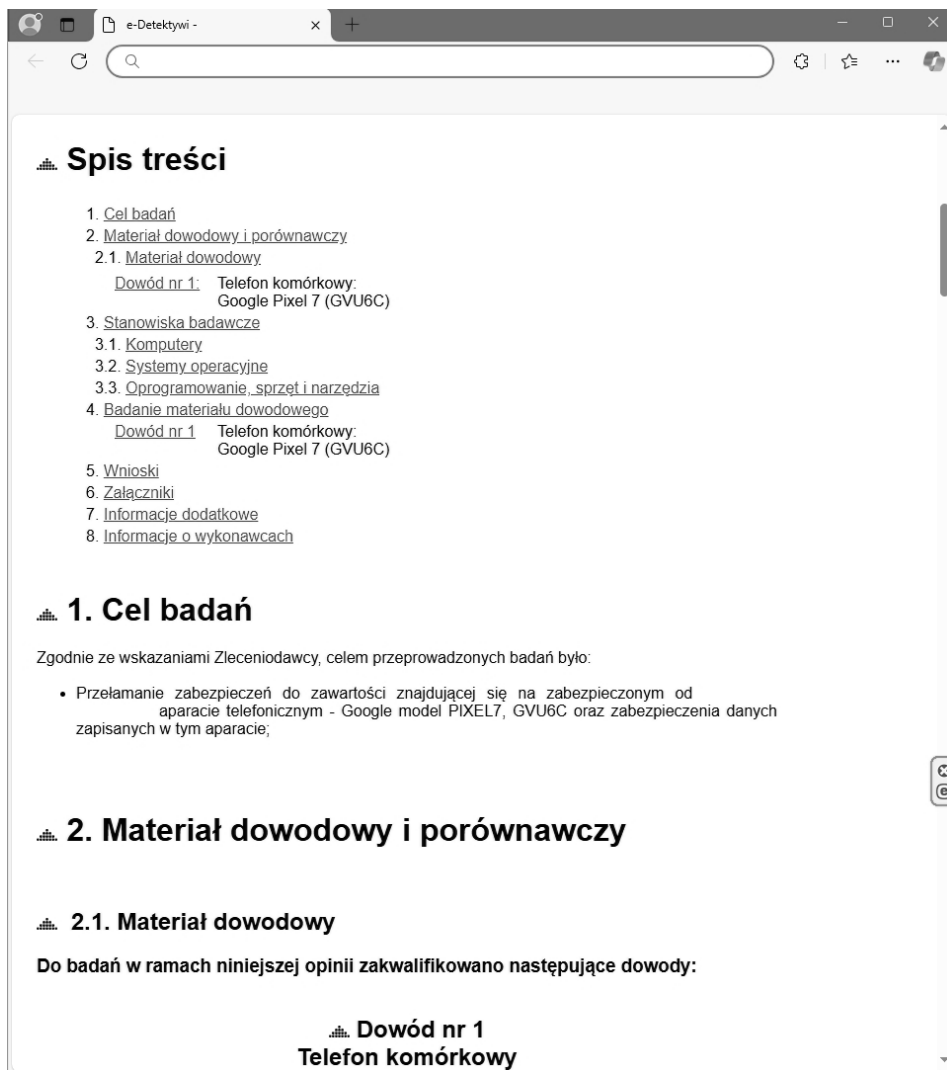
zapoznanie się, np. z przestrzeganiem łańcucha dowodowego, a czasami odniesienie się do podnoszonych przez strony zarzutów, np. co do stanu przekazanych do badań urządzeń.



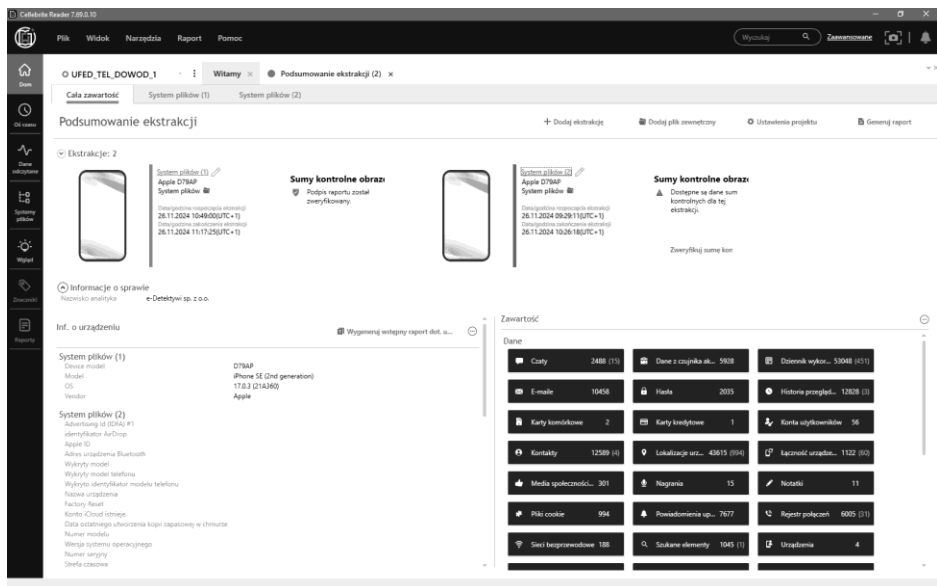
<b>Spis treści</b>	
1.	<u>Cel badań</u>
2.	<u>Materiał dowodowy i porównawczy</u>
2.1.	<u>Materiał dowodowy</u>
	<u>Dowód nr 1:</u> Telefon komórkowy: Google Pixel 7 (GVU6C)
3.	<u>Stanowiska badawcze</u>
3.1.	<u>Komputery</u>
3.2.	<u>Systemy operacyjne</u>
3.3.	<u>Oprogramowanie, sprzęt i narzędzia</u>
4.	<u>Badanie materiału dowodowego</u>
	<u>Dowód nr 1</u> Telefon komórkowy: Google Pixel 7 (GVU6C)
5.	<u>Wnioski</u>
6.	<u>Załączniki</u>
7.	<u>Informacje dodatkowe</u>
8.	<u>Informacje o wykonawcach</u>

Rys. 1. Widok spisu treści opinii w wersji papierowej.

Najważniejszym elementem modułu interaktywnego, w sytuacji gdy przedmiotem opinii było odczytanie wszelkich danych, w tym usuniętych a możliwych do odtworzenia z różnego rodzaju urządzeń cyfrowych, są załączniki zawierające zagregowane dane oraz aplikacje umożliwiające zapoznanie się z nimi. Aplikacje te są dostarczane w wersji udostępnianej przez producenta, i w chwili obecnej, w przypadku rozwiązań stosowanych w spółce e-Detektywi, funkcjonują wyłącznie na komputerach pracujących pod kontrolą systemów z rodziny Microsoft Windows. Oczywiście, jako teoretycznie możliwe, należy uznać wygenerowanie całości danych jako raportu HTML, czy dokumentu (dokumentów) pdf, jednakże korzystanie z nich, zarówno w zakresie wyszukiwania, jak i wyodrębniania pewnych zbiorów danych, należy uznać za mało przydatne. W tym wypadku oczywista wydaje się przewaga narzędzi dostarczanych przez producentów rozwiązań badawczych (tzw. readerów) pozwalających na dalszą analizę danych, bez konieczności posiadania pierwotnej licencji. Aplikacje te pozwalają zarówno na przeszukiwanie danych pod kątem istotnym dla analityka (zakresy dat, słowa kluczowe itp.), jak również tworzenie mniejszych zbiorów danych lub generowanie i wydruk raportów końcowych w różnych popularnych formatach i dołączenie ich do akt postępowania.

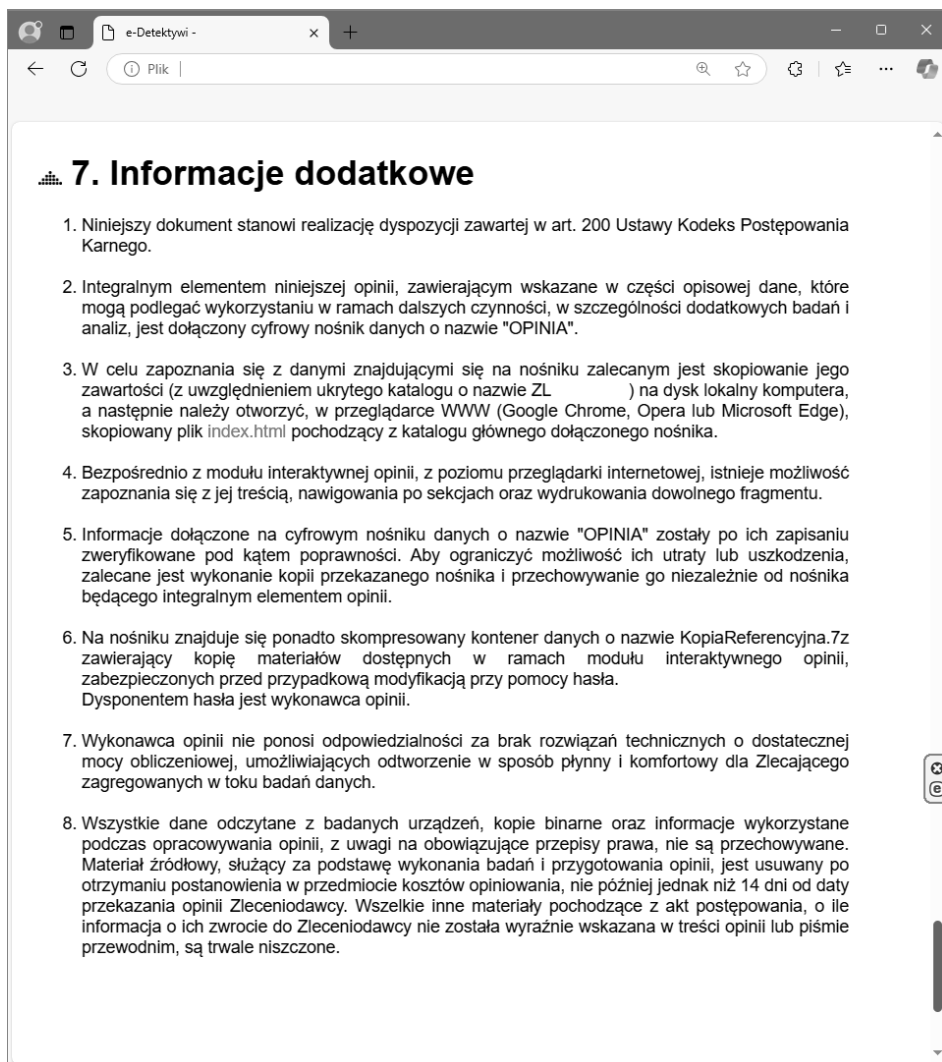


Rys. 2. Widok zrzutu ekranu fragmentu pliku index.html z wersji elektronicznej.



Rys. 3. Widok ekranu głównego narzędzia Cellebrite Reader.

Istotną funkcjonalnością dostarczanych wraz ze zintegrowanymi danymi aplikacji, jest możliwość ich uruchomienia bez konieczności nadawania użytkownikom uprawnień administratora lub zmniejszania poziomu bezpieczeństwa wykorzystywanych urządzeń. Można je uruchomić bezpośrednio z nośnika dołączonego do opinii, jednakże zalecane jest skopiowanie, zarówno aplikacji, jak i kontenerów danych, czyli plików, w których przechowywane są w sposób ustrukturyzowany informacje uzyskane podczas akwizycji danych z badanego urządzenia, na dysk twardy komputera, w celu zwiększenia komfortu pracy. Zasady korzystania z modułu interaktywnego, jak i wszelkie inne istotne informacje dotyczące postępowania z opinią i załącznikami, znajdują się zarówno w wersji papierowej, jak i cyfrowej opinii. Od użytkownika wymaga się jedynie przeczytania ich i postępowania zgodnie z przygotowanymi zaleceniami.



Rys. 4. Widok zrzutu ekranu z informacjami dla użytkownika opinii.

Pracując z dowodami cyfrowymi należy pamiętać o specyficznych cechach, które odróżniają je od innych spotykanych dowodów kryminalistycznych. Kluczową z nich jest możliwość kompromitacji materiału dowodowego poprzez naruszenie jego integralności oraz łatwość zmanipulowania. Dostarczane wraz z opinią jako załączniki kontenery danych wraz z narzędziami do ich odczytu i obróbki, w większości przypadków, mają wbudowane wewnętrzne mechanizmy weryfikacji, niemniej jednak warto pomyśleć o zastosowaniu dodatkowego zabezpieczenia, które zapewni potwierdzenie oryginalności przekazanego materiału dowodowego. W przypadku, jeśli nośniki z załącznikami mają

możliwość dokonywania na nich zapisu – a w większości przypadków, z uwagi na ilość przekazywanych w załącznikach danych, i dołączanie kart pamięci, pendrive'ów czy dysków twardych, taka możliwość istnieje – warto rozważyć wprowadzenie dodatkowej metody zabezpieczenia zawartości. W naszym rozwiązaniu zastosowaliśmy mechanizm tzw. kopii referencyjnej. Jest to zaszyfrowane archiwum z kompletną zawartością modułu interaktywnego opinii, dla którego wyliczona została suma kontrolna w postaci funkcji skrótu SHA-256. Hasło do archiwum jest przechowywane u wykonawcy opinii. W przypadku podejrzenia naruszenia integralności danych stanowiących załącznik do opinii istnieje możliwość wystąpienia do dysponenta hasła z wnioskiem o odszyfrowanie zabezpieczonego pliku. W celu uniemożliwienia zmanipulowania kopii referencyjnej, plik z wyliczoną sumą kontrolną może być dodatkowo zabezpieczony, np. poprzez podpisanie go przy wykorzystaniu kwalifikowanego podpisu elektronicznego.

Za warte rozważenia rozwiązanie należy także uznać rozszerzenie treści przekazywanych zleceniodawcy o tzw. dane surowe, uzyskane na etapie odczytu zawartości nośnika urządzenia czy też wykonywania jego kopii binarnej. Dołączenie ich do opinii pozwala, w przypadku konieczności przeprowadzenia ponownych badań przy wykorzystaniu nowszych wersji aplikacji, na pominięcie procesu akwizycji z urządzenia, która z różnych powodów może być niemożliwa (np. zostało ono zwrócone użytkownikowi lub w wyniku zdarzenia losowego nastąpiła jego utrata lub zniszczenie). Dysponując odpowiednio uwierzytelnionymi danymi surowymi możemy przeprowadzić ponowną ich analizę przy wykorzystaniu innych rozwiązań lub rozwiązania tego samego producenta, ale w nowszej wersji umożliwiającej rozpoznanie i sparsowanie większej ilości danych – większość rozwiązań badawczych wykorzystywanych w informatyce śledczej jest kompatybilna wstecz.

## **PROBLEMY I OGRANICZENIA**

Oczywistym jest, iż w przypadku nowo wdrażanych koncepcji, na początkowym etapie funkcjonowania napotykamy na szereg problemów i ograniczeń, które mają swoje źródło zarówno po stronie wytwórcy opinii jak i po stronie jej odbiorcy. O ile, na część problemów leżących po stronie wykonawcy opinii, można znaleźć rozwiązanie podczas jej powstawania, stosunkowo mało możliwości pozostaje wykonawcy opinii aby rozwiązać problemy po stronie użytkownika końcowego, przy czym często także on sam nie ma żadnego wpływu na niektóre z nich.

Jednym z najbardziej trywialnych problemów, a jednocześnie najczęściej raportowanych w informacji zwrotnej, jest brak zrozumienia zasad funkcjonowania modułu cyfrowego opinii, w tym zasad korzystania z dołączonych załączników. Podnieść należy, iż problem ten, w większości przypadków jest pochodną pobieżnego zapoznania się z opinią, rzadziej zaś jest spowodowany brakiem podstawowych kompetencji cyfrowych po stronie osób zapoznających się z przekazanym materiałem. Rozwiązanie tego problemu znajduje się w zasięgu zlecającego – wystarczy szczegółowo i dokładnie zapoznać się z materiałami informacyjnymi dołączanymi do opinii. W celu jeszcze

łatwiejszego korzystania z dołączonych materiałów, przygotowywane są też samouczki wideo, dostarczane zlecającemu wraz z wersją elektroniczną opinii, a obejmujące zarówno zasady ogólne korzystania z opinii w wersji elektronicznej, jak i z narzędzi pozwalających na nawigację po danych wyekstrahowanych z badanych urządzeń. To ostatnie rozwiązanie zostało wprowadzone dopiero wówczas, kiedy okazało się, iż informacje zawarte w treści opinii (zarówno w wersji drukowanej, jak i cyfrowej) okazują się być, z różnych powodów, niewystarczające.

Problemem zasygnalizowanym w poprzednim akapicie, na który wykonujący opinię nie ma żadnego wpływu, jest brak kompetencji cyfrowych osób, które zapoznają się z przekazanym materiałem. Nie można mówić o jakimkolwiek efektywnym wykorzystaniu przekazanego materiału dowodowego w sytuacji, kiedy prowadzący postępowanie przygotowawcze nie posiada podstawowej wiedzy w zakresie korzystania z komputera, zarówno w zakresie konfigurowania jego podstawowych ustawień, jaki i efektywnego korzystania z przeglądarek internetowych. W takiej sytuacji, nawet najlepiej przygotowane i intuicyjne rozwiązanie się nie sprawdzi.

Kolejną przeszkodą jest brak po stronie odbiorcy opinii komputerów umożliwiających zapoznanie się dostarczonymi materiałami. Jeżeli w 2024 roku, w jednostkach Policji wykorzystywane są nadal urządzenia pracujące pod kontrolą systemu operacyjnego Microsoft Windows 7, to nie można mieć złudzeń, iż komputer taki pozwoli na uruchomienie narzędzia analitycznego i odtworzenie danych odczytanych z telefonu komórkowego, który swoimi parametrami przewyższa urządzenie pozostające w dyspozycji organów ścigania. I trudno odpowiedzialnością za ten fakt obarczać wykonawcę opinii, aczkolwiek zauważyć należy, iż to nie po stronie pionów wykonawczych organów ścigania i wymiaru sprawiedliwości znajdują się kompetencje w zakresie modernizacji i wymiany przestarzałego sprzętu.

Ostatnim z zauważonych problemów, jaki pojawia się podczas wykorzystania cyfrowej wersji opinii z dowodu biegłego jest brak chęci współpracy pionów wykonawczych organów ścigania i instytucji wymiaru sprawiedliwości z pionami IT odpowiedzialnymi za cyberbezpieczeństwo tych instytucji. Bardzo często, z uwagi na stosowane zabezpieczenia i wdrożoną politykę bezpieczeństwa, nie jest możliwe skorzystanie z nośników dostarczanych wraz z opinią na komputerach posiadających dostęp do sieci wewnętrznych zlecającego. I podobnie, jak w przypadku omawianym powyżej rozwiązanie tego problemu leży poza zakresem możliwości i kompetencji wykonawcy opinii. Jako ciekawostkę można wskazać fakt, iż niekiedy odbiorca opinii nie ma możliwości podłączenia zewnętrznych urządzeń przez port USB komputera służbowego, a jednocześnie brak jest jakichkolwiek ograniczeń w korzystaniu z wbudowanego czytnika nośników optycznych.

## PODSUMOWANIE I WNIOSKI

Postępujący rozwój technologiczny i specjalizacja powodują, iż w niedalekiej przyszłości możemy się spodziewać coraz większej cyfryzacji prowadzonych postępowań. I nie chodzi tu tylko o wdrażany w polskim sądownictwie system cyfrowej rejestracji przebiegu rozpraw sądowych, który podobnie jak w przypadku omawianym w niniejszym opracowaniu, traktuje niejako pomocniczo pisemną część protokołu rozprawy w stosunku do protokołu elektronicznego, w pełni oddającego rzeczywisty przebieg rozprawy. Ilość i różnorodność przetwarzanych danych w urządzeniach cyfrowych, będzie wymuszała przedstawianie ich przy wykorzystaniu specjalistycznych rozwiązań, ograniczając jednocześnie wartość wyłącznie papierowej formy opinii, czy też wydruku tych danych. Wzrost roli i znaczenia informacji przechowywanych elektronicznie spowoduje konieczność wypracowania jednolitych zasad i procedur postępowania z nimi, oraz wdrożenie ich do powszechnego stosowania zarówno na etapie postępowania przygotowawczego jak i sądowego. To z kolei pozwoli na przyspieszenie i ułatwienie pracy z dużymi zbiorami danych, jak również na efektywne ich wykorzystanie przez organy ścigania i instytucje wymiaru sprawiedliwości.

## LITERATURA

1. Gaberle A., Dowody w sądowym procesie karnym. Teoria i praktyka. Wydanie II, Wolters Kluwer 2010.
2. Federal Rules of Civil Procedure - <https://www.uscourts.gov/rules-policies/current-rules-practice-procedure/federal-rules-civil-procedure>.
3. Federal Rules of Criminal Procedure - <https://www.uscourts.gov/rules-policies/current-rules-practice-procedure/federal-rules-criminal-procedure>.
4. Federal Rules of Evidence - <https://www.uscourts.gov/rules-policies/current-rules-practice-procedure/federal-rules-evidence>.
5. Lewulis P., Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym, Wydawnictwa Uniwersytetu Warszawskiego 2021.
6. Oettinger W., Informatyka śledcza. Gromadzenie, analiza i zabezpieczanie dowodów elektronicznych dla początkujących. Wydanie II, Helion 2023.
7. Ustawa z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (t.j. Dz. U. z 2024 r. poz. 1568 z późn. zm.).
8. Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (t.j. Dz. U. z 2024 r. poz. 37 z późn. zm.).

# PRZESTĘPCZOŚĆ TELEINFORMATYCZNA - GARŚĆ STATYSTYK

## ICT CRIME - A HANDFUL OF STATISTICS

Maciej SZMIT<sup>1</sup>

**Streszczenie:** Rozdział omawia wybrane statystyki incydentów bezpieczeństwa informacji oraz przestępstw komputerowych w Polsce oraz metodologiczne skutki niespójności sposobów zbierania danych w tym zakresie.

**Słowa kluczowe:** statystyka prawnicza, przestępczość komputerowa, incydenty bezpieczeństwa informacji.

**Summary:** The chapter discusses selected statistics of information security incidents and computer crimes in Poland and the methodological consequences of inconsistency in data collection methods in this area.

**Keywords:** crime descriptive statistics, computer crimes, information security incidents.

### UWAGI WSTĘPNE

Rozumne działanie w zakresie nauk społecznych powinno wykorzystywać – wszędzie tam, gdzie jest to metodologicznie uzasadnione i osiągalne – podejście oparte o dowody (ang. evidence based approach). Do analizy i interpretacji takich dowodów służą między innymi metody statystyczne, jak również sztucznej inteligencji, pozwalające na ilościową ocenę zjawisk, na przykład pomiar dynamiki zmian, oszacowanie siły zależności pomiędzy zmiennymi czy klasyfikację jednostek statystycznych do odpowiednich zbiorów. Jednak, aby z danych móc wydobyć informację, konieczne jest, żeby zebrane były one w sposób sensowny. Żadna, nawet najbardziej zaawansowana metoda, nie potrafi bowiem wygenerować informacji ex nihilo. Jeśli dane są niespójne, niewiarygodne czy nadmiernie zaszumione, próba ich analizy prowadzić będzie do sytuacji opisywanej slangowym skrótowcem GIGO (ang. Garbage In – Garbage Out). Stąd też kapitalne znaczenie ma właściwe zbieranie danych. Jednym z jego warunków, przynajmniej, jeśli mowa o analizie dynamiki zjawisk, jest stosowanie przez cały czas tego samego sposobu zbierania danych, o jednakowo zdefiniowanej cesze statystycznej, a przynajmniej możliwość łatwego przeliczenia zebranych danych, tak aby otrzymać wartość tej cechy. Choć to wszystko, co napisano powyżej wydaje się być wiedzą

---

<sup>1</sup> Uniwersytet Łódzki, maciej.szmit@uni.lodz.pl; ORCID: 0000-0002-6115-9213.

elementarną, praktyka pokazuje, że – przynajmniej w odniesieniu do przestępczości teleinformatycznej – wiedza ta wydaje się być z jakiegoś powodu nieznaną, a przynajmniej nie stosowaną w praktyce. W konsekwencji nie można sensownie badać dynamiki przestępczości, ocenić choćby skuteczności działań prewencyjnych czy naprawczych, szacować ryzyka związanego z poszczególnymi rodzajami przestępstw itd. W miejsce rozważanego od lat przez futurologów wsparcia władzy ustawodawczej czy sądowniczej przez prawometrię czy sztuczną inteligencję, rola nauki sprowadza się do co najwyżej studiów poszczególnych przypadków oraz – jak powiedziano wyżej – poważnie ułomnej metodologicznie rejestracji liczby zjawisk.

## **STATYSTYKI PRZESTĘPCZOŚCI**

Do roku 2020 upubliczniane były z jednej strony statystyki policyjne (strona [statystyka.policja.pl](http://statystyka.policja.pl)), w których można było znaleźć liczby postępowań wszczętych oraz przestępstw stwierdzonych (zob. Tabela 1) a z drugiej – statystyki Ministerstwa Sprawiedliwości o liczbie skazań dorosłych według czynu głównego (zob. Tabela 2). Porównując rzędy wielkości tych liczb (stwierdzonych przestępstw i skazań) można było oszacować – wprawdzie bardzo zgrubnie – skuteczność prawnej ochrony bezpieczeństwa informacji.

Sytuacja uległa zmianie w roku 2021. Zgodnie z zarządzeniem Ministra Sprawiedliwości z dnia 19 stycznia 2021 r. w sprawie wzorów formularzy statystycznych w sądach powszechnych i wojskowych (Dz. U. M. S. poz. 4) wszystkie sądy powszechne i wojskowe mają obowiązek przygotować odpowiednie zestawienia statystyczne dotyczące między innymi przestępstw i przekazać je do Ministerstwa Sprawiedliwości. Poszczególne sądy publikują zazwyczaj również odpowiednie zestawienia na swoich stronach www, jednak z oczywistych względów próba zebrania danych, czy to ze stron bez mała czterystu sądów, czy w drodze ich odpytywania byłaby niezwykle czasochłonna. Dla lat 2021 oraz 2022 Ministerstwo Sprawiedliwości opublikowało na stronie Informatora Statystycznego Wymiaru Sprawiedliwości zestawienia informacji o wybranych rodzajach przestępstw (ale nie ma wśród nich, m.in. przestępstw komputerowych). Sytuacja taka stała się przyczyną wystosowania przez Fundację „Indicium” petycji z postulatem o rozpoczęcie publikacji sumarycznych informacji statystycznych w Biuletynie Informacji Publicznej Ministerstwa Sprawiedliwości. Ministerstwo opublikowało raporty zbiorcze za rok 2023 na tyle szczegółowe, że można poznać z nich statystyki nie tylko przestępstw, ale również wykroczeń (co jest nowością w stosunku do raportów z lat 2006-2020), na przykład wykroczenia zoombombingu (art. 107a KW): w roku 2023 wszczęto 65 postępowań, w pierwszej instancji zapadło 70 rozstrzygnięć, 4 postępowania umorzono, 54 razy orzeczono kary, dwa razy orzeczono uniewinnienie.

Tabela 1. Statystyki policyjne wybranych przestępstw przeciwko ochronie informacji: liczba postępowań wszczętych i przestępstw stwierdzonych przez policję.

Rok	Naruszenie tajemnicy korespondencji (art. 267)		Udaremnienie lub utrudnienie korzystania z informacji (art. 268 i 268a)		Niszczenie danych informatycznych (art. 269)		Sabotaż komputerowy (art. 269a)		Wytwarzanie programu komputerowego do popełnienia przestępstwa (art. 269b)	
	Liczba post. wszczęt.	Liczba przest. stwierdz.	Liczba post. wszczęt.	Liczba przest. stwierdz.	Liczba post. wszczęt.	Liczba przest. stwierdz.	Liczba post. wszczęt.	Liczba przest. stwierdz.	Liczba post. wszczęt.	Liczba przest. stwierdz.
1999	182	113	59	49	10	1	-	-	-	-
2000	249	240	66	48	7	5	-	-	-	-
2001	259	175	60	118	9	5	-	-	-	-
2002	294	215	89	167	6	12	-	-	-	-
2003	362	232	114	138	2	2	-	-	-	-
2004	378	248	105	89	12	0	-	-	-	-
2005	430	260	152	98	2	3	1	1	6	6
2006	538	370	201	136	3	4	19	19	9	9
2007	616	384	244	168	6	0	11	11	4	4
2008	694	505	366	249	6	2	13	13	12	12
2009	982	645	555	1 115	6	2	34	243	23	18
2010	1 194	1 102	690	479	7	0	22	18	35	71
2011	1 583	948	885	629	3	5	38	30	38	29
2012	1 657	1 513	796	884	9	5	35	30	21	27
2013	2 203	1 655	765	589	14	9	37	34	42	28
2014	2 868	1 901	743	572	10	6	27	48	47	43

Tabela 2. Statystyki skazań za wybrane przestępstwa przeciwko ochronie informacji: liczba prawomocnych skazań osób dorosłych za przestępstwa komputerowe – czyn główny, sprawy z oskarżenia publicznego.

Rok	Naruszenie tajemnicy korespondencji (art. 267)											Udaremnienie lub utrudnienie korzystania z informacji (art. 268 i 268a)			
	Art.2 67 §1 kk	Art.2 67 §2 kk	Art.2 67 §3 kk	Art.2 67 §3 zw. z §1	Art.2 67 §4 kk	Art.2 67 §4 zw. z §1	Art.2 67 §4 kk w zw. z §2	Art.2 67 §4 kk w zw. z §3	Art.26 7 §4 kk w zw. z §3	Art.2 68 §1 kk	Art.2 68 §2 kk	Art.2 68 §3 kk	Art.2 68 §3 zw. z §1	Art.2 68a §1 kk	Art.2 68a §2 kk
2006	22	8		13						14	7		1	3	
2007	23	16	1	3						11	7			9	
2008	29	6	1							19	13			17	
2009	42	3	1	3	1					13	5			25	
2010	52		11	4	1					12	11	1		33	1
2011	37	1	7							12	5	2		40	
2012	49	3	14		1	5				8	2			28	
2013	47	2	6			1				4	5			22	
2014	44		11							5	6	1		18	
2015	35	1	21							7	3	1		24	
2016	52	5	25		2	1				15	5	1		16	
2017	50	2	39		2					11	3	1		15	
2018	59	9	41		3	3		2		4	7			20	
2019	65	4	51			1	1			8	1			17	
2020	45	6	50		1	2		2		9	3			15	1

Tabela 3. Statystyki skazań za wybrane przestępstwa przeciwko ochronie informacji: liczba prawomocnych skazań osób dorosłych za przestępstwa komputerowe – czyn główny, sprawy z oskarżenia publicznego.

Rok	Niszczenie danych informatycznych (art. 269)		Sabotaż komputerowy (art.269a)	Wytwarzanie programu komputerowego do popełnienia przestępstwa (art. 269b)		
	Art.269 §1 kk	Art.269 §2 kk		Art.269a kk	Art.269b §1 kk	Art.269b §1 kk w zw. z art.165 §1 pkt 4 kk
2006		1	1			1
2007	3		2			
2008	1	2	1		1	
2009		1	2	3		
2010	1	1	3	1		
2011			6	4		
2012			3	2		1
2013			4	1		
2014			1	1		
2015			4	1		
2016			2	2	1	
2017	1			3		
2018			1	3		
2019	1		4	2		
2020	1			3		

*Źródło: Dane za lata 2006-2007 za: Szmit M.: Wybrane zagadnienia opiniowania sądowo-informatycznego, Wydanie II, rozszerzone i uzupełnione, Polskie Towarzystwo Informatyczne, Warszawa 2014 s. 131 i nast. Skazania w latach 2008-2020 wg <https://isws.ms.gov.pl> Informator Statystyczny Wymiaru Sprawiedliwości (arkusz „Skazania prawomocne z oskarżenia publicznego - dorosli - wg rodzajów przestępstw i wymiaru kary w l.2008-2020”).*

Podobne statystyki można znaleźć oczywiście również dla poszczególnych przestępstw wymienionych w tabelach 1 oraz 2, niemniej dane takie będą nieporównywalne: do 2020 roku publikowane były informacje o liczbie prawomocnie skazanych dorosłych, a w danych z roku 2023 – o liczbie skazanych, niezależnie od wieku, w pierwszej instancji (zob. Tabela 4), choć więc dane z roku 2023 są bardziej szczegółowe, nie da się z nich wyliczyć wartości poprzednio badanej cechy statystycznej, a więc nie da się scharakteryzować *dynamiki jej zmian*.

Tabela 4. Statystyki skazań za wybrane przestępstwa przeciwko ochronie informacji: liczba osób osądzonych oraz skazanych za przestępstwa komputerowe

Rok	Art.267 §1 kk		Art. 268a kk		Art. 269 kk	
	Osądz.	Skazanych	Osądz.	Skazanych	Osądz.	Skazanych
2023	159	98	45	32	3	3

Rok	Art. 269a KK		Art. 269b KK	
	Osądz.	Skazanych	Osądz.	Skazanych
2023	4	2	21	5

*Źródło: Informator Statystyczny Wymiaru Sprawiedliwości <https://isws.ms.gov.pl> Informator Statystyczny Wymiaru Sprawiedliwości.*

Interesujące mogłoby być na przykład również sprawdzenie, czy potwierdziły się – formułowane w literaturze przedmiotu – obawy dotyczące podobieństwa ustawowych znamion czynów zabronionych określonych w dyspozycji nowego artykułu KW oraz w artykułach 268 i 268a KK i „udaremnianiem lub utrudnianiem przekazywania informacji” z art. 107a § 1 KW. Przesłanką przemawiającą za potwierdzeniem takiej hipotezy mógłby być spadek (ewentualnie zaburzenia trendu) dynamiki skazań z tych artykułów KK po uchwaleniu zmian w KW (ustawą z dnia 19 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19, Dz.U. z 2020 r. poz. 1086, zwaną Tarcza 4.0). Niestety, z powodów wymienionych powyżej, a także z powodu braku danych dla lat 2021 oraz 2022, nie można takiego wniosku przeprowadzić. Wyjątkiem zdaje się być art. 268 KK, z którego nie było żadnego skazania (a przynajmniej w raportach nie ma informacji na ten temat). Być może więc rzeczywiście wykroczenie zoombombingu „skonsumowało” przestępstwo utrudniania zapoznania się z informacją, trudno jednak uznać za mocny dowód pojedynczy pomiar. Pozostaje mieć nadzieję, że dane za lata 2021 i 2022 zostaną udostępnione. Ministerstwo Sprawiedliwości utrzymuje, że zamierza to uczynić (zob. Rys. 1).

## STATYSTYKI CERT/CSIRT

Statystyki zespołów CERT (zarówno krajowych jak i dużych operatorów sieciowych) są cennym źródłem informacji o złośliwych aktywnościach w sieciach, a przynajmniej powinny być takim źródłem, gdyby statystyki były zbierane odpowiednio. Na mocy ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa utworzono, w miejsce jednego zespołu CERT.PL, trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego: CSIRT MON, CSIRT GOV oraz CSIRT NASK. Odnosnie do statystyk CERTów - CERT.PL (wchodzący w skład CSIRT NASK) stosuje od lat tę samą VI wersję klasyfikacji przyjętej przez European CSIRT Network, co ułatwia porównanie danych za kolejne lata, z wyjątkiem ostatniego raportu (za rok 2023), w którym zastosowano już agregację na wyższym niż poprzednio poziomie.



DSF-II.082.151.2024  
Warszawa, 28 maja 2024 r.

Pan  
dr inż. Maciej Szmit

Szanowny Panie

W odpowiedzi na korespondencję z dnia 20 maja 2024 roku Departament Strategii i Funduszy Europejskich uprzejmie informuje, że na portalu Informator Statystyczny Wymiaru Sprawiedliwości (ISWS) <https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/> zamieszczone są pliki o tytułach „Skazania prawomocne z oskarżenia publicznego - dorośli - w latach 2002-2020” i „Skazania prawomocne z oskarżenia publicznego - dorośli - wg rodzajów przestępstw i wymiaru kary w l.2008-2020.

Dane statystyczne dotyczące prawomocnie skazanych osób dorosłych gromadzone są na podstawie bazy danych statystycznych Krajowego Rejestru Karnego w cyklach rocznych, informacje za lata 2021-2023 będą dostępne w terminie późniejszym.

Drugim głównym źródłem danych są sprawozdania statystyczne wypełniane przez pracowników sądów powszechnych poprzez system informatyczny dedykowany dla potrzeb sprawozdawczości statystycznej.

Należy mieć na uwadze, że zasób danych gromadzonych w sprawozdaniach statystycznych ograniczony jest budową formularzy, a co za tym idzie nie ma możliwości wyodrębnienia wszystkich informacji na temat spraw toczących się w sądach w sposób szczegółowy. Wzory sprawozdań statystycznych znajdują się do wglądu na portalu ISWS pod adresem <https://isws.ms.gov.pl/pl/baza-statystyczna/wzory-formularzy/> , natomiast sprawozdania statystyczne za rok 2023 pod adresem <https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-jednoroczne-w-tym-pliki-dostepne-cyfrowo/rok-2023/download,3858,3.html> .

Z wyrazami szacunku  
Piotr Krasieński  
Dyrektor  
Departament Strategii i Funduszy Europejskich  
/podpisano elektronicznie/

*Rys. 3. Odpowiedź Ministerstwa Sprawiedliwości na zapytanie o dane.*

*Źródło: archiwum autora*

Tabela 5. Wybrane statystyki incydentów CERT.PL.

Rok	Atak blokujący serwis (DoS)	Rozproszony atak blokujący serwis (DDoS)	Sabotaż komputerowy	Złośliwe oprogramowanie	Ogólna liczba incydentów
1996	.	.	.	.	50
1997	.	.	.	.	75
1998	.	.	.	.	100
1999	.	.	.	.	105
2000	.	.	.	.	126
2001	.	.	.	.	741
2002	.	.	.	.	1013
2003	10	10	0	80	1196
2004	15	62	0	165	1222
2005	13	14	1	594	2516
2006	20	19	1	340	2427
2007	8	32	0	295	2108
2008	4	22	0	276	1796
2009	5	11	0	193	1292
2010	1	10	0	91	674
2011	3	11	0	46	605
2012	8	17	0	226	1082
2013	0	43	0	746	1219
2014	6	63	0	98	1282
2015	2	33	0	142	1456
2016	3	30	2	211	1926
2017	11	41	0	854	3182
2018	7	35	0	862	3739
2019	4	33	1	969	6484
2020	0	43	0	746	10420
2021	6	74	1	2847	29483
2022	6	97	0	3409	39683
2023 <sup>1</sup>	.	.	.	1650 <sup>2</sup>	80267

<sup>1</sup> W raporcie z 2023 roku podano statystyki na wyższym poziomie agregacji tej samej klasyfikacji, stąd brak części danych. Warto odnotować, że w roku 2023 niemal 95% incydentów (75917 szt.) zaliczono do kategorii „oszustwa komputerowe”.

<sup>2</sup> Opisane jako „szkodliwe oprogramowanie”.

*Źródła:*

- *[https://cert.pl/uploads/docs/Raport\\_CP\\_2023.pdf](https://cert.pl/uploads/docs/Raport_CP_2023.pdf);*
- *Raport roczny z działalności CERT Polska 2022. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2022.pdf](https://cert.pl/uploads/docs/Raport_CP_2022.pdf);*
- *Raport roczny z działalności CERT Polska 2021. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2021.pdf](https://cert.pl/uploads/docs/Raport_CP_2021.pdf);*
- *Raport roczny z działalności CERT Polska 2020. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2020.pdf](https://cert.pl/uploads/docs/Raport_CP_2020.pdf);*
- *Raport roczny z działalności CERT Polska 2019. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2019.pdf](https://cert.pl/uploads/docs/Raport_CP_2019.pdf);*
- *Raport roczny z działalności CERT Polska 2018. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2018.pdf](https://cert.pl/uploads/docs/Raport_CP_2018.pdf);*
- *Raport roczny z działalności CERT Polska 2017. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2017.pdf](https://cert.pl/uploads/docs/Raport_CP_2017.pdf);*
- *Raport roczny z działalności CERT Polska 2016. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2016.pdf](https://cert.pl/uploads/docs/Raport_CP_2016.pdf);*
- *Raport roczny z działalności CERT Polska 2015. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2015.pdf](https://cert.pl/uploads/docs/Raport_CP_2015.pdf);*
- *CERT Polska Raport 2014. [https://cert.pl/uploads/docs/Raport\\_CP\\_2014.pdf](https://cert.pl/uploads/docs/Raport_CP_2014.pdf);*
- *CERT Polska Raport 2013. [https://cert.pl/uploads/docs/Raport\\_CP\\_2013.pdf](https://cert.pl/uploads/docs/Raport_CP_2013.pdf);*
- *Raport 2012 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne [https://cert.pl/uploads/docs/Raport\\_CP\\_2012.pdf](https://cert.pl/uploads/docs/Raport_CP_2012.pdf);*
- *Raport 2011 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne w roku 2011 [https://cert.pl/uploads/docs/Raport\\_CP\\_2011.pdf](https://cert.pl/uploads/docs/Raport_CP_2011.pdf);*
- *Raport 2010 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne [https://cert.pl/uploads/docs/Raport\\_CP\\_2010.pdf](https://cert.pl/uploads/docs/Raport_CP_2010.pdf);*
- *Raport 2009 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2009 [https://cert.pl/uploads/docs/Raport\\_CP\\_2009.pdf](https://cert.pl/uploads/docs/Raport_CP_2009.pdf);*
- *Raport 2008 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2008 [https://cert.pl/uploads/docs/Raport\\_CP\\_2008.pdf](https://cert.pl/uploads/docs/Raport_CP_2008.pdf);*
- *Raport 2007 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2007 [https://cert.pl/uploads/docs/Raport\\_CP\\_2007.pdf](https://cert.pl/uploads/docs/Raport_CP_2007.pdf);*
- *Raport 2006 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2006 [https://cert.pl/uploads/docs/Raport\\_CP\\_2006.pdf](https://cert.pl/uploads/docs/Raport_CP_2006.pdf);*

- *Raport 2005 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2005*  
[https://cert.pl/uploads/docs/Raport\\_CP\\_2005.pdf](https://cert.pl/uploads/docs/Raport_CP_2005.pdf);
- *Raport 2004 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2004*  
[https://cert.pl/uploads/docs/Raport\\_CP\\_2004.pdf](https://cert.pl/uploads/docs/Raport_CP_2004.pdf);
- *Raport 2003 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespołu CERT Polska w roku 2003*  
[https://cert.pl/uploads/docs/Raport\\_CP\\_2003.pdf](https://cert.pl/uploads/docs/Raport_CP_2003.pdf)

CSIRT GOV (CERT.GOV.PL) raportuje incydenty od 2010 roku stosując inny podział, a w zasadzie inne podziały. Sposób klasyfikacji był wielokrotnie zmieniany, co więcej, użyta typologia wydaje się być nie do końca spójna. Dla przykładu: w poszczególnych latach występują obok siebie takie kategorie jak „atak” i „niedostępność” (choć oczywiście niedostępność usługi bądź zasobu może być skutkiem ataku) i „DDoS” (choć rozproszony atak odmowy usług ma na celu właśnie naruszenie dostępności), „podatność” (a nie jest przecież ona incydem bezpieczeństwa informacji) itd. Co ciekawe, ogólna liczba incydentów w 2022 roku według CERT.GOV.PL wyniosła 3 1234040, a więc była ponad piętnastokrotnie wyższa niż liczba incydentów raportowana przez CERT.PL. Oczywiście nie można z tego wysnuwać wniosku, że piętnastokrotnie razy częściej atakowano sieć rządową niż resztę polskiego Internetu, tylko że metodologia zbierania i klasyfikowania danych o incydentach jest zupełnie różna, co jest kolejnym elementem utrudniającym wykorzystanie takich danych.

Trzeci z wymienionych w ustawie zespołów – CERT MON – nie publikuje informacji statystycznych o incydentach.

## **PODSUMOWANIE**

Jak wspomniano powyżej, głębsza analiza danych dotyczących przestępczości komputerowej jest, przy przyjętych sposobach ich zbierania, zadaniem w zasadzie niemożliwym. Powstaje pytanie, czy w takiej sytuacji można mówić o racjonalnym kształtowaniu polityki karnej, przynajmniej odnośnie do przestępczości komputerowej? Jak się wydaje – przynajmniej w zakresie poruszonym w niniejszym tekście i przynajmniej w odniesieniu do postulatu evidence based approach – nie ma przesłanek, by na to pytanie odpowiedzieć pozytywnie.

---

<sup>3</sup> Za: Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku,  
<https://csirt.gov.pl/download/3/214/RaportostaniebezpieczenstwacyberprzestrzeniRPw2022.pdf>

## BIBLIOGRAFIA

1. CERT Polska Raport 2013. [https://cert.pl/uploads/docs/Raport\\_CP\\_2013.pdf](https://cert.pl/uploads/docs/Raport_CP_2013.pdf)
2. CERT Polska Raport 2014. [https://cert.pl/uploads/docs/Raport\\_CP\\_2014.pdf](https://cert.pl/uploads/docs/Raport_CP_2014.pdf)
3. Fundacja „Indicium”: Petycja w zakresie rozpoczęcia publikacji wybranych informacji statystycznych sądów powszechnych oraz wojskowych <https://www.gov.pl/attachment/28dfd886-4c50-4921-99fd-30d7084c2a56>
4. Informator Statystyczny Wymiaru Sprawiedliwości <https://isws.ms.gov.pl>
5. Raport 2003 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2003 [https://cert.pl/uploads/docs/Raport\\_CP\\_2003.pdf](https://cert.pl/uploads/docs/Raport_CP_2003.pdf)
6. Raport 2004 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2004 [https://cert.pl/uploads/docs/Raport\\_CP\\_2004.pdf](https://cert.pl/uploads/docs/Raport_CP_2004.pdf)
7. Raport 2005 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2005 [https://cert.pl/uploads/docs/Raport\\_CP\\_2005.pdf](https://cert.pl/uploads/docs/Raport_CP_2005.pdf)
8. Raport 2006 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2006 [https://cert.pl/uploads/docs/Raport\\_CP\\_2006.pdf](https://cert.pl/uploads/docs/Raport_CP_2006.pdf)
9. Raport 2007 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2007 [https://cert.pl/uploads/docs/Raport\\_CP\\_2007.pdf](https://cert.pl/uploads/docs/Raport_CP_2007.pdf)
10. Raport 2008 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2008 [https://cert.pl/uploads/docs/Raport\\_CP\\_2008.pdf](https://cert.pl/uploads/docs/Raport_CP_2008.pdf)
11. Raport 2009 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne zgłaszanych do zespół CERT Polska w roku 2009 [https://cert.pl/uploads/docs/Raport\\_CP\\_2009.pdf](https://cert.pl/uploads/docs/Raport_CP_2009.pdf)
12. Raport 2010 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne [https://cert.pl/uploads/docs/Raport\\_CP\\_2010.pdf](https://cert.pl/uploads/docs/Raport_CP_2010.pdf)
13. Raport 2011 CERT Polska analiza incydentów naruszających bezpieczeństwo teleinformatyczne w roku 2011 [https://cert.pl/uploads/docs/Raport\\_CP\\_2011.pdf](https://cert.pl/uploads/docs/Raport_CP_2011.pdf)
14. Raport 2012 CERT Polska. Analiza incydentów naruszających bezpieczeństwo teleinformatyczne [https://cert.pl/uploads/docs/Raport\\_CP\\_2012.pdf](https://cert.pl/uploads/docs/Raport_CP_2012.pdf)
15. Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2022 roku, <https://csirt.gov.pl/download/3/214/RaportostaniebezpieczenstwacyberprzestrzeniRPw2022.pdf>
16. Raport roczny z działalności CERT Polska 2015. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2015.pdf](https://cert.pl/uploads/docs/Raport_CP_2015.pdf)

17. Raport roczny z działalności CERT Polska 2016. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2016.pdf](https://cert.pl/uploads/docs/Raport_CP_2016.pdf);
18. Raport roczny z działalności CERT Polska 2017. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2017.pdf](https://cert.pl/uploads/docs/Raport_CP_2017.pdf)
19. Raport roczny z działalności CERT Polska 2018. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2018.pdf](https://cert.pl/uploads/docs/Raport_CP_2018.pdf);
20. Raport roczny z działalności CERT Polska 2019. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2019.pdf](https://cert.pl/uploads/docs/Raport_CP_2019.pdf)
21. Raport roczny z działalności CERT Polska 2020. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2020.pdf](https://cert.pl/uploads/docs/Raport_CP_2020.pdf)
22. Raport roczny z działalności CERT Polska 2021. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2021.pdf](https://cert.pl/uploads/docs/Raport_CP_2021.pdf)
23. Raport roczny z działalności CERT Polska 2022. Krajobraz Bezpieczeństwa polskiego internetu [https://cert.pl/uploads/docs/Raport\\_CP\\_2022.pdf](https://cert.pl/uploads/docs/Raport_CP_2022.pdf)
24. Raport roczny z działalności CERT Polska 2023, [https://cert.pl/uploads/docs/Raport\\_CP\\_2023.pdf](https://cert.pl/uploads/docs/Raport_CP_2023.pdf)
25. Sewastianowicz M.: Grzywną w nieproszonego gościa na Zoom party, Prawo.pl 30.05.2020, <https://www.prawo.pl/oswiata/grzywna-za-przerywanie-zdalnych-lekcji-wykroczenie,500657.html>
26. Statystyki Policji [statystyka.policja.pl](http://statystyka.policja.pl)
27. Szmit M.: O pewnym nowym przepisie i jednym precedensowym wyroku, „Rocznik Bezpieczeństwa Morskiego”, 2021, nr 2020, s. 195-208
28. Ustawa z dnia 19 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19, Dz.U. z 2020 r. poz. 1086
29. Ustawa z dnia 5 lipca 2018 r. O krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077)
30. Wala K.: Ratio legis oraz analiza ustawowych znamion wykroczenia z art. 107a k.w., „Prokuratura i prawo” 3/2021 s 68-90

# OCHRONA INTERNETU PRZED NIELEGALNYMI TREŚCIAMI - PIRACTWO TREŚCI AUDIOWIZUALNYCH ONLINE

## PROTECTING THE INTERNET FROM ILLEGAL CONTENT - PIRACY OF AUDIOVISUAL CONTENT ONLINE

**Luiza PISKOREK**<sup>1</sup>

**Streszczenie:** W niniejszym rozdziale przedstawione zostały zagadnienie tzw. blokowania nielegalnych treści w internecie jako narzędzia do walki z naruszeniami online, ze szczególnym uwzględnieniem blokowania nielegalnego rozpowszechniania treści audiowizualnych. Przedstawiono obowiązujące w Europie i Polsce przepisy i mechanizmy prawne blokowania nielegalnych treści. Zwrócono uwagę na ich nie wystarczającą skuteczność.

**Słowa kluczowe:** piractwo audiowizualne, nielegalne treści, blokowanie.

**Summary:** This chapter presents the issue of the so-called blocking of illegal content on the Internet as a tool to combat online violations, with a particular focus on blocking illegal distribution of audiovisual content. The regulations and legal mechanisms in force in Europe and Poland for blocking illegal content are presented. Attention was drawn to their insufficient effectiveness.

**Keywords:** illegal content, audiovisual piracy, blocking.

### WSTĘP

Internet od wielu lat jest nieodłącznym elementem rzeczywistości. Dawno już przestał to być świat tylko wirtualny, a stał się realną częścią czynności w każdym niemal wymiarze, w tym społecznym, informacyjnym, rozrywkowym, ekonomicznym, czy politycznym. Także Polska w ostatnich latach doświadcza znacznego wzrostu transformacji cyfrowej. Wzrost poziomu cyfryzacji w różnych aspektach życia codziennego podnosi jego jakość, ale także sprawia, że użytkownicy internetu są bardziej zależni od usług cyfrowych. W ślad za rozwojem aktywności w internecie idzie rozwój cyberprzestępczości i innych naruszeń prawa w internecie. W związku z powyższym, tak jak w rzeczywistości offline, tak samo w rzeczywistości online, konieczne są narzędzia do walki z naruszeniami i możliwość szybkiego zatrzymania ich szybkiego rozprzestrzeniania się w internecie.

---

<sup>1</sup> Radca prawny, Kancelaria Prawna Media, Stowarzyszenie Sygnał.

W niniejszym opracowaniu przedstawione zostanie zagadnienie tzw. blokowania nielegalnych treści w internecie jako narzędzia do walki z naruszeniami online, ze szczególnym uwzględnieniem blokowania nielegalnego rozpowszechniania treści audiowizualnych. Wspomniane wyżej blokownie to termin użyty dla różnych form uniemożliwiania dostępu do nielegalnych treści. Może tu chodzi zarówno o takie formy blokowania jak zablokowanie przez dostawcę usług dostępu internetu możliwości dostępu do tych treści przez użytkowników internetu, ale też usuwanie nielegalnych treści przez platformy udostępniania online treści zamieszczanych w nich przez użytkowników platform lub inne formy ograniczania dostępności treści, w zależności od technologii, której to dotyczy. Wszelkie te formy ograniczania dostępności nielegalnych treści będą na potrzeby niniejszego opracowania zwane blokowaniem. Natomiast nielegalne treści, to wszelkie treści (informacje) rozpowszechniane z naruszeniem prawa, które same w sobie (w sensie zawartości przekazu) stanowią treść naruszającą prawo (np. treść o charakterze terrorystycznym) lub naruszają prawo przez odniesienie do działania, w tym sprzedaży produktów lub świadczenia usług (np. sama treść jest zgodna z prawem, jak np. utwór audiowizualny jak film, ale jego rozpowszechnianie w internecie następuje bez zgody podmiotu mającego prawa do tego filmu).

W opracowaniu pokazane zostaną podstawowe dostępne w Polsce systemy blokowania nielegalnych treści rozpowszechnianych w internecie, wraz z odpowiedzią na pytania, jakie nielegalne treści mogą być blokowane w poszczególnych systemach, kto decyduje o takim blokowaniu, jak też kto realizuje decyzje o blokowaniu. Na tym tle dokładniej zostanie przedstawione blokowanie nielegalnego rozpowszechniania treści audiowizualnych chronionych prawem. Jak zostanie to wskazane w dalszej części niniejszego opracowania, aktualnie dostępne w Polsce mechanizmy prawne do walki z piractwem online treści audiowizualnych nie są skuteczne do walki z rozwiniętymi technologicznie pirackimi usługami, pomimo istotnych zmian w polskim prawie w tym zakresie w ostatnim czasie. Chociaż nielegalne rozpowszechnianie treści audiowizualnych jest tylko wycinkiem zagadnienia rozpowszechniania nielegalnych treści w internecie, ma ono wiele negatywnych aspektów zarówno na poziomie ekonomicznym, jak też na poziomie społecznym, a także niesie za sobą wiele istotnych zagrożeń, jak cyberprzestępczość.

## **SYSTEMY BLOKOWANIA NIELEGALNYCH TREŚCI W POLSKIM PRAWIE**

Przepisy prawa polskiego nie przewidują jednego spójnego systemu blokowania nielegalnych treści w internecie. Nie dotyczą też one wszelkich nielegalnych treści w internecie, ale każdy z tych systemów dotyczy blokowania określonego rodzaju naruszeń w internecie. W zw. z ostatnimi zmianami w prawie, jak też zmianami planowanymi, o czym niżej w opracowaniu, katalog tych treści ulega poszerzaniu. Dla różnych systemów różne są organy wydające decyzje o blokowaniu treści w internecie, różne są też kategorie podmiotów będące wykonawcami tych decyzji.

Opisane niżej podstawowe systemy blokowania zostały sklasyfikowane ze względu na tryb blokowania przewidziany w przepisach. Są to przede wszystkim rejestry domen podlegających blokowaniu, decyzje administracyjne, decyzje sądu lub prokuratora.

## **1. Rejestry domen podlegających blokowaniu**

### **• Rejestr domen oferujących gry hazardowe niezgodnie z ustawą o grach hazardowych - Ministerstwo Finansów**

Przykładem systemu blokowania opartego na rejestrze jest publiczny rejestr domen oferujących gry hazardowe niezgodnie z ustawą o grach hazardowych<sup>2</sup>. Za prowadzenie rejestru odpowiada Minister Finansów. Wpis do rejestru dokonywany jest z urzędu po jego zatwierdzeniu przez Ministra Finansów albo wyznaczony przez niego organ Krajowej Administracji Sądowej. Wpisowi podlega nazwa domeny internetowej dostępnej dla użytkowników Internetu znajdujących się na terytorium Polski, wykorzystywanej do urządzania gier hazardowych lub do ich promowania lub reklamowania.

Rejestr działa w sposób zautomatyzowany. Prowadzony jest w systemie teleinformatycznym, który umożliwia automatyczne przekazywanie informacji do systemów teleinformatycznych przedsiębiorców telekomunikacyjnych świadczących usługi dostępu do sieci Internet. Komunikacja pomiędzy rejestrem a systemem blokującym przedsiębiorcy odbywa się za pośrednictwem interfejsu. Wpis do rejestru automatycznie powoduje powstanie po stronie przedsiębiorcy telekomunikacyjnego obowiązku zablokowania dostępu do konkretnej domeny wpisanej do rejestru, które musi nastąpić w ciągu 48 godzin od dokonania wpisu<sup>3</sup>. Ponadto, przedsiębiorca telekomunikacyjny ma obowiązek przekierowania połączenia odwołującego się do nazwy domeny wpisanej do rejestru do innej strony internetowej zawierającej komunikat dla użytkownika Internetu o nielegalnym charakterze danej gry hazardowej, jak też powiadomienie o grożącej odpowiedzialności karno-skarbowej uczestnika gier urządzanych wbrew przepisom ustawy.

Przedsiębiorca telekomunikacyjny nie ma obowiązku ani oceny legalności urządzania gry hazardowej pod nazwą domeny, ani tym bardziej wyszukiwania w Internecie domen z nielegalnymi grami hazardowymi. Jego obowiązkiem jest zablokowanie dostępu do konkretnych domen pobranych automatycznie z rejestru.

### **• Lista ostrzeżeń stron wyludzających dane użytkowników Internetu - SCRI T NASK**

Kolejnym przykładem blokowania opartego na rejestrze działającego podobnie do rejestru domen oferujących gry hazardowe niezgodnie z ustawą o grach hazardowych,

---

<sup>2</sup> Art. 15f ustawy z dnia 19 listopada 2009 r. o grach hazardowych (Dz.U.2023.227 t.j. z dnia 2023.02.02)

<sup>3</sup> Zgodnie z treścią art. 15f ust 5 pkt 1) ustawy o grach hazardowych, jest to obowiązek „nieodpłatnego uniemożliwienia dostępu do stron internetowych wykorzystujących nazwy domen internetowych wpisanych do Rejestru poprzez ich usunięcie z systemów teleinformatycznych przedsiębiorców telekomunikacyjnych, służących do zamiany nazw domen internetowych na adresy IP”.

jest tzw. rejestr stron wyłudzających dane użytkowników Internetu. Jest to lista ostrzeżeń zawierająca domeny internetowe służące do wyłudzeń danych lub niekorzystnego rozporządzenia mieniem użytkowników Internetu. Lista ta prowadzona jest przez CSIRT NASK<sup>4</sup>, na podstawie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej<sup>5</sup> oraz porozumienia pomiędzy Prezesem Urzędu Komunikacji Elektronicznej, ministrem właściwym do spraw informatyzacji, NASK oraz przedsiębiorcami telekomunikacyjnymi dotyczącego prowadzenia listy ostrzeżeń oraz uniemożliwienia dostępu do tych stron. Jest to rejestr działający na zasadzie dobrowolności, a nie na podstawie wynikającego z ustawy obowiązku blokowania, jak ma to miejsce w przypadku rejestru domen nielegalnie oferujących gry hazardowe. Przepisy ustawy dają podstawę prawną do tego, aby przedsiębiorcy telekomunikacyjni przystępujący do porozumienia mieli prawną możliwość blokowania domen wpisanych na listę ostrzeżeń SCIRT NASK, tj. uniemożliwienia użytkownikom internetu dostępu do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę ostrzeżeń, przez ich usunięcie z systemów teleinformatycznych przedsiębiorców telekomunikacyjnych służących do zamiany nazw domen internetowych na adresy IP. W takim przypadku przedsiębiorca telekomunikacyjny przekierowuje połączenia odwołujące się do nazw domen internetowych wpisanych na listę ostrzeżeń do strony internetowej prowadzonej przez CSIRT NASK zawierającej informację skierowaną do użytkowników internetu zawierającą w szczególności informacje o lokalizacji listy ostrzeżeń, wpisaniu szukanej nazwy domeny internetowej na listę ostrzeżeń oraz o możliwej próbie wyłudzenia danych lub niekorzystnego rozporządzenia mieniem. Domenę internetową do SCIRT NASK w celu wpisania jej na listę ostrzeżeń może zgłosić każdy. Zgłoszenie weryfikowane jest przez do SCIRT NASK.

- **Rejestr domen wykorzystywanych do prowadzenia nielegalnej działalności z zakresie kryptoaktywów**

Według projektowanej ustawy o rynku kryptoaktywów (projekt z dnia 9 sierpnia 2024 r.)<sup>6</sup> Komisja Nadzoru Finansowego (KNF) ma zyskać uprawnienie do prowadzenia rejestru domen internetowych wykorzystywanych do prowadzenia działalności w zakresie kryptoaktywów bez wymaganego prawem zezwolenia albo posiadania innego uprawnienia lub działalności w inny sposób sprzecznej z przepisami prawa. Rejestr ten ma działać na zasadach podobnych do dwóch opisanych wyżej rejestrów. Podobnie jak powyższe rejestry, jest on prowadzony w systemie teleinformatycznym umożliwiającym automatyczne przekazywanie informacji do systemów teleinformatycznych przedsiębiorców telekomunikacyjnych i dostawców usług hostingowych oraz jest jawny.

---

<sup>4</sup> NASK - Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy. Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, NASK został wskazany jako jeden z tzw. CSIRT - Zespołów Reagowania na Incydenty Komputerowe, który koordynuje obsługę incydentów zgłaszanych przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny.

<sup>5</sup> Art. 20 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz.U.2023.1703 z dnia 2023.08.25 z późn zmn).

<sup>6</sup> <https://legislacja.rcl.gov.pl/projekt/12382311/katalog/13040399#13040399>

Podobnie jak w przypadku dwóch powyższych rejestrów, przedsiębiorca telekomunikacyjny świadczący usługi dostępu do sieci Internet jest obowiązany do zablokowania dostępu do stron internetowych wykorzystujących nazwę domeny internetowej wpisanej do rejestru. Według projektu ustawy, taka blokada musi nastąpić nie później niż w ciągu 48 godzin od dokonania wpisu do rejestru. Również w przypadku tego rejestru, przedsiębiorca byłby zobowiązany do przekierowania połączeń odwołujących się do nazwy domeny internetowej wpisanej do rejestru do strony internetowej prowadzonej przez KNF z komunikatem o wpisaniu szukanej nazwy domeny internetowej do rejestru oraz ostrzeżeniem o ryzyku wyrządzenia poważnych szkód interesom klientów lub posiadaczom kryptoaktywów. W przypadku wpisu domeny do rejestru, KNF może także zażądać od dostawcy usług hostingowych usunięcia albo wyłączenia interfejsu internetowego lub ograniczenia dostępu do interfejsu internetowego lub usunięcia wskazanej przez KNF treści. Komisja może także skierować żądanie do rejestru domen lub rejestratorów domen usuwają nazwę domeny internetowej oraz bezterminowo lub na czas wskazany w żądaniu zarejestrowania tej nazwy na rzecz KNF.

## 2. Decyzje administracyjne

### • **Blokowanie nadużyć w komunikacji elektronicznej – Prezes UKE**

Ta sama ustawa, która wprowadziła listę ostrzeżeń CSIRT NASK<sup>7</sup>, daje też podstawę do wydawania przez Prezesa UKE nakazów zablokowania przez przedsiębiorcę telekomunikacyjnego dostępu do numeru lub usługi, jeśli jest to uzasadnione ochroną użytkowników końcowych przed nadużyciami w komunikacji elektronicznej. Czym jest zatem „nadużycie w komunikacji elektronicznej”, przed którym chronić mają użytkowników internetu nakazy Prezesa UKE zablokowania dostępu do numeru lub usługi? Jest to świadczenie lub korzystanie z usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, jeśli celem lub skutkiem takiego korzystania jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu lub użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści dla podmiotu dopuszczającego się nadużycia w komunikacji elektronicznej, innej osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej. Prezes UKE może określić termin nawet 6 godzin (nie krótszy niż 6 godzin) do wykonania jego nakazu zablokowania dostępu do numeru lub usługi.

### • **Blokowanie zagrożeń bezpieczeństwu państwa lub porządkowi publicznemu – Prezes UKE**

Prezes UKE ma także prawo nakładania na przedsiębiorców telekomunikacyjnych, w drodze decyzji, obowiązku blokowania połączeń lub komunikatów elektronicznych (albo obowiązek umożliwienia dokonania takiej blokady przez uprawnione podmioty), jeżeli mogą one zagrażać obronności, bezpieczeństwu państwa oraz bezpieczeństwu i

---

<sup>7</sup> Art. 23 ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej.

porządkowi publicznemu, albo obowiązek umożliwienia dokonania takiej blokady przez uprawnione podmioty<sup>8</sup>. Blokowanie musi zostać zrealizowane nie później niż w terminie 6 godzin liczonych od otrzymania decyzji. Decyzja może być przekazana przedsiębiorcy także ustnie, a następnie doręczona na piśmie w terminie 14 dni od dnia ustnego przekazania.

- **Treści o charakterze terrorystycznym – Szef ABW**

Szef Agencji Bezpieczeństwa Wewnętrznego został wyposażony w prawo wydawania nakazów usunięcia zobowiązujących dostawców usług hostingowych do usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści o charakterze terrorystycznym<sup>9</sup>. Nakazy usunięcia wydawane są w trybie decyzji administracyjnej i podlegają natychmiastowemu wykonaniu.

- **Projektowane blokowanie nielegalnych treści w internecie na podstawie tzw. nakazów blokujących UKE**

W przeciwieństwie do dotychczasowego podejścia ustawodawcy do blokowania wybiórczo określonych treści stanowiących naruszenie prawa, jak też wybiórczo określonych adresatów takiego nakazu, projekt zmian do ustawy o świadczeniu usług drogą elektroniczną<sup>10</sup> szeroko określa zakres treści podlegających blokowaniu ze względu na ich nielegalny charakter. Projekt ten wdraża do polskiego porządku prawnego Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych (DSA). Jednocześnie wprowadza on postawę prawną do ochrony użytkowników Internetu przed nielegalnymi treściami w Internecie. Nielegalne treści, które będą podlegały blokowaniu to wszelkie informacje, które same w sobie lub przez odniesienie do działania, w tym sprzedaży produktów lub świadczenia usług, nie są zgodne z prawem. W celu umożliwienia blokowania takich nielegalnych treści, projekt wyposaża Prezesa Urzędu Komunikacji Elektronicznej (UKE) w uprawnienie do wydawania tzw. nakazów blokujących, czyli nakazów podjęcia działań przeciwko nielegalnym treściom, w formie decyzji administracyjnej. Prezes UKE będzie odpowiedzialny za nakazywanie blokowania treści naruszających dobra osobiste, wyczerpujących znamiona czynu zabronionego lub pochwalających lub nawołujących do popełnienia czynu zabronionego, a także naruszających prawa własności intelektualnej. Nakazy blokujące będą wydawane w ciągu 7 dni od złożenia wniosku przez uprawnione podmioty (21 dni w sprawach szczególnie skomplikowanych). Decyzje w sprawach nakazów blokujących będą podlegały natychmiastowemu wykonaniu. Projekt ustawy szeroko określa nie tylko zakres nielegalnych treści podlegających blokowaniu, ale też zakres podmiotów będących

---

<sup>8</sup> Art. 53 ustawy z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz.U.2024.1221 z dnia 2024.08.09 z późn zm)

<sup>9</sup> Rozdział 5a ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (w wersji obowiązującej od 3.12.2024 r.)

<sup>10</sup> Projekt z dnia 27.11.2024 r. ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną (ustawy z dnia 18 lipca 2002 r.): <https://legislacja.rcl.gov.pl/docs//2/12383101/13045617/13045618/dokument694959.pdf>

wykonawcami nakazów blokujących i podmiotów, które mogą wnioskować o wydanie nakazu w celu ochrony praw w internecie. Wykonawcami nakazów blokujących będą dostawcy usług pośrednich, czyli dostawcy usług „zwykłego przekazu” polegających na transmisji w sieci telekomunikacyjnej informacji przekazanych przez odbiorcę usługi lub na zapewnianiu dostępu do sieci telekomunikacyjnej, „cachingu” polegających na transmisji w sieci telekomunikacyjnej informacji przekazanych przez odbiorcę usługi, obejmującą automatyczne, pośrednie i krótkotrwałe przechowywanie tej informacji, dokonywane wyłącznie w celu usprawnienia późniejszej transmisji informacji na żądanie innych odbiorców, jak też „hostingu” polegających na przechowywaniu informacji przekazanych przez odbiorcę usługi oraz na jego żądanie. O wydanie nakazu blokującego mogą wnioskować różne podmioty w zależności od rodzaju nielegalnych treści, czyli w zależności czyje prawa lub dobra zostają naruszone i w jaki sposób. W przypadku nielegalnych treści naruszających prawa ochrony konsumentów, wniosek o blokowanie do Prezesa UOKiK może złożyć usługobiorca, czyli użytkownik usługi internetowej lub zaufany podmiot sygnalizujący, o którym mowa w DSA. W przypadku nielegalnych treści naruszających dobra osobiste, wniosek może złożyć każdy, czyje dobro osobiste zostało naruszone. Jeśli chodzi o nielegalne treści, których rozpowszechnianie stanowi czyn zabroniony lub pochwalających lub nawołujących do popełnienia czynu zabronionego, wnioskodawcą może być Prokurator, Policja, usługobiorca lub zaufany podmiot sygnalizujący. Jeśli chodzi natomiast o nielegalne treści, które naruszają prawa własności intelektualne, wniosek o blokowanie ich rozpowszechniania w internecie może złożyć każdy, czyje prawo własności intelektualnej zostaje naruszone, Policja lub zaufany podmiot sygnalizujący. W każdym przypadku, w którym uprawnienie do złożenia wniosku o blokowanie przysługuje Policji, uprawnienie to przysługuje też organom Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Krajowej Administracji Skarbowej, Centralnego Biura Antykorupcyjnego, Żandarmerii Wojskowej, Państwowej Inspekcji Sanitarnej oraz Inspekcji Handlowej, w zakresie ich właściwości.

### **3. Postanowienia sądu lub prokuratora**

W przypadku treści zamieszczanych w internecie, które stanowią określone przestępstwa, sąd lub prokurator mogą nałożyć obowiązek uniemożliwienia dostępu do danych informatycznych przechowywanych systemie informatycznym (lub w urządzeniach zawierających te dane na nośniku)<sup>11</sup>. Dotyczy to takich treści jak propagowanie pedofilii, rozpowszechnianie, utrwalanie, posiadanie określonego rodzaju treści pornograficznych, w tym z udziałem małoletniego, treści mogących ułatwić popełnienie przestępstwa o charakterze terrorystycznym, treści dotyczących nielegalnych środków określonych w przepisach dotyczących przeciwdziałania narkomanii<sup>12</sup>. Katalog podmiotów, na który może zostać nałożony taki obowiązek jest szeroki i obejmuje także

---

<sup>11</sup> Art. 218a ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz.U.2024.37 t.j. z dnia 2024.01.11 z późn zmn)

<sup>12</sup> [https://sip.lex.pl/Rozdział\\_7\\_ustawy\\_z\\_dnia\\_29\\_lipca\\_2005\\_r.\\_o\\_przeciwdziałaniu\\_narkomanii](https://sip.lex.pl/Rozdział_7_ustawy_z_dnia_29_lipca_2005_r._o_przeciwdziałaniu_narkomanii) (Dz. U. z 2023 r. poz. 1939 z późn zmn)

przedsiębiorców prowadzących działalność telekomunikacyjną lub świadczących usługi drogą elektroniczną oraz dostawców usług cyfrowych.

Sąd może także postanowić o usunięciu lub blokadzie dostępności danych informatycznych, które mają związek ze zdarzeniem o charakterze terrorystycznym lub uprawdopodobniającym popełnienie przestępstwa szpiegostwa lub określonych usług teleinformatycznych służących lub wykorzystywanych do spowodowania zdarzenia o charakterze terrorystycznym lub uprawdopodobniającego popełnienie przestępstwa szpiegostwa.<sup>13</sup> Usługodawca świadczący usługi drogą elektroniczną może być adresatem żądania zarówno usunięcia, jak też zablokowania dostępności danych, natomiast przedsiębiorca telekomunikacyjny może być adresatem żądania zablokowania dostępności danych. Sąd wydaje takie postanowienie na pisemny wniosek Szefa ABW złożony po uzyskaniu pisemnej zgody Pierwszego Zastępcy Prokuratora Generalnego Prokuratora Krajowego.

#### **4. Kto blokuje, czyli jakie podmioty są wykonawcami obowiązku blokowania?**

Przepisy prawa określają nie tylko różne systemy blokowania, ale też różnie określają podmioty, do których kierowany jest obowiązek wykonania blokowania danej nielegalnej treści. Jednakże podkreślenia wymaga, że niezależnie od systemu blokowania, podmioty, do których kierowany jest obowiązek wykonania blokowania danej nielegalnej treści, czy to w formie wpisu do rejestru, czy postanowienia, czy też decyzji administracyjnej, jest jedynie wykonawcą tej decyzji. Oznacza to, że podmioty te nie mogą decydować ani o tym, czy dane treści są nielegalne, ani czy mają ona podlegać blokowaniu. Podmioty te nie ponoszą także odpowiedzialności wobec tych, których treści zostaną zablokowane, jeśli realizują blokowanie zgodnie z wpisem do rejestru, postanowieniem albo decyzją. Rozwiązanie takie wynika także z założenia, że są to tzw. nakazy blokujące wydawane wobec podmiotu niewinnego, nieuczestniczącego aktywnie w przekazywaniu nielegalnych treści, które zamieszcza w jego usługach osoba trzecia, a będących wykonawcami nakazów blokujących z tego powodu, że ich usługi są wykorzystywane do przekazywania nielegalnych treści, a jako dostawcy tych usług mają techniczną możliwość zablokowania przekazywania tych treści. Podmioty te mogą wprawdzie ponosić własną odpowiedzialność za przekazywanie lub utrzymywanie nielegalnych treści w swoich usługach, jednak na podstawie innego reżimu prawnego niż wykonywanie tzw. nakazów blokujących. Koncepcja nakazów blokujących wydawane wobec podmiotu niewinnego została przedstawiona szerzej w pkt III niniejszego opracowania.

Jako wykonawców blokowania nielegalnych treści przepisy prawa wskazują przede wszystkim przedsiębiorców telekomunikacyjnych, jak np. w przypadku listy ostrzeżeń CSIRT NASK oraz niektórych decyzji. Na pytanie, co to jest za rodzaj przedsiębiorcy,

---

<sup>13</sup> Art. 32c ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (w brzmieniu obowiązującym od 3 grudnia 2024 r.)

odpowiada Prawo komunikacji elektronicznej<sup>14</sup>. Zgodnie z art. pkt 40 ww. ustawy, przedsiębiorca telekomunikacyjny to przedsiębiorcę (lub inny podmiot uprawniony do wykonywania działalności gospodarczej na podstawie odrębnych przepisów), który wykonuje działalność gospodarczą polegającą na dostarczaniu publicznej sieci telekomunikacyjnej, świadczeniu powiązanych usług lub świadczeniu publicznie dostępnych usług telekomunikacyjnych, przy czym przedsiębiorca telekomunikacyjny, uprawniony do: a) świadczenia publicznie dostępnych usług telekomunikacyjnych (dostawca usług telekomunikacyjnych), b) dostarczania publicznej sieci telekomunikacyjnej lub świadczenia powiązanych usług (operator).

Niektóre z przepisów dotyczących blokowania treści zawężają krąg wykonawców nakazów blokujących wskazując, że podmiotami zobowiązanymi do blokowania są tylko tacy przedsiębiorcy telekomunikacyjni, którzy świadczą usługi dostępu do sieci Internet, jak ma to miejsce w przypadku rejestru domen oferujących gry hazardowe niezgodnie z ustawą o grach hazardowych, jak też rejestru domen internetowych wykorzystywanych do prowadzenia działalności w zakresie kryptoaktywów sprzecznie z projektowaną ustawą o rynku kryptoaktywów. W przypadku nakazów Szefa ABW usunięcia treści o charakterze terrorystycznym lub uniemożliwienia dostępu do treści o charakterze terrorystycznym, adresatami tych nakazów są dostawcy usług hostingowych.

Z kolei przepisy przyznające prawo do blokowania treści sądowi lub prokuratorowi w przypadku określonych przestępstw, szeroko zakreślają krąg podmiotów, które mogą zostać zobowiązane do blokowania. Wśród nich są zarówno przedsiębiorcy prowadzący działalność telekomunikacyjną, ale też świadczący usługi drogą elektroniczną oraz dostawcy usług cyfrowych.

Podobnie, projekt ustawy zmieniający ustawę o świadczeniu usług drogą elektroniczną jako adresatów nakazów blokujących wskazuje dostawców usług pośrednich, czyli podmioty świadczące usługi zwykłego przekazu, cachingu lub hostingu. Usługa zwykłego przekazu polega na transmisji w sieci telekomunikacyjnej informacji przekazanych przez odbiorcę usługi lub na zapewnianiu dostępu do sieci telekomunikacyjnej. Usługa cachinu polega na transmisji w sieci telekomunikacyjnej informacji przekazanych przez odbiorcę usługi, obejmującą automatyczne, pośrednie i krótkotrwałe przechowywanie tej informacji, dokonywane wyłącznie w celu usprawnienia późniejszej transmisji informacji na żądanie innych odbiorców. Z kolei usługa hostingu, polega na przechowywaniu informacji przekazanych przez odbiorcę usługi oraz na jego żądanie.<sup>15</sup>

---

<sup>14</sup> Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz.U.2024.1221 z dnia 09.08.2024)

<sup>15</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)

## **I. BLOKOWANIE NIELEGALNEGO ROZPOWSZECHNIANIE TREŚCI AUDIOWIZUALNYCH W INTERNECIE**

Jak wśród tych systemów blokowania wygląda ochrona treści audiowizualnych przez ich nielegalnym rozpowszechnianiem w Internecie i dlaczego jest to ważne? Jak wygląda ochrona treści audiowizualnych przez ich nielegalnym rozpowszechnianiem w formie blokowania w prawie UE? Czy obowiązujące w Polsce przepisy prawa są zgodne z prawiem UE i zapewniają wystarczające mechanizmy prawne do walki z piractwem online treści w internecie?

Przed podjęciem próby odpowiedzi na te pytania, warto na wstępie wyjaśnić pewne pojęcia używane w dalszej części opracowania.

Na wstępie podkreślić należy, że mówiąc o blokowaniu nielegalnych treści w odniesieniu do treści audiowizualnych podlegających ochronie jako przedmioty prawa autorskiego lub praw pokrewnych lub takich jak transmisje wydarzeń sportowych lub innych wydarzeń na żywo (łącznie zwanych dalej „treściami audiowizualnymi”), chodzi o zatrzymanie ich nielegalnej dystrybucji, tj. rozpowszechniania w internecie bez zgody uprawnionych do tych treści. W analizie tego zagadnienia nie chodzi o ocenę legalności przekazu zawartego w tych treściach. W przypadku, gdy dana treść jest treścią nielegalną, gdyż z uwagi na zawarty w niej przekaz przykładowo wypełnia znamiona czynu zabronionego (jak np. nawoływanie do popełnienia przestępstwa), podlegać ona może blokowaniu także z innego tytułu. Zasadniczym problemem dla uprawnionych do treści audiowizualnych jest działalność audiowizualnych usług pirackich. Piractwo treści audiowizualnych przybiera różne formy, takie jak nielegalny streaming wideo na żądanie (VOD), transmisji programów (kanałów) telewizyjnych, treści na żywo takich jak wydarzenia sportowe, obok innych form nielegalnego korzystania z treści audiowizualnych, jak np. z wykorzystaniem IPTV, cardsharing’u współdzielenia kont. W Polsce największym problemem jest nielegalny streaming treści audiowizualnych udostępnianych przez pirackie usługi w formie serwisów na żądanie (VOD) oraz platform udostępniania wideo, które są strukturalnie przeznaczone do korzystania z cudzych treści audiowizualnych bez zezwolenia w formie zarobkowej w sposób zorganizowany i zazwyczaj na dużą skalę (dalej będą zwane łącznie „serwisami prackimi”).

### **1. Dlaczego blokowanie nielegalnego rozpowszechniania treści audiowizualnych jest ważne?**

Działalność serwisów pirackich niesie za sobą znaczne straty finansowe, przy czym nie tylko dla samej branży audiowizualnej. Z raportu Deloitte sporządzonego w lipcu 2023 r.<sup>16</sup> dla Stowarzyszenia Sygnał, wartość konsumpcji treści wideo w nielegalnych źródłach w Internecie wynosiła 7,36 mld zł. Straty branży z tytułu piractwa treści audiowizualnej według raportu mogły sięgać prawie 3 mld złotych rocznie, a z

---

<sup>16</sup> Raport Deloitte "Kradzież treści wideo w Internecie. Analiza wpływu zjawiska piractwa internetowego treści audiowizualnych, w tym telewizyjnych, na gospodarkę Polski". Warszawa, lipiec 2023 r., [https://sygnał.org.pl/wp-content/uploads/2023/07/2023\\_raport\\_kradziezinternetwideo\\_deloitte.pdfz](https://sygnał.org.pl/wp-content/uploads/2023/07/2023_raport_kradziezinternetwideo_deloitte.pdfz)

nielegalnych serwisów dystrybuujących treści telewizyjne korzystało w Polsce 7,3 mln użytkowników (w roku 2023 r.), co wynosi nawet trzykrotnie więcej niż oglądalność legalnych serwisów VOD powiązanych ze stacjami TV. Straty Skarbu Państwa sięgały nawet 1,86 mld zł, straty Państwowego Instytutu Sztuki Filmowej przekraczały 100 mln zł rocznie. Starty dla branży audiowizualnej oznaczają straty nie tylko dla firm zajmujących się produkcją i dystrybucją treści wideo (jak producenci, nadawcy, serwisy streamingowe). Pociąga to za sobą mniejsze możliwości inwestycyjne w nowe treści, a zatem w konsekwencji odbija się to na współtwórcach takich treści i artystach wykonawcach (np. aktorach) biorących udział w ich tworzeniu, jak też może prowadzić do zmniejszenia się różnorodności, a także jakości tych treści, a wobec tego ostatecznie niesie negatywne konsekwencje także dla widzów.

Oprócz aspektów finansowych, ważne podkreślenia jest ryzyko konsumenckie związane z działalnością serwisów pirackich związane z cyberbezpieczeństwem. Korzystanie z serwisów pirackich niesie za sobą takie zagrożenia jak złośliwe oprogramowanie i wirusy, kradzież tożsamości, naruszenia danych, straty finansowe i potencjalne konsekwencje prawne. Pirackie serwisy często zawierają ukryte złośliwe oprogramowanie lub wirusy, stanowiąc zagrożenie dla użytkowników, którzy mogą nieświadomie zainfekować swoje urządzenia. To z kolei niejednokrotnie prowadzi do takich ryzyk jak: kradzież danych osobowych i kradzież tożsamości, kradzież danych dostępowych do rachunków bankowych, wyłudzenia finansowe, uszkodzenie oprogramowania, utrata danych użytkownika lub przejęcie zarządzania systemem informatycznym użytkownika. Według badania „Consumer Risk from Piracy in Poland” autorstwa Paul A. Watters PhD, ryzyko napotkania cyberzagrożeń podczas korzystania z pirackich serwisów w Polsce jest bardzo wysokie. Polscy konsumenci odwiedzając serwisy pirackie są niemal 40-krotnie bardziej narażeni na cyber zagrożenia niż podczas korzystania z legalnych źródeł. Jest to pierwsze badanie, które z taką szczegółowością opisuje skalę cyber zagrożeń, które są ściśle związane z korzystaniem przez konsumentów w Polsce z serwisów pirackich, w tym nielegalnych serwisów streamingowych. Również według Wojsk Obrony Cyberprzestrzeni<sup>17</sup>, Polska jest krajem, w którym odbywa się najwięcej cyberataków na świecie.

Dostępne w Polsce mechanizmy zwalczania piractwa online treści audiowizualnych nie są wystraszająco skutecznie. W październiku 2023 roku Stowarzyszenie Sygnał przeprowadziło badanie wśród największych dostawców treści audiowizualnych w Polsce, którego celem było między innymi zrozumienie wybranych skali nielegalnej dystrybucji treści audiowizualnych<sup>18</sup>. Badaniem objęto pułę treści audiowizualnych na żądanie (VOD) oraz transmisji na żywo. W tej puli, od września 2022 roku do sierpnia 2023 roku zarejestrowano ponad 6,1 mln naruszeń prawa do ich dystrybucji, głównie w

---

<sup>17</sup> <https://www.trade.gov/market-intelligence/poland-ict-mostcyber-attacked-country-world>

<sup>18</sup> <https://sygnał.org.pl/wp-content/uploads/2024/02/Raport-Stowarzyszenia-Sygnał-Skuteczność-zgłoszeń-naruszeń-treści-audiowizualnych.pdf>

odniesieniu do treści VOD, które stanowiły 99,8% przypadków. Według ww. badania, oznacza to, że średnio każdy z tych materiałów był dystrybuowany w sposób nielegalny ponad 3600 razy w skali roku, co daje ponad 300 przypadków miesięcznie oraz 10 dziennie na każdy tytuł.

## **2. Jaki wygląda blokowanie nielegalnego rozpowszechniania treści audiowizualnych w prawie UE?**

Przed analizą mechanizmów prawnych służących do walki z nielegalnym rozpowszechnianiem treści audiowizualnych online dostępnych na podstawie obowiązujących w Polsce przepisów oraz oceną ich wystarczalności dla realizacji powyższego celu, niezbędne jest przedstawienie, jak kwestia ta wygląda w prawie UE.

Przed wszystkim przepisy prawa UE dotyczące praw autorskich i pokrewnych oraz praw własności intelektualnej wprowadziły tzw. nakazy blokujące wobec podmiotów, których usługi wykorzystywane w celu rozpowszechniania treści naruszających ww. prawa, niezależnie od oceny odpowiedzialności własnej dostawców takich usług, czyli tzw. nakazy wobec podmiotu niewinnego. Tzw. nakazy blokujące to postanowienia sądów cywilnych lub karnych lub decyzje organów administracji dotyczące uniemożliwienia dostępu do nielegalnych treści. Celem takich nakazów jest szybkie zatrzymanie rozpowszechniania w internecie treści bez zezwolenia osób uprawnionych w celu ograniczania szkód wywołanych ich nielegalną dystrybucją. Im dłużej dana treść dostępna jest w usługach pirackich, tym większe szkody przynosi to podmiotom uprawnionym do tych treści oraz przychody podmiotom nielegalnie je dystrybuując. Nakazy blokujące nie wyłączają i zastępują dochodzenia odpowiedzialności, w tym odszkodowawczej, przeciwko sprawcom naruszeń praw do treści audiowizualnych. Tylko sprawcy naruszeń mogą być pociągnięci do odpowiedzialności karnej lub cywilnej, w tym odszkodowawczej. Adresaci nakazów blokujących są jedynie ich faktycznymi wykonawcami na żądanie sądy lub właściwego organu.

Państwa członkowskie zostały zobowiązane do wprowadzenia wskazanych wyżej nakazów blokujących wobec podmiotów, których usługi wykorzystywane są przez osoby trzecie w celu naruszania praw autorskich lub pokrewnych już ponad dwadzieścia lat temu, na podstawie dyrektywy 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym („Dyrektywa Autorska”). Zgodnie z art. 8 ust. 3 Dyrektywy Autorskiej, *„Państwa Członkowskie zapewnią, aby podmioty praw autorskich mogły wnioskować o wydanie nakazu przeciwko pośrednikom, których usługi są wykorzystywane przez stronę trzecią w celu naruszenia praw autorskich lub pokrewnych.”* Uzasadnienie dla takiej decyzji ustawodawcy unijnego dobrze podsumowuje motyw (59) Dyrektywy Autorskiej, zgodnie z którym: *„Usługi pośredników mogą być, w szczególności w środowisku cyfrowym, coraz częściej wykorzystywane przez osoby trzecie w działalności naruszającej prawa. W wielu przypadkach pośrednicy tacy mają największą możliwość, aby zakończyć takie naruszenia. Dlatego, z zastrzeżeniem wszystkich innych*

*dostępnych sankcji lub środków naprawczych, podmioty praw autorskich powinny mieć możliwość domagania się wydania zakazu skierowanego do pośrednika, który w sieci utrzymuje naruszenia praw autorskich utworu lub innego przedmiotu objętego ochroną przez osobę trzecią. Możliwość taka powinna być dostępna, nawet jeżeli działania pośrednika stanowią przedmiot wyjątku na mocy art. 5. Warunki i metody dotyczące takich nakazów powinny być uregulowane w ramach prawa krajowego Państw Członkowskich”.*

Następnie, dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej rozszerzyła zakres praw, które mogą i powinny być chronione w formie stosowania tego rodzaju nakazów, na inne prawa własności intelektualnej. Zgodnie z art. 11 ww dyrektywy: *„Państwa Członkowskie zapewniają, że tam, gdzie podjęta została decyzja sądu stwierdzająca naruszenie prawa własności intelektualnej, organy sądowe mogą wydawać naruszającym zakaz kontynuacji naruszenia. Jeśli tak przewiduje prawo krajowe, niewypelnienie zakazu poddaje naruszającego, gdzie właściwe, powtarzalnej karze pieniężnej w celu zapewnienia zgodności z zakazem. Państwa Członkowskie zapewniają też właścicielom możliwość składania wniosku o zakaz wobec pośredników, z usług których korzysta strona trzecia do naruszania prawa własności intelektualnej, bez uszczerbku dla postanowień art. 8 ust. 3 dyrektywy 2001/29/WE.”* Motyw (23) ww dyrektywy wyjaśnia, że: *„Bez uszczerbku dla wszelkich innych dostępnych środków, procedur i środków naprawczych, podmioty uprawnione powinny mieć możliwość wystąpienia o nakaz sądowy przeciwko pośrednikowi, z którego usług korzystała strona trzecia przy naruszaniu prawa własności przemysłowej należącego do podmiotu uprawnionego. Warunki i procedury odnoszące się do takich nakazów należy pozostawić prawu wewnętrznemu Państwa Członkowskiego. W zakresie naruszeń praw autorskich i praw pokrewnych, pełny poziom harmonizacji został już przewidziany w dyrektywie 2001/29/WE. Z tego względu niniejsza dyrektywa nie może mieć wpływu na art. 8 ust. 3 dyrektywy 2001/29/WE.”*

Wskazane wyżej dyrektywy celowo nie precyzują, o jakich pośrednikach chodzi, aby nie zawęzić tego zakresu wobec technologicznego rozwoju usług pośrednich, tj. pośredniczących pomiędzy dostawcami usług lub produktów a ich odpowiadamy za pośrednictwem, w uproszczeniu, internetu, z jednej strony, ale też wobec wykorzystywania coraz nowszych technologii w celu nielegalnego rozpowszechniania treści chronionych prawem autorskim lub prawami pokrewnymi, jak też szerzej pojętym prawem własności intelektualnej.

### **3. Dlaczego adresatami nakazów blokujących są dostawcy internetu?**

Możliwych adresatów nakazów blokujących precyzuje orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (TSUE), które potwierdziło zarówno możliwość, jak i zasady stosowania nakazów blokujących. Jednym z rodzajów „pośredników”, do których mogą być kierowane nakazy blokujące, są dostawcy usług dostępu do internetu

(dostawcy internetu). Ten rodzaj usług został wskazany jako szczególny z uwagi na możliwości techniczne i technologiczne zatrzymania nielegalnego rozpowszechniania w internecie treści chronionych prawem autorskim lub prawami pokrewnymi już w orzeczeniu TSUE z dnia 27 marca 2014 r. w sprawie UPC Telekabel v Constantin Film / Wega (C-314/12). Sąd wskazał, po pierwsze, że *„Można zakazać dostawcy Internetu umożliwiania jego klientom dostępu do określonej strony internetowej udostępniającej przedmioty objęte ochroną bez zgody podmiotów praw autorskich”*. Po drugie, ww orzeczenie wskazuje, że: *„Jako że dostawca dostępu do Internetu, ze względu na to, iż udziela dostępu do sieci, w sposób nieunikniony uczestniczy każdorazowo w przekazywaniu naruszenia w Internecie pomiędzy jednym ze swoich klientów a osobą trzecią (...), należy uznać, że dostawca dostępu do Internetu, taki jak w postępowaniu głównym, który umożliwia swoim klientom dostęp do przedmiotów objętych ochroną publicznie udostępnionych w Internecie przez osoby trzecie, jest pośrednikiem, którego usługi są wykorzystywane w celu naruszenia praw autorskich lub pokrewnych w rozumieniu art. 8 ust. 3 dyrektywy 2001/29.”* Kierunek ten został wyrażony także w orzeczeniach TSUE, jak np. orzeczeniu w sprawie Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (C-70/10) z dn. 24.11.2011 r., czy też sprawie McFadden v Sony (C-484/14) z 15.09.2026 r.

W uproszczeniu, z uwagi na technologię dystrybucji treści audiowizualnych lub innych treści chronionych prawem w internecie, usługi dostawców internetu są niejako po drodze pomiędzy naruszcicielami praw do treści chronionych prawem własności intelektualnej (pirackimi serwisami VOD oraz platformami udostępniania wideo) a użytkownikami tego rodzaju pirackich usług, będącymi jednocześnie odbiorcami usług dostępu do internetu. Ponadto, co równie istotne, odbiorcy usług dostępu do internetu zlokalizowani są w tej samej jurysdykcji, co dostawcy tych usług. Tymczasem, jeśli chodzi o pirackie usługi rozpowszechniania treści audiowizualnych, często są to podmioty świadczące swoje usługi z lokalizacji poza polską, czyli w innych jurysdykcji, co utrudnia skuteczne i szybkie dochodzenie od nich zaniechania naruszeń i odszkodowania. Dodatkowo, w związku z tym, że są to usługi systemowo nakierowane na nielegalne wykorzystywanie cudzych treści audiowizualnych oraz unikanie odpowiedzialności z tego tytułu, identyfikacja podmiotów odpowiedzialnych za tę działalność jest niejednokrotnie niemożliwa lub długotrwała. Wówczas zablokowanie dostępu do tych treści na poziomie dostawcy usług dostępu do Internet jest najbardziej skuteczną, a czasem jedyną realnie możliwą formą zapobieżenia powiększaniu się szkody po stronie uprawnionych.

#### **4. Co kwestii nakazów blokujących mówi „prawo miękkie” UE**

Konieczność zapewnienia szybkiego blokowania rozpowszechniania nielegalnych treści naruszających prawa własności intelektualnej, w tym treści audiowizualnych rozpowszechnianych z naruszeniem praw uprawnionych, zaważyły też instytucje UE.

Komunikat Komisji do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego z dnia 29 listopada 2017 r. zatytułowany „Wytuczne dotyczące niektórych aspektów dyrektywy 2004/48/WE Parlamentu Europejskiego i Rady w sprawie egzekwowania praw własności intelektualnej” (COM(2017)0708) wskazuje, że:

→ usługi pośredników mogą być, w szczególności w środowisku cyfrowym, coraz częściej wykorzystywane przez osoby trzecie w działalności naruszającej prawa; w wielu sytuacjach tacy pośrednicy mają najwięcej możliwości, aby zakończyć takie naruszenia;

→ możliwość wydania nakazu przeciwko pośrednikowi na podstawie dyrektywy w sprawie egzekwowania praw własności intelektualnej nie zależy od odpowiedzialności pośrednika za (domniemane) naruszenie, którego dotyczy sprawa;

→ właściwe organy sądowe nie mogą wymagać od wnioskodawcy wykazania chociażby pośredniej odpowiedzialności pośrednika za (domniemane) naruszenie w ramach warunku wydania nakazu sądowego

→ według TSUE podmiot gospodarczy może być uznany za pośrednika, gdy świadczy usługę, która może być wykorzystana przez co najmniej jedną osobę do naruszenia co najmniej jednego prawa własności intelektualnej lub do uzyskania dostępu do treści lub towarów naruszających takie prawa<sup>19</sup> - podmiot gospodarczy, aby być uznanym za takowego pośrednika, nie musi jednak być powiązany w konkretny sposób z tymi osobami, na przykład poprzez stosunek umowny<sup>20</sup>

Zalecenie Komisji (UE) 2023/1018 z dnia 4 maja 2023 r. w sprawie zwalczania piractwa internetowego wydarzeń sportowych i innych wydarzeń na żywo wskazuje na:

→ kluczową rolę dostawców usług pośrednich w blokowaniu nielegalnego rozpowszechniania piractwa internetowego,

→ dynamiczne nakazy obejmujące nowe lokalizacje internetowe, jako skuteczny środek zapobiegający nieuprawnionej retransmisji i jej kontynuacji, zwłaszcza wobec strategii odporności opracowanych przez pirackie serwisy, na przykład zakładania lustrzanych stron pod różnymi nazwami domen lub przechodzenia na różne adresy IP w celu obejścia środków blokujących,

→ zaangażowanie państw członkowskich i organów krajowych, uprawnionych i dostawców usług pośrednich do stosowania skutecznych, odpowiednich i proporcjonalnych środków w celu zwalczania nieuprawnionych retransmisji wydarzeń sportowych i innych wydarzeń na żywo w zgodności z prawem Unii, w tym z Kartą Praw Podstawowych Unii Europejskiej i współpracy w tym zakresie.

---

<sup>19</sup> Zob. C-314/12 UPC Telekabel; wyrok Trybunału (trzecia izba) z dnia 24 listopada 2011 r.

<sup>20</sup> Wyrok TSUE (druga izba) z dnia 7 lipca 2016 r., C-494/15, Tommy Hilfiger Licensing LLC i inni przeciwko DELTA CENTER a.s., pkt 23. W odniesieniu do art. 8 ust. 3 dyrektywy o społeczeństwie informacyjnym – zobacz również C-314/12 UPC Telekabel, pkt 34–35.

Rezolucja Parlamentu Europejskiego z dnia 19 maja 2021 r. zawierająca zalecenia dla Komisji w sprawie wyzwań stojących przed organizatorami wydarzeń sportowych w środowisku cyfrowym (2020/2073(INL)) podkreśla, że:

→ zwalczanie piractwa internetowego wydarzeń sportowych transmitowanych „na żywo”, których wartość ekonomiczna wynika z transmisji „na żywo”, jest głównym wyzwaniem wymaga podjęcia działań legislacyjnych na szczeblu unijnym;

→ konieczne jest, aby pośrednicy internetowi usuwali nielegalne transmisje wydarzeń sportowych na żywo lub uniemożliwiali do nich dostęp bezzwłocznie lub jak najszybciej, a w każdym razie nie później niż w ciągu 30 minut od otrzymania powiadomienia o takiej nielegalnej transmisji, przekazanego przez podmioty praw autorskich lub certyfikowany zaufany podmiot sygnalizujący.

## **5. Blokowanie nielegalnych treści a wolność słowa w orzecznictwie TSUE**

Istotną kwestią w aspekcie blokowania rozpowszechniania nielegalnych treści w internecie jest kwestia ochrony praw podstawowych określonych w Karcie Praw Podstawowych Unii Europejskiej. Do praw podstawowych należą wolność wypowiedzi i informacji, w tym prawo dostępu do internetu. Nie można jednak zapominać, że jednym z praw podstawowych, z których wszystkie są równorzędne, jest prawo do ochrony własności intelektualnej. Wobec powyższego, mechanizmy prawne pozwalające na blokowanie nielegalnych treści naruszających prawa własności intelektualnej nie mogą z zasady być uznawane za naruszające prawo wolność wypowiedzi i informacji, jako jednego z praw podstawowych, gdyż jednocześnie służą ochronie innego prawa podstawowego – prawa do ochrony własności intelektualnej, w tym praw do treści audiowizualnych.

Orzecznictwo TSUE na przestrzeni lat wypracowało już zasady przy zachowaniu których stosowanie nakazów blokujących wobec naruszeń praw autorskich i praw pokrewnych jest zgodne z Kartą Praw Podstawowych UE i nie narusza wolności wypowiedzi i informacji<sup>21</sup>. Zgodnie z tym orzecznictwem, nakazy blokujące mogą być stosowane, jeśli zachowują one równowagę pomiędzy prawem chronionym poprzez nałożenie takiego nakazu blokującego, a ochroną praw podstawowych. Chodzi tu przede wszystkim o równowagę pomiędzy potrzebą ochrony praw własności intelektualnej a ochroną wolności wypowiedzi i informacji użytkowników internetu oraz prawem dostawcy usług, do którego kierowane są nakazy blokujące w celu ich wykonania, do swobody prowadzenia działalności gospodarczej. Wydając nakazy blokujące, sądy i organy administracji państw członkowskich muszą zapewniać, aby środki stosowane w ramach nakazów blokujących były słuszne i sprawiedliwe, nie były niepotrzebnie

---

<sup>21</sup> Zob. m.in.: GS Media (C - 160/15), Scarlet Extended (C - 70/10), Glawischnig-Piesczek v Facebook Ireland Limited (C-18/18); UPC Telekabel v Constantin Film / Wega (C-314/12), McFadden v Sony (C-484/14), SABAM v Netlog NV (C-360/10)

skomplikowane ani kosztowne, nie pociągały za sobą nieuzasadnionych okresów obowiązywania, były skuteczne (prowadziły do zamierzonego celu) i zniechęcające do naruszeń (odstrasżające), jak też zawierały odpowiednie zabezpieczenia przed ich nadużyciem. Ważną wytyczną jest też to, że środki przyjęte w ramach nakazu blokującego powinny być ściśle ukierunkowane na osiągnięcie skutku w postaci zaprzestania naruszeń praw autorskich lub pokrewnych osób trzecich oraz nie wpływają w ten sposób negatywnie na użytkowników korzystających z usług online w celu zgodnego z prawem uzyskania dostępu do informacji.

Tytułem przykładu, w sprawie *McFadden v Sony* (C-484/14) TSUE wskazał, że:

- (...) *środek użyty musi być precyzyjny w tym sensie, że musi służyć położeniu kresu naruszaniu przez osoby trzecie prawa autorskiego lub prawa pokrewnego w taki sposób, aby nie miało to wpływu na możliwość uzyskania legalnego dostępu do informacji przez użytkowników Internetu korzystających z usług tego dostawcy. W przeciwnym wypadku ingerencja tego dostawcy w wolność informacji tych użytkowników byłaby nieuzasadniona w kontekście realizowanego celu (wyrok z dnia 27 marca 2014 r., *UPC Telekabel Wien*, C-314/12, EU:C:2014:192, pkt 56).*
- (...) *środki przyjęte przez adresata nakazu takiego jak nakaz sporny w postępowaniu głównym w ramach jego wykonania muszą być dostatecznie skuteczne, by zapewnić skuteczną ochronę przedmiotowego prawa podstawowego, to znaczy muszą mieć skutek w postaci zapobiegania szukaniu dostępu do przedmiotów objętych ochroną, na który nie udzielono zgody, bądź przynajmniej uczynienia tego trudno wykonalnym i poważnie zniechęcać użytkowników Internetu korzystających z usług adresata tego nakazu do szukania dostępu do przedmiotów udostępnionych im z naruszeniem tego prawa podstawowego (wyrok z dnia 27 marca 2014 r., *UPC Telekabel Wien*, C-314/12, EU:C:2014:192, pkt 62).*

## **6. Jak na tle prawa UE wyglądają mechanizmy ochrony treści dostępne w Polsce**

### **• Postępowania karne i cywilne wobec naruszcycieli**

W przepisach prawa polskiego formalnie istnieją mechanizmy prawne umożliwiające dochodzenie ochrony prawnej treści audiowizualnych rozpowszechnianych nielegalnie, tj. bez zgody uprawnionych. Ochrona ta, z uwagi na specyfikę treści audiowizualnych jest z punktu widzenia uprawnionych do tych treści nieefektywna, a platformy oraz serwisy VOD udostępniające treści rozpowszechniane bez zgody uprawnionych odnoszą znaczne korzyści kosztem uprawnionych.

Jest to wynikiem tego, że podstawowym dostępnym mechanizmem prawnym do walki z nielegalnym rozpowszechnianiem treści audiowizualnych, czyli piractwem tych treści, jest możliwość dochodzenia zaniechania nielegalnego rozpowszechniania tych oraz odszkodowania z tytułu szkody poniesionej z tego tytułu w drodze postępowania karnego lub cywilnego. Korzystanie z treści audiowizualnych będących przedmiotem prawa autorskiego lub praw pokrewnych, w tym ich rozpowszechnianie bez zgody

uprawnionego, stanowi przestępstwo<sup>22</sup>, którego sprawcy mogą być ścigani w drodze postępowania karnego. Ponadto, żądanie od podmiotów nielegalnie rozpowszechniających treści audiowizualne zaprzestania naruszeń oraz zapłaty odszkodowania możliwe jest też w postępowaniu cywilnym. Problemem w ściganiu piractwa internetowego treści audiowizualnych w postępowaniach sądowych jest długotrwałość. Kolejną przeszkodą w skutecznej ochronie przed piractwem treści audiowizualnych w internecie jest kwestia ustalenia sprawcy lub pozwanego, tj. podmiotu, który w sposób zawiniony przyczynia się do takiej nielegalnej dystrybucji. W przypadku pirackich platform oraz serwisów, ustalenie podmiotu odpowiedzialnego za nielegalne rozpowszechnianie treści jest przynajmniej czasochłonne, a niejednokrotnie niemożliwe. Ukrywanie możliwości identyfikacji przez serwisy pirackie jest immanentnie związane z tego rodzaju działalnością. Przewaga po stronie tego rodzaju naruszcycieli wobec uprawnionych do treści wynika z także z tego, że w czasie, w którym uprawnieni inwestują zasoby w prowadzenie postępowań przeciwko naruszcicielom, ci ostatni w tym czasie odnoszą korzyści z nieuprawnionego rozpowszechniania cudzych treści. W tym czasie, dla uprawnionych treści audiowizualne tracą swoją wartość na skutek ich nielegalnej dystrybucji. Dostępność tych treści w serwisach pirackich „za darmo” lub za wynagrodzeniem niższym niż legalny dostęp analogicznego katalogu treści powoduje, że zmniejsza się ilość nabywców dostępu do usług audiowizualnych działających legalnie. Dodatkowo, w przeciwieństwie do uprawnionych, serwisy pirackie nie ponoszą kosztów inwestycji w produkcję i legalną dystrybucję treści audiowizualnych.

- **Żądania odwrócenia grożącego niebezpieczeństwa na podstawie art. 439 kodeksu cywilnego**

Oprócz postępowań karnych i cywilnych, w których uprawnieni do treści audiowizualnych mogą dochodzić zaniechania naruszeń i odszkodowania od naruszcycieli, przepisy obowiązujące w Polsce zawierają też inne mechanizmy prawne. Jednakże one także nie zapewniają uprawnionym skutecznej walki z rozwiniętym technologicznie piractwem internetowym tych treści. Jednym z tych mechanizmów jest możliwość skierowania do sądu cywilnego przez uprawnionego żądania odwrócenia grożącego niebezpieczeństwa na podstawie art. 439 kodeksu cywilnego<sup>23</sup>. Takie żądanie kierowane jest za pośrednictwem sądu nie do bezpośredniego naruszcyciela praw do treści audiowizualnych, a do podmiotu, z którego usług korzysta naruszciciel w celu nielegalnego udostępniania treści, jak na przykład dostawca usług hostingu, czy dostawca usług udostępniania treści online (jak platformy udostępniania wideo, udostępniające treści zamieszczane przez użytkowników).

---

<sup>22</sup> Rozdział 14 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. Dz.U.2022.2509 t.j. z dnia 06.12.2022 r. z późn.zm.)

<sup>23</sup> Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny.

Zgodnie z treścią art. 439 KC: „*Ten, komu wskutek zachowania się innej osoby, w szczególności wskutek braku należytego nadzoru nad ruchem kierowanego przez nią przedsiębiorstwa lub zakładu albo nad stanem posiadanego przez nią budynku lub innego urzędnienia, zagraża bezpośrednio szkoda, może żądać, ażeby osoba ta przedsięwzięła środki niezbędne do odwrócenia grożącego niebezpieczeństwa, a w razie potrzeby także, by dała odpowiednie zabezpieczenie.*”

Na podstawie powyższego przepisu formalnie możliwe jest żądanie, aby sąd nakazał podmiotowi, którego usługi są wykorzystywane do nielegalnego rozpowszechniania treści audiowizualnych, zatrzymania takiego rozpowszechniania przez uniemożliwienie dostępu do tej treści (zablokowanie, usunięcie lub w inny sposób uniemożliwienie dostępu do niej, w zależności od rodzaju usługi, z której wykorzystaniem rozpowszechniane są nielegalnie treści). Jednak przepis ten ze względów prawnych i praktycznych nie może spełnić swojej roli jako środek prawny będący podstawą szybkiego skutecznego blokowania nielegalnie rozpowszechnianych treści audiowizualnych. Zastosowanie tego przepisu wymaga bowiem wykazania nie tylko samego faktu, iż z wykorzystaniem usług danego dostawcy usług (np. platformy udostępniania wideo) rozpowszechniane są nielegalnie treści, ale też prawdopodobieństwa poniesienia szkody przez uprawnionego w stopniu znacznym<sup>24</sup> oraz bezprawności działania dostawcy usług, czyli wymagane jest, aby działaniu dostawcy usług, również mogła zostać przypisana obiektywna nieprawidłowość jego działań (bezprawność)<sup>25</sup>. Wprawdzie przepis ten nie wymaga wykazania zawinionego udziału dostawcy usługi rozpowszechnianiu treści z naruszeniem prawa, jednak już sama konieczność wykazania przed sądem powyższych dwóch przesłanek w postępowaniu sądowym sprawia, biorąc pod uwagę faktyczny czas trwania procesu sądowego, że przepis ten, w aktualnych realiach, nie może być skutecznego środka do walki z piractwem online treści audiowizualnych, gdzie serwisy pirackie w ciągu minut, a nawet sekund od emisji danej treści, są w stanie rozpowszechnić ją nielegalnie, jak np. w przypadku nielegalnych transmisji wydarzeń sportowych i innych treści na żywo, bądź też filmowych premier telewizyjnych.

Warto przy tej okazji zwrócić uwagę Wyrok Sądu Najwyższego z dnia 27 maja 2022 r. o sygn. II CSKP 3/22 dotyczący platformy udostępniania treści online, która umożliwiała dostęp do treści zamieszczanych w niej przez użytkowników. Znamienne w kontekście omawiania skuteczności dostępnych mechanizmów prawnych w walce z piractwem online jest to, że wyrok Sądu Najwyższego w tej sprawie zapadł po około 10 latach od jej wszczęcia przed sądem pierwszej instancji. Sąd Najwyższy odniósł się w uzasadnieniu wyroku do art. 439 kodeksu cywilnego jako środka ochrony przed nielegalnym rozpowszechnianiem treści chronionych prawem jedynie przez ogólne

---

<sup>24</sup> Tak też: wyrok Sądu Apelacyjnego w Gdańsku z dnia 25 listopada 2014 r., V ACa 637/14

<sup>25</sup> Zob też: Ciszewski Jerzy (red.), Kodeks cywilny. Komentarz, wyd. II; Opublikowano: LexisNexis 2014; Balwicka-Szczyrba Małgorzata (red.), Sylwestrzak Anna (red.), Kodeks cywilny. Komentarz aktualizowany. Opublikowano: LEX/el. 2023

wskazanie, że: „*Położenie w ustawodawstwie unijnym nacisku na zagwarantowanie podmiotowi praw autorskich ochrony przez danie mu do dyspozycji środków mających na celu zapobieżenie wszelkim dalszym szkodom oznacza, że w stosunku do operatora platformy internetowej, który mając wiarygodną wiadomość o przechowywaniu przez użytkowników plików zawierających utwory chronione prawem autorskim, prowadzi także działalność polegającą na współpracy z takimi użytkownikami w udostępnianiu takich plików innym osobom w ten sposób, że za zapłatą stosownego wynagrodzenia zapewnia innym osobom dostęp do treści tego pliku i umożliwia sporządzenie przez nich kopii utworu, nie jest wyłączone roszczenie oparte na art. 439 k.c.*” Nie można pomijać faktu, że Sąd Najwyższy wskazał na możliwość zastosowania art. 439 kodeksu cywilnego w ściśle określonych okolicznościach, tj. w których operatorowi platformy internetowej została wykazana wiedza o rozpowszechnianiu z wykorzystaniem jego usług treści chronionych prawem autorskim i aktywna współpraca z naruszcycielem. Prowadzi to do odpowiedzialności własnej takiego dostawcy usług pośrednich. Sąd Najwyższy wskazał w uzasadnieniu, że: „*Co więcej, sposób działania strony pozwanej jest taki, że samodzielnie i aktywnie angażuje się w udostępnianie plików nieograniczonej liczbie osób, w tym plików zawierających dane bezprawne oraz współpracuje w udostępnianiu konkretnych plików zawierających utwory chronione prawem autorskim, (...)*”. Dalej Sąd Najwyższy wskazuje: „*W stanie faktycznym sprawy zastosowanie przez Sąd drugiej instancji art. 439 k.c. jest prawidłowe, tak co do zasady, jak i zakresu. Jak wspomniano już powołane przepisy prawa unijnego nie stoją na przeszkodzie skorzystaniu przez poszkodowanego z uprawnienia przewidzianego w art. 439 k.c., tym bardziej, że do czasu zakończenia postępowania w drugiej instancji, tj. przez okres pięciu lat, strona pozwana nie podjęła jakichkolwiek działań mających na celu zapobieżenie dalszemu naruszaniu majątkowych praw autorskich powodów, co potwierdza realność naruszania tych praw w przyszłości.*” Dla Sądu Najwyższego nie uległo wątpliwości ustalenie w stanie faktycznym sprawy, iż: „*Nie ulega wątpliwości, że deliktowe zachowanie pozwanej było zawinione i taka negatywna ocena jest uzasadniona z punktu widzenia obiektywnego jak i subiektywnego.*” Nie jest to zatem żądanie zatrzymania naruszeń kierowane do dostawcy usług pośrednich w rozumieniu nakazu blokującego wydawanego wobec podmiotu niewinnego, bez konieczności istnienia przesłanek do negatywnej oceny jego własnych działań, który ma jedynie zatrzymać naruszenie dokonywane przez naruszydca, z uwagi na swoje możliwości techniczne.

- **Odpowiedzialność dostawców usług pośrednich za nielegalne treści w ich usługach na podstawie DSA**

Powyższy wyrok Sądu Najwyższego może stanowić wstęp do omówienia, na czym polega odpowiedzialność tzw. dostawców usług pośrednich, czyli także takich podmiotów jak pozwana w omówionej sprawie internetowa platforma udostępniania wideo lub też przedsiębiorca telekomunikacyjny świadczący usługi dostępu do internetu (tzw. dostawca internetu).

Odpowiedzialność własna dostawców usług pośrednich zostanie omówiona na podstawie przepisów Aktu o Usługach Cyfrowych (DSA)<sup>26</sup>, pomimo tego, że w polskich przepisach nadal obowiązuje regulacja tej odpowiedzialności na podstawie art. 12 – 15 w Rozdziale 3 ustawy o świadczeniu usług drogą elektroniczną<sup>27</sup>, zatytułowanym „Wyłączenie odpowiedzialności usługodawcy z tytułu świadczenia usług drogą elektroniczną”. Wynika to z następujących zasadniczych powodów. Materia ww. Rozdziału 3 ustawy regulowana jest art. 4 – 8 Rozdziału II DSA zatytułowanym „Odpowiedzialność dostawców usług pośrednich”. DSA jest aktem mającym bezpośrednie zastosowanie w państwach członkowskich UE i obowiązuje od 17 lutego 2024 r. Ponadto, proces legislacyjny ustawy wdrażającej DSA jest na aktualnie na końcowym etapie rządowym. Projekt ustawy zmieniającej ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344)<sup>28</sup> uchyla Rozdział 3 ustawy o świadczeniu usług drogą elektroniczną. W to miejsce będą obowiązywały art. 4 – 8 Rozdziału II DSA. Zasady odpowiedzialności dostawców usług pośrednich według DSA są podobne do tych obowiązujących obecnie na podstawie ustawy o świadczeniu usług drogą elektroniczną.

Dostawcami usług pośrednich zgodnie z DSA są dostawcy usług „zwykłego przekazu” polegających na transmisji w sieci telekomunikacyjnej informacji przekazanych przez odbiorcę usługi lub na zapewnianiu dostępu do sieci telekomunikacyjnej, „cachingu” polegających na transmisji w sieci telekomunikacyjnej informacji przekazanych przez odbiorcę usługi, obejmującą automatyczne, pośrednie i krótkotrwałe przechowywanie tej informacji, dokonywane wyłącznie w celu usprawnienia późniejszej transmisji informacji na żądanie innych odbiorców, jak też „hostingu” polegających na przechowywaniu informacji przekazanych przez odbiorcę usługi oraz na jego żądanie. Przepisy Rozdziału II DSA wskazują przesłanki, odrębnie dla danego rodzaju dostawcy usług pośrednich, w których dostawca usług nie ponosi odpowiedzialności za informacje (treści) osób trzecich (usługobiorców) znajdujących się w jego usługach. Zasadniczo statuują one zasadę, według której dostawca usług nie ponosi odpowiedzialności własnej za treści (informacje) znajdujące się w jego usługach zamieszczane tam lub przekazywane z wykorzystaniem jego usług przez osoby trzecie wówczas, gdy dostawca pozostaje neutralny, nie ma wiedzy o nielegalnym charakterze treści znajdujących się w jego usługach i nie bierze aktywnego udziału w ich przekazie.

W kontekście nielegalnego rozpowszechniania treści audiowizualnych istotny jest art. 6 DSA w zw. z art. 16 DSA. Art. 6 DSA wskazuje, kiedy dostawca usług hostingu,

---

<sup>26</sup> Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)

<sup>27</sup> Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.2024.1513 t.j. z dnia 2024.10.14 z późn.zm.)

<sup>28</sup> Projekt z dnia 27.11.2024 r. ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną (ustawy z dnia 18 lipca 2002 r.): <https://legislacja.rcl.gov.pl/docs//2/12383101/13045617/13045618/dokument694959.pdf>

ale też dostawca platformy internetowej, nie ponoszą odpowiedzialność za nielegalne treści znajdujące się w ich usługach. Dostawcy ci nie ponoszą odpowiedzialności za nielegalne treści przekazywane za udostępniane za pośrednictwem ich usług przez osoby trzecie korzystające z tych usług, jeśli nie mają faktycznej wiedzy o nielegalnej działalności lub nielegalnych treściach, a w odniesieniu do roszczeń odszkodowawczych – nie wiedzą o stanie faktycznym lub okolicznościach, które świadczą o nielegalnej działalności lub nielegalnych treściach. Ponadto, dostawcy ci nie ponoszą odpowiedzialności, jeśli po uzyskaniu takiej wiedzy podejmą bezzwłocznie odpowiednie działania w celu usunięcia lub uniemożliwienia dostępu do nielegalnych treści. Taką wiedzę dostawcy wskazanych wyżej usług mogą uzyskać w wyniku zastosowania mechanizmu notice and action (zgłaszania i działania) przewidzianego w art. 16 DSA. Zgodnie z art. 16 DSA, dostawcy usług hostingu i platform internetowych mają obowiązek umożliwienia każdemu zgłoszenie im obecności w ich usłudze określonych informacji, które zgłaszający uważają za nielegalne treści. Po uzyskaniu takiego zgłoszenia dostawca usług podejmuje decyzje, czy potraktuje daną informację jako nielegalną treść i ograniczy ją dostępność, np. usunie, czy nie. Jednak niezależnie od podjętej decyzji, zgłoszenia te dają podstawę do uzyskania faktycznej wiedzy lub wiadomości do celów art. 6 w odniesieniu do określonej informacji, której dotyczą, jeżeli umożliwiają dostawcy usług hostingu działającemu z należytą starannością stwierdzenie – bez szczegółowej analizy prawnej – nielegalnego charakteru danej działalności lub informacji. Jeśli zatem dostawca usługi podejmie decyzję o nieusuwaniu informacji, która następnie okaże się być nielegalną treścią, przestaje działać wyłącznie jego odpowiedzialności za informacje osób trzecich znajdujące się w jego usłudze. W tej sytuacji istnieje podstawa do ustalenia odpowiedzialności własnej dostawcy usług pośrednich, za jego własne działania dotyczące nielegalnych treści znajdujących się w jego usługach zamieszczonych tam przez osoby trzecie. Wracając do wspomnianego wyżej wyroku Sądu Najwyższego z dnia 27 maja 2022 r. o sygn. II CSKP 3/22, w uzasadnieniu wyroku wskazano na wiedzę platformy internetowej co do występowania w jej usługach treści z naruszeniem prawa autorskiego oraz zawiniony udział własny platformy w tym naruszeniu. Zatem w rozumieniu DSA istniała podstawa do ustalenia odpowiedzialności własnej z tytułu udostępniania przez platformę nielegalnych treści zamieszczane w niej przez osobę trzecią.<sup>29</sup>

Odpowiedzialność dostawców usług pośrednich za nielegalne treści przekazywane z wykorzystaniem ich usług przez osoby trzecie (użytkowników tych usług), jak też mechanizm zgłaszania i działania, to zatem zupełnie inne instrumenty prawne dostępne dla uprawnionych, których treści audiowizualne są rozpowszechniane nielegalnie, niż nakazy blokujące. Nie mają one tej skuteczności, co nakazy zablokowania określonych

---

<sup>29</sup> Należy jednak zaznaczyć, że wyrok został wydany w stanie prawnym, w którym obowiązywała ustawa dnia 18 lipca 2002 r. w wersji implementującej Dyrektywę 2000/31/WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego na rynku wewnętrznym (dyrektywa o handlu elektronicznym).

nielegalnych treści wydawane przez sąd lub organ administracji publicznej, które dostawca usług ma obowiązek wykonać i które wydawane się niezależnie od oceny działań dostawy usługi, jako do podmiotu niewinnego. Dostawca usług hostingu może na podstawie zgłoszenia zdecydować, jakie działanie podejmie w stosunku do informacji zgłoszonej jako nielegalna treść. Nie jest zobowiązany do jej usunięcia lub w inny sposób ograniczenia dostępu do niej. Jeśli jej nie usunie, może ponieść własną odpowiedzialność wobec uprawnionego, z tytułu wysłanych działań w stosunku do nielegalnych treści, o których miał wiedzę, w postępowaniu przed odpowiednim organem, gdzie w Polsce jest to sąd. Potwierdza to też treść ust. 4 w art. 6 DSA, zgodnie z którym zasady odpowiedzialności dostawców usług określone w art. 6 DSA nie mają wpływu na możliwość wymagania od dostawcy usług przez organy sądowe lub administracyjne, zgodnie z systemem prawnym państwa członkowskiego, żeby przerwał naruszanie prawa lub mu zapobiegł. Są to zatem niezależne od siebie mechanizmy, działające w inny sposób pod względem prawnym i mające inną skuteczność.

Istotną kwestią w opisanym wyżej zasadzie odpowiedzialności dostawców usług i mechanizmie zgłaszania i działania jest to, że dotyczy to dostawców usług hostingu i platform internetowych. Mechanizm zgłaszania i działania nie dotyczy dostawców usług cachingu oraz zwykłego przekazu, w tym dostawców internetu, którzy mają bezpośrednią możliwość uniemożliwienia dostępu do nielegalnych treści użytkownikom ich usług. Wobec tych podmiotów nie istnieje zatem obowiązek działania na zgłoszenie nielegalnej treści, który może być podstawą do uznania, iż dostawcy ci mieli wiedzę lub wiadomość co do nielegalnych treści w ich usługach, co z kolei może prowadzić do ustalenia tej odpowiedzialności. Nie znaczy to, że nie można ustalić odpowiedzialności własnej tych dostawców usług za nielegalne treści w ich usługach w inny sposób, jednak nie ma podstawy prawnej do żądania od nich działania w ramach opisanego mechanizmu zgłaszania i działania. Jednocześnie w praktyce, w przypadku pirackich platform udostępniania wideo, czyli takich które strukturalnie są przeznaczone do rozpowszechniania treści audiowizualnych bez zgody uprawnionych albo nie ma możliwości dokonania zgłoszenia, w związku z tym, że platforma nie udostępnia takiej możliwości, albo platformy nie reagują na takie zgłoszenia. W dalszym ciągu istnieje możliwość ustalenia odpowiedzialności własnej platformy, jednak często podmiot odpowiedzialny wobec przeciwko któremu mógłby toczyć się taki proces jest trudny albo niemożliwy do zidentyfikowania. W przypadku ustalenia podmiotu odpowiedzialnego, często okazuje się, że jest podmiot prowadzący działalność z zagranicy, a prowadzenie wobec niego procesu jest często praktycznie niemożliwe z uwagi na unikanie odpowiedzialności. Nawet jednak zidentyfikowanie naruszcyciela nie rozwiązuje zagadnienia długotrwałości procesu cywilnego lub karnego, w czasie którego nielegalne rozpowszechnianie treści przez platformy pirackie trwa, a wartość treści dla podmiotu uprawnionego maleje, co wielokrotnie oznacza znaczną stratę w stosunku do inwestycji poczynionych w wyprodukowanie tej treści lub nabycie do niej praw.

Wobec powyższego przepisy DSA nie adresują w pełni potrzeb uprawnionych do treści audiowizualnych w zakresie walki z praktykami serwisami

- **Blokowanie treści chronionych prawem autorskim przez dostawców usług udostępniania treści online na podstawie prawa autorskiego**

Uprawnieni do treści audiowizualnych będących przedmiotem prawa autorskiego lub praw pokrewnych zyskali narzędzie do walki z nielegalnym rozpowszechnianiem tych treści na skutek implementacji Dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE („Dyrektywa DSM”). Dyrektywa DSM została implementowana ustawą z dnia 26 lipca 2024 r. o zmianie ustawy o prawie autorskim i prawach pokrewnych, ustawy o ochronie baz danych oraz ustawy o zbiorowym zarządzaniu prawami autorskimi i prawami pokrewnymi, a wraz z nią art. 17 Dyrektywy DSM dotyczący odpowiedzialności dostawców usług udostępniania treści online, takie jak platformy udostępniania wideo, za legalne korzystanie z treści chronionych prawem autorskim lub prawami pokrewnym. Przed wdrożeniem Dyrektywy DSM, to użytkownik platformy udostępniania treści online odpowiedzialny był za zamieszczenie na niej treści bez zgody uprawnionego. W tej sytuacji egzekwowanie usunięcia treści oraz odpowiedzialności za jej nielegalne udostępnianie od pojedynczych osób, użytkowników platformy, często trudnych do ustalenia, było znacznie utrudnione. Wdrożenie Dyrektywy DSM zmieniło powyższą zasadę. Zgodnie z nową zasadą wprowadzoną ww. ustawą dnia 26 lipca 2024 r., dostawcy usług udostępniania treści online, w tym platformy udostępniania wideo, stali się podmiotami odpowiedzialnymi za udzielanie przez nich publicznego dostępu do utworu zamieszczonego przez usługobiorcę. Według nowych przepisów stanowi to publiczne udostępnienie utworu przez tego dostawcę, na dokonanie którego to dostawca (platforma udostępniania online) musi pozyskać zgodę uprawnionych. W przeciwnym razie będzie on odpowiedzialny za nielegalne publiczne udostępnienie utworu, na przykład audiowizualnego, chyba że wykaże, że dopełnił on obowiązków, które zgodnie z ustawą zwalniają dostawcę z takiej odpowiedzialności. Aby zwolnić się z odpowiedzialności za udostępnienie treści bez zgody uprawnionego, dostawca musi wykazać, że dołożył należytej staranności, aby uzyskać tę zgodę, ale także, że dołożył należytej staranności, aby uniemożliwić dostęp do utworu (jeżeli uprawniony przekazał mu informacje odpowiednie i niezbędne do osiągnięcia tego celu, pozwalające w szczególności na ustalenie uprawnionego i identyfikację utworu z uwzględnieniem dostępnych środków technologicznych), oraz działał niezwłocznie po otrzymaniu od uprawnionego należyte uzasadnione żądanie zablokowania dostępu do tego utworu lub usunięcia go ze swoich stron internetowych, a także dołożył należytej staranności, aby uniemożliwić dostęp do tego utworu w przyszłości (jeżeli uprawniony przekazał mu odpowiednie informacje). Wobec czego, w przypadku braku zgody uprawnionego, dostawcy usług udostępniania online muszą, w uproszeniu, blokować rozpowszechnianie na ich platformie treści, na

rozpowszechnianie których nie uzyskali zgody. W celu takiego blokowania muszą uzyskać informacje od uprawnionych, które pomogą dostawcom platform zidentyfikować konkretne treści do ich blokowania. Chodzi tutaj na przykład o odpowiednie oznaczanie treści z wykorzystaniem stosowanych technologii cyfrowych, takich jak watermarking, czy fingerprinting, pozwalających systemom stosowanym przez platformy na wykrywanie i blokowanie zamieszczania w ich usługach oznaczonych w ten sposób treści przez osoby nieuprawnione. Obowiązki te są ograniczone w stosunku do platform nie przekraczających określonych w ustawie progów.

Jednak co bardziej istotne dla oceny, czy opisany wyżej mechanizm jest efektywnym i wystarczającym narzędziem do walki z piractwem online treści audiowizualnych, dotyczy on tylko platform udostępniania online, a nie dotyczy pirackich serwisów VOD, które pozostają poza jego regulacją. Ponadto, mechanizm ten dotyczy specyficznego rodzaju platform, to jest tzw. dużych platform udostępniania online, których głównym przedmiotem działalności jest przechowywanie i udzielanie publicznego dostępu do znacznej liczby utworów lub przedmiotów praw pokrewnych zamieszczanych przez usługobiorców, które to utwory lub przedmioty praw pokrewnych są przez niego organizowane i promowane w celach zarobkowych. Dodatkowo, po części analogicznie do rozwiązania przyjętego w mechanizmie zgłaszania i działania oraz odpowiedzialności dostawców usług przyjętych w DSA, platforma ma wprawdzie obowiązek blokowania udostępniania wskazanych przez uprawnionego treści, ale obowiązek ten ma inny charakter prawny niż obowiązek wykonania nakazu blokowania w drodze decyzji sądu lub organu administracji publicznej. Brak wykonania obowiązku blokowania przez platformę na podstawie informacji przekazanych przez uprawnionego rodzi odpowiedzialność po stronie platformy, której uprawniony może dochodzić w drodze postępowania sądowego. W przypadku platform pirackich, systemowo przeznaczonych do udostępniania treści audiowizualnych bez zgody uprawnionych, w praktyce mechanizm ten nie będzie skutecznym środkiem do ochrony przed piractwem treści online.

- **Reakcje serwisów pirackich na zgłoszenia nielegalnych treści**

Wspomniane wyżej badanie Stowarzyszenia Sygnał z października 2023<sup>30</sup>. Zbadało także reakcje serwisów pirackich na zgłoszenia nielegalnych treści. Kluczowy podział objął dwa typy podmiotów: takie, które same w sobie nie działają w intencji kradzieży treści (mogą to być na przykład platformy, na których sami użytkownicy Internetu udostępniają treści AV), tzw. serwisy pirackie, których model funkcjonowania jest stworzony w celu czerpania korzyści z nielegalnej dystrybucji treści. Z ww badania wynika, że te pierwsze co do zasady współpracują z właścicielami materiałów. Jednak

---

<sup>30</sup><https://sygнал.org.pl/wp-content/uploads/2024/02/Raport-Stowarzyszenia-Sygnał-Skuteczność-zgłoszeń-naruszeń-treści-audiowizualnych.pdf>

współpraca ta nie jest w pełni efektywna, gdyż – około jedna trzecia zgłoszeń to tzw. „zgłoszenia iluzoryczne”, ponieważ usunięte treści pojawiają się ponownie na tych samych platformach. Jak wskazuje badanie: „Masę krytyczną (ponad 8,2 mln) zgłoszeń stanowiły te, które były wysyłane do serwisów pirackich, a więc intencjonalnie prowadzonych w celu czerpania korzyści z nielegalnej dystrybucji treści. To 99% wszystkich przypadków. Prawie wszystkie takie zgłoszenia, poza nielicznymi wyjątkami, były wysyłane za pomocą niezautomatyzowanej formy. Wśród nich aż 70% to wspomniane wcześniej problematyczne zgłoszenia iluzoryczne (prawie 6 mln przypadków). W przypadku tego typu serwisów zautomatyzowany mechanizm zgłoszeń praktycznie nie funkcjonuje. Istnieją także takie serwisy, które nie dają w ogóle możliwości przesłania zgłoszenia (brak formularzy, danych kontaktowych itp.). Z tego powodu prawie 1600 naruszeń nie zostało w ogóle zgłoszonych. W obydwu przypadkach – zarówno platform, jak i serwisów pirackich – 58% stanowiły zgłoszenia skuteczne.”

## **PODSUMOWANIE**

Jak wynika z powyższej analizy, dostępne w obowiązujących w Polsce przepisach mechanizmy prawne nie są wystarczające skuteczne do wale z piractwem treści audiowizualnych online i nie odpowiadają koncepcji możliwości stosowania tzw. nakazów blokujących wobec podmiotu niewinnego wynikającej z Dyrektywy Autorskiej oraz dyrektywy 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej, czyli wobec pośredników internetowych, którzy sami nie ponoszą odpowiedzialności za nielegalne rozpowszechnianie treści przez sprawców naruszeń, ale których usługi wykorzystywane są przez tych sprawców w celu dotarcia do użytkowników.

W polskim prawie możliwe jest wprowadzenie dochodzenia zaniechania naruszeń i odszkodowania od naruszcyciela, będącego zidentyfikowanym podmiotem, w postępowaniu sądowym, a także skierowanie żądania zablokowania lub usunięcia nielegalnej treści (lub uniemożliwienia dostępu do niej w inny sposób) do dostawcy usług hostingu lub platformy internetowej (na podstawie DSA) lub dostawcy usług udostępniania treści online, jak np. platforma udostępniania wideo (na podstawie ustawy o prawie autorskim i prawach pokrewnych). Jednak długotrwałe postępowania sądowe nie są efektywnym mechanizmem w obliczu działalności serwisów pirackich. W przypadku natomiast kierowania żądania do wymienionych wyżej dostawców usług, inaczej niż w przypadku skierowania do nich nakazu blokującego wydanego przez sąd lub organ administracji, dostawcy ci mogą odmówić blokowania treści, jeśli ich zdaniem nie jest ona nielegalna. Taka błędna ocena może rodzić odpowiedzialność własną dostawców usług pośrednich za rozpowszechnianie nielegalnych treści, w tym odszkodowawczą, dochodzoną na drodze sądowej. Jednak nie spełnia to funkcji i celu nakazu blokującego wydawanego wobec tzw. podmiotu niewinnego, który ma być środkiem pozwalającym na szybkie zatrzymanie rozpowszechniania nielegalnej treści online.

Potrzenie wprowadzenia do polskich przepisów mechanizmów prawnych umożliwiających wydawanie nakazów blokujących wobec osób niewinnych, zgodnie z opisaną wyżej koncepcją przyjętą przez prawodawcę unijnego, dopowiada w znacznej części propozycja zmian do ustawy o świadczeniu usług drogą elektroniczną<sup>31</sup>. Projekt zmian do ww. ustawy wprowadza podstawę prawną do wydawania nakazów blokujących, a konkretnie „*nakazu podjęcia działań przeciwko nielegalnym treściom polegającego na uniemożliwieniu dostępu do nielegalnych treści występujących w usłudze świadczonej przez dostawcę usług pośrednich*”. Chodzi tu o kilka rodzajów nielegalnych treści podlegających blokowaniu, a mianowicie treści naruszających dobra osobiste, treści których rozpowszechnianie wyczerpuje znamiona czynu zabronionego lub pochwalających lub nawołujących do popełnienia czynu zabronionego, a także treści naruszających prawa własności intelektualnej. Nakazy mają być wydawane na wniosek, w trybie administracyjnym w formie decyzji, przez Prezesa Urzędu Komunikacji Elektronicznej. Nakazy te mają być wydawane wobec dostawców usług pośrednich, których usługi są wykorzystywane do przekazywania użytkownikom usług (internautom) nielegalnych treści przez inne podmioty (odbiorców tych usług). Stosowanie tych nakazów ułatwiłoby znacznie uprawnionym do treści audiowizualnych zwalczanie nielegalnego rozpowszechniania tych treści. Przewidziane w projekcie ustawy zmieniającym ustawę o świadczeniu usług drogą elektroniczną rozwiązanie może znacznie ułatwić uprawnionym do treści audiowizualnych zwalczanie nielegalnego rozpowszechniania tych treści. Jednak w dalszym ciągu nie odpowiada ono w pełni potrzebie zwalczania piractwa treści audiowizualnych online i nie nadąża za stosowanymi już od dawna sposobami działania serwisów i platform strukturalnie przeznaczonych do naruszania praw uprawionych.

Usługi pirackie mają dużą zdolność do szybkiego udostępniania treści pod różnymi lokalizacjami oraz zmian tych lokalizacji. Na przykład serwis VOD udostępniany pod nazwą domeny xyz.com, po skutecznym zablokowaniu jego dostępności pod tą nazwą domeny w wyniku zastosowania nakazu blokującego, udostępnia te same treści często niemal natychmiast pod inną nazwą domeny, np. xyz2.com. Dochodzi więc do wielokrotnego udostępniania tych samych treści np. pod zmienioną nazwą domeny lub zmienionym adresem IP tak, aby były one trudne do namierzenia i skutecznego zablokowania. Są to tzw. pączkujące strony lub „mirror sites”.

Wobec powyższego, dla zwalczania nielegalnego rozpowszechniania treści przez takie „mirror sites” niezbędna jest możliwość wydawania tzw. dynamicznych nakazów blokujących. Jest to rodzaj nakazów, wydawanych w trybie sądowym lub administracyjnym, które umożliwiają zablokowanie dostępu do tych samych (lub zasadniczo takich samych) treści, do których dostęp pod określoną lokalizacją został już

---

<sup>31</sup> Projekt z dnia 27.11.2024 r. ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną (ustawy z dnia 18 lipca 2002 r.): <https://legislacja.rcl.gov.pl/docs//2/12383101/13045617/13045618/dokument694959.pdf>

objęty wydanym nakazem blokującym. Możliwość stosowania nakazów dynamicznych potwierdzona została już w orzecznictwie TSUE, a potrzeba ich wprowadzenia została podkreślona także w Zaleceniu Komisji (UE) 2023/1018 z dnia 4 maja 2023 r. w sprawie zwalczania piractwa internetowego wydarzeń sportowych i innych wydarzeń na żywo. Zalecenie to wskazuje na dynamiczne nakazy obejmujące nowe lokalizacje internetowe jako skuteczny środek zapobiegający nieuprawnionej retransmisji i jej kontynuacji, zwłaszcza wobec strategii odporności opracowanych przez pirackie serwisy, na przykład zakładania lustrzanych stron pod różnymi nazwami domen lub przechodzenia na różne adresy IP w celu obejścia środków blokujących.

Ponadto, dla skutecznego zwalczania nielegalnych transmisji wydarzeń sportowych, innych wydarzeń na żywo, a także takich treści jak np. premiery telewizyjne, konieczna jest możliwość stosowania tzw. nakazów live, które pozwalają na blokowanie takich nielegalnych transmisji natychmiast, w czasie emisji oryginalnej transmisji. W przypadku takich treści ważne jest natychmiastowe zablokowanie nielegalnych udostępnień, ze względu na to, że mają największą wartość w chwili transmisji na żywo, a wartość tę tracą w przeważającej części lub w całości z chwilą ich nielegalnego udostępnienia. Nakazy live, aby mogły spełnić swój cel, powinny być wydawane jako nakazy dynamiczne, tj. powinny obejmować lokalizacje pod którą pojawią się te same treści już po wydaniu nakazu.

Przepisy wielu krajów członkowskich UE przewidują możliwość dynamicznego blokowania live, niezależnie od tego, czy korzystają z procedury cywilnej czy administracyjnej, jak np. we Włoszech, czy w Portugalii<sup>32</sup>. Rozwiązaniem stosowanym, np. w Wielkiej Brytanii oraz we Włoszech jest wydanie nakazu blokującego jeszcze przed rozpoczęciem nielegalnej transmisji. Taki nakaz może zostać wydany na podstawie zapowiedzi nielegalnych transmisjach, które pojawiają się np. na stronach pirackich jeszcze przed jej rozpoczęciem, np. promowanie dostępu do nielegalnej transmisji danego wydarzenia jeszcze przed jego rozpoczęciem. Taki nakaz blokujący live wydawany jest jeszcze przed rozpoczęciem transmisji na żywo, ale może on zostać wykonany przez dostawcę usług pośrednich, tj. dostęp do danej nielegalnej treści może zostać zablokowany, dopiero w momencie rozpoczęcia jej nielegalnego udostępniania. Istnieją zatem rozwiązania prawne, które działają w praktyce często od wielu lat, z których można skorzystać w celu wypracowania skutecznego mechanizmu blokowania nielegalnego rozpowszechniania treści audiowizualnych online i szerzej naruszeń praw własności intelektualnej.

---

<sup>32</sup> LEGGE 14 luglio 2023, n. 93 "Disposizioni per la prevenzione e la repressione della diffusione illecita di contenuti tutelati dal diritto d'autore mediante le reti di comunicazione elettronica". (23G00103) (GU Serie Generale n.171 del 24-07-2023) / *Law No. 93 of 14 July 2023 'Provisions for the prevention and suppression of the unlawful distribution of copyright-protected content through electronic communication networks (23G00103) (OJ General Series No. 171 of 24-07-2023)*  
<https://www.gazzettaufficiale.it/eli/id/2023/07/24/23G00103/sg>; Law No. 82/2021 of. 30.11.2021 (Portugal)

W bieżącym stanie prawnym w Polsce, ważnym krokiem będzie skuteczne wprowadzenie do polskiego porządku prawnego wyraźnej podstawy prawnej do wydawania nakazów blokujących, chociażby w takiej formule jak proponuje to projekt ustawy zmieniającej ustawę o świadczeniu usług drogą elektroniczną<sup>33</sup>. Przy założeniu skutecznego działania proponowanego przez ww mechanizmu, znacznie ułatwi on uprawnionym do tych treści ochronę ich praw przez dystrybucją przez serwisy pirackie. Ważne jest jednak także to, że serwisy pirackie to rozwinięte technologicznie usługi, dla zwalczania których konieczne są rozwiązania prawne nadążające za tym rozwojem, jak chociażby możliwość wydawania nakazów dynamicznych i nakazów live. Jest to istotne nie tylko dla podmiotów zaangażowanych w legalną produkcję i dystrybucję treści audiowizualnych i ich znacznych inwestycji finansowych w tę działalność, ale też dla ochrony konsumentów przed zagrożeniami, jakie dla ich bezpieczeństwa w sieci może nieść za sobą korzystanie z serwisów pirackich.

## **BIBLIOGRAFIA**

1. Balwicka-Szczyrba M., Sylwestrzak A. (red.), Kodeks cywilny. Komentarz aktualizowany. Opublikowano: LEX/el. 2023
2. Ciszewski J. (red.), Kodeks cywilny. Komentarz, wyd. II; Opublikowano: LexisNexis 2014
3. Dyrektywa 2000/31/WE z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego na rynku wewnętrznym (dyrektywa o handlu elektronicznym)
4. <https://legislacja.rcl.gov.pl/projekt/12382311/katalog/13040399#13040399>
5. <https://sygnal.org.pl/wp-content/uploads/2024/02/Raport-Stowarzyszenia-Sygnal-Skuteczność-zgłoszeń-naruszeń-treści-audiowizualnych.pdf>
6. <https://www.trade.gov/market-intelligence/poland-ict-most-cyber-attacked-country-world>
7. Komunikat Komisji do Parlamentu Europejskiego, Rady i Europejskiego Komitetu Ekonomiczno-Społecznego z dnia 29 listopada 2017 r. zatytułowany „Wytyczne dotyczące niektórych aspektów dyrektywy 2004/48/WE Parlamentu Europejskiego i Rady w sprawie egzekwowania praw własności intelektualnej” (COM(2017)0708)
8. Projekt z dnia 27.11.2024 r. ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną (ustawy z dnia 18 lipca 2002 r.): <https://legislacja.rcl.gov.pl/docs//2/12383101/13045617/13045618/dokument694959.pdf>

---

<sup>33</sup> Projekt z dnia 27.11.2024 r. ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną (ustawy z dnia 18 lipca 2002 r.): <https://legislacja.rcl.gov.pl/docs//2/12383101/13045617/13045618/dokument694959.pdf>

9. Raport Deloitte "Kradzież treści wideo w Internecie. Analiza wpływu zjawiska piractwa internetowego treści audiowizualnych, w tym telewizyjnych, na gospodarkę Polski". Warszawa, lipiec 2023 r., [https://sygnal.org.pl/wp-content/uploads/2023/07/2023\\_raport\\_kradziezinternetwideo\\_deloitte.pdf](https://sygnal.org.pl/wp-content/uploads/2023/07/2023_raport_kradziezinternetwideo_deloitte.pdf)
10. Rezolucja Parlamentu Europejskiego z dnia 19 maja 2021 r. zawierająca zalecenia dla Komisji w sprawie wyzwań stojących przed organizatorami wydarzeń sportowych w środowisku cyfrowym (2020/2073(INL))
11. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych)
12. Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (w wersji obowiązującej od 3.12.2024 r.)
13. Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz.U.2024.1221 z dnia 2024.08.09 z późn.zm.)
14. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U.2024.1513 t.j. z dnia 2024.10.14 ze zmn)
15. Ustawa z dnia 19 listopada 2009 r. o grach hazardowych (Dz.U.2023.227 t.j. z dnia 2023.02.02).czec

# SAMOLOTY, OSINT I WIELKA POLITYKA

## AIRPLANES, OSINT AND BIG POLITICS

**Krystian WOJCIECHOWSKI**<sup>1</sup>

**Streszczenie:** W artykule opisano wybrane zagadnienia związane z opartą na źródłach otwartych analizą danych lotniczych. Skupiono się na systemie zbierania danych o przebiegu lotu serwisach publikujących dane i problemach z jakością danych wynikających z celowych zakłóceń. Artykuł oparto na licznych przykładach opisanych w sieci internet lub zaobserwowanych przez autora. Tekst stanowi pisemną wersję prezentacji wygłoszonej na konferencji PTXXI w Gdyni w 2024 roku.

**Słowa kluczowe:** OSINT, śledzenie lotów, GPS, ADS-B, dezinformacja.

**Summary:** The article describes selected issues related to open-source based analysis of aviation data. The focus is on the system of collecting flight data services publishing data and data quality problems resulting from intentional interference. The article is based on numerous examples described on the Internet or observed by the author. The text is a written version of a presentation given at the 2024 PTXXI Conference in Gdynia.

**Keywords:** OSINT, flight tracking, GPS, GPS jamming, GPS spoofing, ADS-B, disinformation.

### WSTĘP

Samolot Embraer E190AR o numerze rejestracyjnym 4K-AZ65 Azerskich linii lotniczych wystartował w dniu 25 grudnia 2024 o godzinie 03:55 UTC z lotniska w Baku. Portem docelowym był Grozny w Czeczeni (Rosja). Samolot nie zdołał wylądować w Grozным, oficjalnie z powodu silnej mgły. Nie przyjęły go także pobliskie lotniska we Władykaukazie i Machaczkałe. Pilot postanowił nie wracać do Baku, ale wylądować po drugiej stronie Morza Kaspijskiego w kazachskim Aktau. Niestety przy próbie lądowania samolot rozbił się, a z 62 pasażerów i pięciu członków załogi przeżyło 29 osób. Jak większość wypadków lotniczych przykuł on uwagę mediów i był szeroko komentowany, tym bardziej od samego początku pojawiały się informacje, że przyczyną katastrofy nie

---

<sup>1</sup> Oficer policji w stanie spoczynku. Trener, współtwórca podyplomowych studiów analiz kryminalnej na AGH w Krakowie, biegły sądowy i konsultant w Hexagon Geosystems AG w Szwajcarii, krystianw@me.com.

były problemy z mgłą i zderzenie ze stadem ptaków. Jak się później okazało samolot został ostrzelany przez rosyjską obronę przeciw lotniczą, która we mgle uznała rejsowy samolot za atakujący Grozny ukraiński dron<sup>2</sup>. W Internecie bardzo szybko pojawiły się oficjalne komunikaty i wykonane przez uczestników akcji ratowniczej zdjęcia wraku samolotu uprawdopodobniające wersję o zestrzeleniu maszyny. Kanały Telegramu zajmujące się tematyką lotniczą oraz lokalne kazachskie, azerskie lub specjalizujące się w tematyce kaukaskiej jednoznacznie wskazując jako przyczynę rosyjski ostrzał. Niedługo po zdarzeniu swój raport na temat katastrofy opublikowano na stronie należącej do Flightradar 24<sup>3</sup>, jednego z kilku najważniejszych portali gromadzących i wizualizujących informację o przebiegu lotów. Raport, a w szczególności jedno zdjęcie zrobiło ogromne wrażenie, uświadamiając czytelnikom grozę ostatnich minut lotu.



Rys. 1. Wizualizacja ostatnich minut lotu samolotu Embraer E190AR 4K-AZ65.

## W JAKI SPOSÓB SERWISY UZYSKUJĄ INFORMACJE O POŁOŻENIU I PRZEBIEGU LOTÓW SAMOLOTÓW?

Głównym źródłem informacji są dane emitowane przez transpondery systemu ADS-B (Automatic Dependent Surveillance-Broadcast). Działa on na zasadzie automatycznego nadawania przez samolot swojej lokalizacji i innych danych na częstotliwości radiowej, które mogą być odbierane przez stacje naziemne lub inne statki powietrzne. W skrócie,

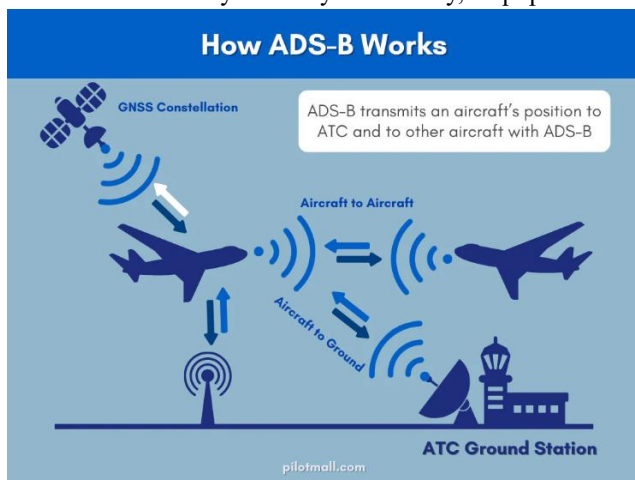
<sup>2</sup> <https://www.aa.com.tr/ru/мир/крушение-самолета-embraer-190-в-актау-версии-потерпевших-пассажиров-и-аналитиков/3434860>

<sup>3</sup> <https://www.flightradar24.com/blog/azerbaijan-airlines-e190-crashes-near-aktau/>

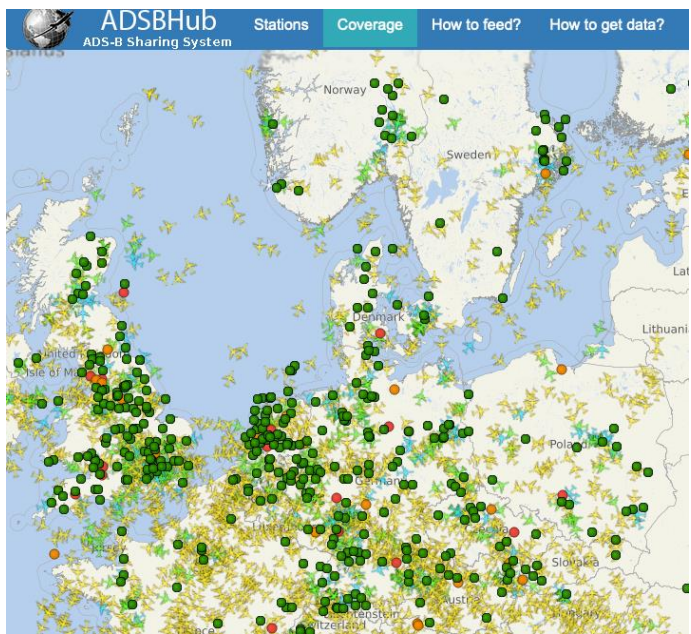
ADS-B jest zależny od systemów nawigacji satelitarnej (takich jak GPS) i używa tych informacji do określenia pozycji statku powietrznego.

### JAK DZIAŁA ADS-B?

1. Zbieranie danych o położeniu: Samolot wyposażony w transponder ADS-B otrzymuje informacje o swojej pozycji z systemu GNSS. Oprócz pozycji, ADS-B może również nadawać inne dane, takie jak prędkość, wysokość, kierunek lotu, identyfikator samolotu oraz inne informacje telemetryczne.
2. Transmisja sygnału: Co pewien czas, transponder samolotu nadaje te dane w postaci sygnału radiowego na częstotliwości 1090 MHz (ADS-B Out). W zależności od konfiguracji samolotu, może również odbierać sygnały innych samolotów (ADS-B In).
3. Odbiór sygnału: Stacje naziemne (na przykład w kontrolowanej przestrzeni powietrznej) lub inne samoloty wyposażone w odbiorniki ADS-B odbierają te sygnały. Informacje o położeniu i prędkości samolotu są następnie przekazywane do systemów monitorujących ruch lotniczy.
4. Przetwarzanie danych: Otrzymane dane są wykorzystywane przez służby kontroli ruchu lotniczego (ATC) do śledzenia samolotów, monitorowania ich położenia w czasie rzeczywistym, a także do zapewnienia odpowiedniej separacji między statkami powietrznymi. W przypadku odbioru przez inne samoloty, system pozwala na widoczność innych maszyn w okolicy, co poprawia bezpieczeństwo.



Rys. 2. Zasada działania systemu ADS-B. Źródło: [www.pilotmall.com](http://www.pilotmall.com).



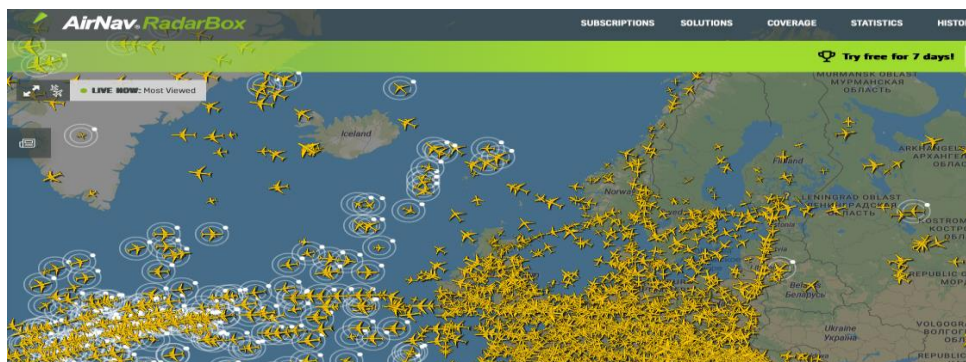
Rys. 3. Położenie naziemnych stacji odbiorczych systemu ADS-B w Europie.  
 Źródło ADSBhub<sup>4</sup>.

Dane systemu są ogólnie dostępne i np. Flightradar24 dystrybuje specjalne oprogramowanie do samodzielnego ich pobierania, w ten sposób hobbysta zainteresowany lotnictwem ma dostęp do danych lotów w rejonie jego zamieszkania i jednocześnie wzmacnia jakość serwisu.

Do precyzyjnego obliczania pozycji samolotów wykorzystywany jest także system MLAT (Multi-Lateration) który, oblicza dokładną pozycję statku powietrznego na podstawie czasu, w jakim sygnał dotarł do różnych odbiorników. Ten system jest szczególnie przydatny do monitorowania lotu samolotów nad oceanami. W serwisie RadarBox<sup>5</sup> samoloty znajdujące się poza zasięgiem lądowych stacji odbiorczych są oznaczane specjalnymi okręgami. W ten sposób użytkownik serwisu zostaje powiadomiony, że dane mogą być nie tak pełne, jak te zbierane za pośrednictwem stacji naziemnych.

<sup>4</sup> <https://www.adsbhub.org/>

<sup>5</sup> <https://www.radarbox.com/>



Rys. 4. Zrzut ekranu serwisu RadarBox

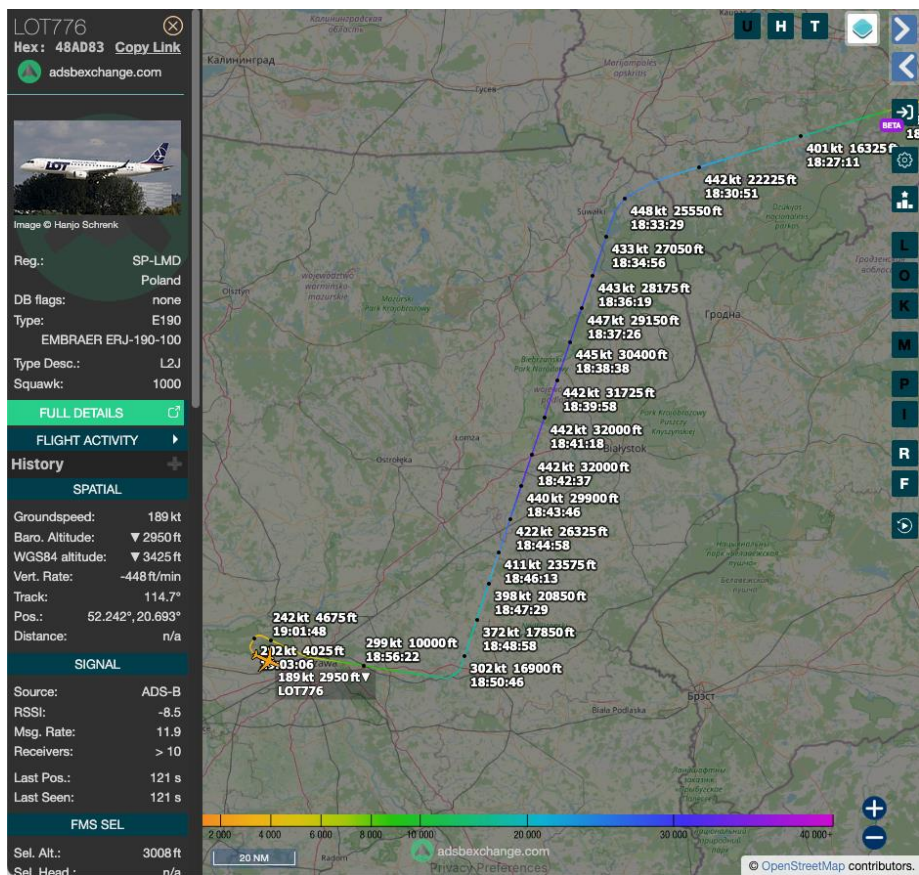
Dane prezentowane w serwisach FlightRadar24 i RadarBox są filtrowane i uzupełnione o dane MLAT. Osoby preferujące analizę surowych danych korzystają z serwisu ADSBExchange<sup>6</sup>, który nie filtruje żadnych danych. Jego wizualizacje są często mniej efektowne i trudniejsze w odbiorze, ale w zamian widzimy dane takimi, jak odebrały je stacje naziemne. Jest to szczególnie przydatne przy analizie zakłóceń lokalizacji, które omówione zostaną w dalszej części artykułu.

## WIZUALIZACJA LOTU

Popularne serwisy pokazują tor lotu samolotów rysując linię łączącą lotnisko startu z miejscem docelowym – dotyczy to oczywiście tych lotów, które mają te informacje określone i podane. Stąd też często na początku lotów, np. z Turcji do Rosji wizualizacja wskazuje na lot przez teren Ukrainy lub zamkniętych obszarów Rosji. Takie wizualizacje często są zgłaszane przez obserwujących i komentowane, np. na facebookowych grupach spoterskich. Te pierwotne hipotetyczne linie zwykle są dość szybko korygowane i otrzymujemy rzeczywistą trasę lotu.

---

<sup>6</sup> <https://www.adsbexchange.com>

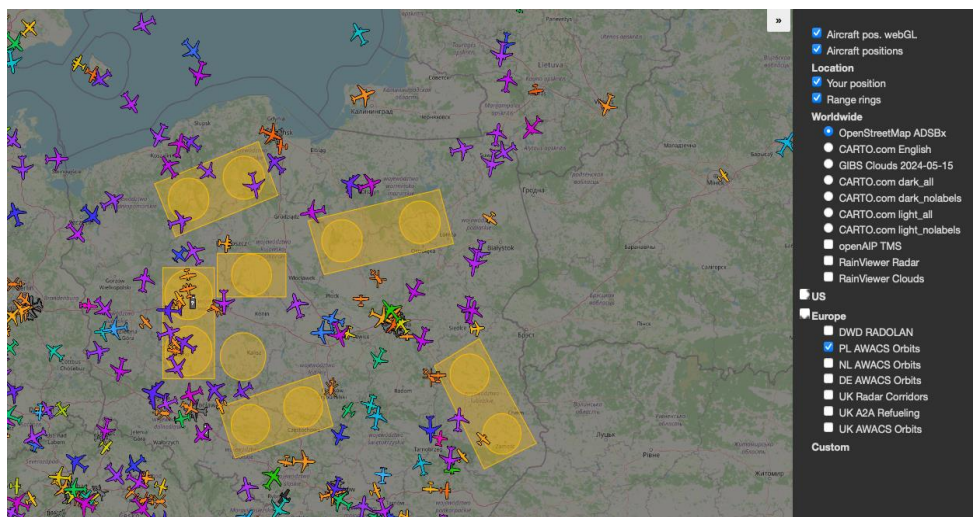


Rys. 5. Zapis lotu samolotu rejsowego PLL LOT według serwisu ADSBExchange

Z danych, które publikuje serwis ADSBExchange możemy odczytać dokładnie, w którym momencie transponder samolotu przekazał informacje o położeniu, prędkości i wysokości. Tak jak w większości serwisów trasa lotu podzielona jest na różnokolorowe odcinki. W ten sposób wyróżniony jest start, lot na wysokości podróźnej, przygotowanie do lądowania i samo lądowanie.

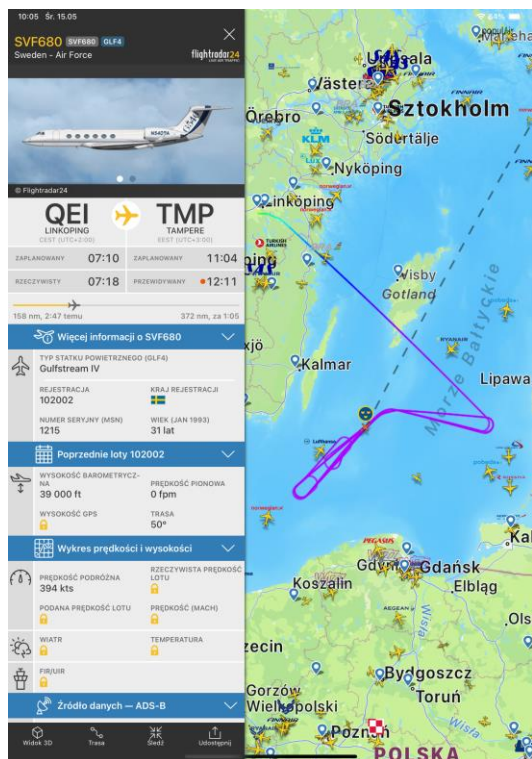
W związku ze wzrostem zainteresowania śledzenia aktywności lotnictwa wojskowego ADSBExchange przygotował także predefiniowane orbity aktywności samolotów. W przypadku Polski są to obszary, na których operują najczęściej samoloty wczesnego ostrzegania typu AWACS<sup>7</sup>

<sup>7</sup> <https://www.polska-zbrojna.pl/home/articleshow/41759?t=Wszystkie-misje-AWACS-a>



Rys. 6. Zrzut ekranu serwisu ADSBExchange z zaznaczonymi orbitami Awacs

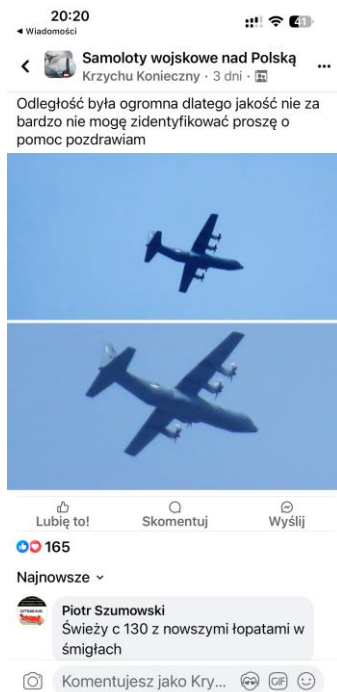
W podobny, choć pozbawiony szczegółów danych chwilowych, sposób prezentowane są loty w serwisie FlightRadar24. Tutaj także łatwo odróżnimy poszczególne fazy lotu, gdyż oznaczono je różnymi kolorami. Na poniższym rysunku (Rys. 7) widzimy zapis przykładowej misji samolotu wywiadu sygnałowego S102B Korpen SIGINT szwedzkich sił zbrojnych. Wizualizacja pozwala nam ustalić w jakim obszarze operował samolot. Widzimy, że przez dłuższy czas znajdował się na jednakowym pułapie. Samolot odbył lot na trasie z Linköping w Szwecji do Tampere w Finlandii. Część jego lotu jest jednakże niedostępna, ponieważ pilot zdecydował o wyłączeniu transpondera. Stąd część zapisu jest hipotetyczną linią przerywaną.



Rys. 7. Zrzut z serwisu FlightRadar24

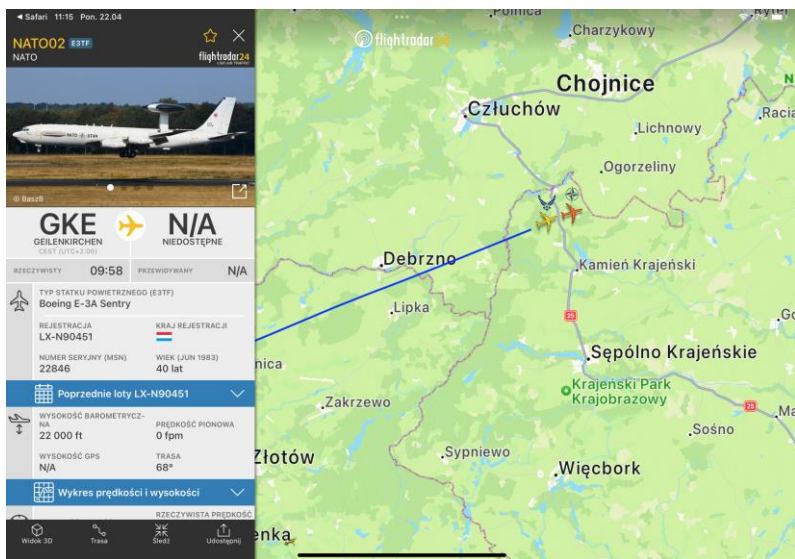
## CZEGO NIE WIDZIMY W SERWISACH?

Przeglądając grupy spoterskie w mediach społecznościowych często przewija się pytanie, dlaczego nie widzimy lotów wojskowych. Wydaje się to oczywiste, że samoloty wojskowe lub inne wykonujące zadania wymagające dyskrecji latają z wyłączonymi transponderami, a nadzór nad ich lotem odbywa się kanałami służbowymi. Wiele osób śledzi loty samolotów nad Polską – tylko jedna prywatna grupa w serwisie Facebook „Samoloty wojskowe nad Polską” ma ponad 86 tysięcy członków. Publikowane są tutaj zdjęcia zarówno z oficjalnych imprez lotniczych, jak i zaobserwowane przelatujące samoloty.



Rys. 8. Zrzut z grupy „samoloty wojskowe nad Polską”

Jednym z pojawiających się motywów są zdjęcia tankujących samolotów – myśliwców lub AWACS-ów. Jak już wiemy, samoloty AWACS operują na pewnych ustalonych orbitach, a krążące samoloty cysterny zwykle działają z włączonymi transponderami. Operacja tankowania także odbywa się zazwyczaj z włączonym transponderem AWACS-a. Jest więc chwilowo widoczna, np. w serwisie Flightradar 24, co możemy zobaczyć na zrzucie ekranowym poniżej (Rys. 9).



Rys. 9. Tankowanie w powietrzu

Wojskowe samoloty bez włączonego transpondera operujące wewnątrz kraju są oczywiście monitorowane za pośrednictwem innych, właściwych systemów. Przeloty w przestrzeni międzynarodowej wymagają identyfikacji. Jednym ze źródeł informujących o naruszeniach międzynarodowych kanałów komunikacyjnych na Bałtykiem przez samoloty wojskowe Federacji Rosyjskiej jest oficjalne konto niemieckich sił zbrojnych o nazwie „Team Luftwaffe”<sup>8</sup>. Publikacje na portalu X i w Instagramie zawierają zwykle podstawowe informacje o przechwyceniach rosyjskich samolotów lecących bez identyfikacji i planu lotu. Z opisu modelu i modyfikacji przechwyconego samolotu możemy wnioskować o charakterze misji.

<sup>8</sup> [https://x.com/team\\_luftwaffe](https://x.com/team_luftwaffe)

**Team Luftwaffe** @Tea... · 5 dni ...  
24/7 ist unsere QRA in  Lielvarde in Alarmbreitschaft! Erneut sind unsere  #Eurofigther von VAPB zu einem Alpha Scamble aufgestiegen und identifizierten eine  AN-30 CLANK ohne Flugplan und Transpondersignal.  
[#WeAreNato](#) [#StrongerTogether](#)



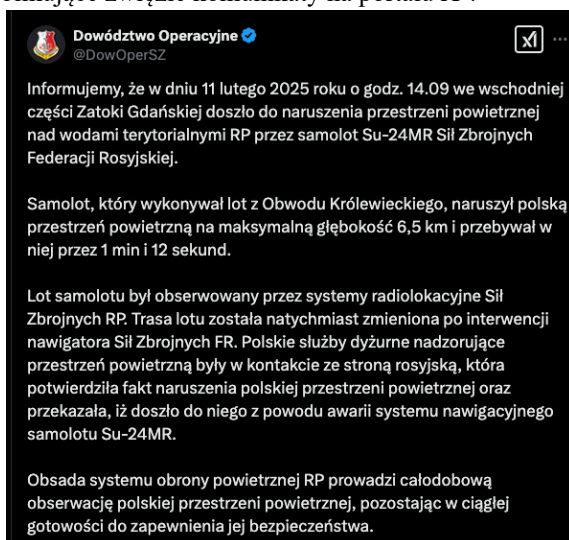
**Team Luftwaffe** @Tea... · 4 dni ...  
Das zweite mal heute das unsere  #Eurofigther zum Alpha Scramble aufsteigen! Dabei sind wir auf zwei  Luftfahrzeuge getroffen eine TU-214 und eine Il-78 MIDAS die ohne Flugplan und Transpondersignal identifiziert und begleitet wurden.  
[#strongerTogether](#) [#WeAreNATO](#)



Rys. 10. Zrzuty z konta Team Luftwaffe na portalu X

Wymieniony AN 30 z oznaczeniem NATO Clank to wywiadowcza i rozpoznawcza wersja samolotu AN 24. Z kolei IŁ 78 MIDAS to samolot cysterna przeznaczony do tankowania w powietrzu.

Doskonałym źródłem informacji jest także konto Dowództwa Operacyjnego Sił Zbrojnych RP publikujące związane komunikaty na portalu X<sup>9</sup>.



**Dowództwo Operacyjne** @DowOperSZ

Informujemy, że w dniu 11 lutego 2025 roku o godz. 14.09 we wschodniej części Zatoki Gdańskiej doszło do naruszenia przestrzeni powietrznej nad wodami terytorialnymi RP przez samolot Su-24MR Sił Zbrojnych Federacji Rosyjskiej.

Samolot, który wykonywał lot z Obwodu Królewieckiego, naruszył polską przestrzeń powietrzną na maksymalną głębokość 6,5 km i przebywał w niej przez 1 min i 12 sekund.

Lot samolotu był obserwowany przez systemy radiolokacyjne Sił Zbrojnych RP. Trasa lotu została natychmiast zmieniona po interwencji nawigatora Sił Zbrojnych FR. Polskie służby dyżurne nadzorujące przestrzeń powietrzną były w kontakcie ze stroną rosyjską, która potwierdziła fakt naruszenia polskiej przestrzeni powietrznej oraz przekazała, iż doszło do niego z powodu awarii systemu nawigacyjnego samolotu Su-24MR.

Obsada systemu obrony powietrznej RP prowadzi całodobową obserwację polskiej przestrzeni powietrznej, pozostając w ciągłej gotowości do zapewnienia jej bezpieczeństwa.

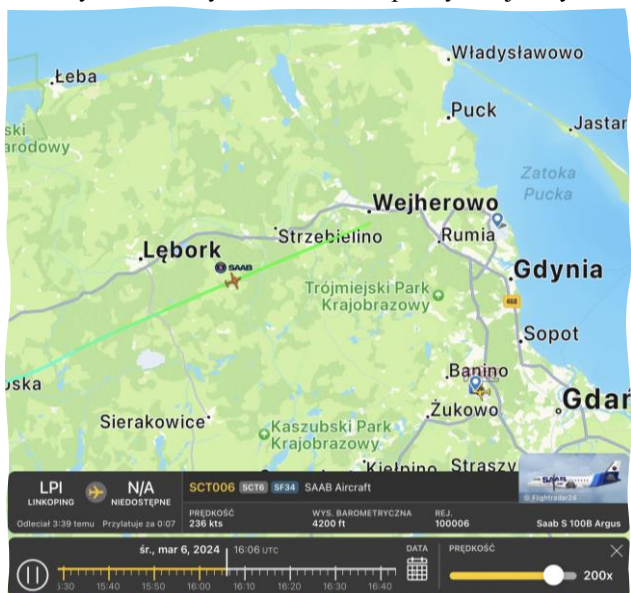
Rys. 11. Komunikat o incydencie naruszenia przestrzeni powietrznej RP.

<sup>9</sup> <https://x.com/DowOperSZ>

Także i w tym przypadku możemy próbować postawić wstępne hipotezy co do charakteru lotu wykonywanego przez rosyjski samolot. Su-24MR jest bowiem wariantem samolotu dostosowanym specjalnie do zadań wywiadowczych. Samolot jest wykorzystywany do rozpoznania fotograficznego, radarowego oraz elektronicznego. Jest to samolot przeznaczony do pozyskiwania informacji wywiadowczych i monitoringowych na dużych obszarach.

## INFORMACJA I DEZINFORMACJA

Wymienione powyżej przykłady komunikatów o aktywności samolotów pokazują dobre praktyki informowania o aktywności lotniczej. Innym przykładem jest sprawa z latającym w polskich barwach samolotem wczesnego wykrywania i ostrzegania SAAB 340 AEW. Jego pojawienie się w serwisach wzbudziło ogromne zainteresowanie i spekulacje na temat miejsca bazowania. Samolot lecąc z Linkoping nie podawał lotniska docelowego, a w okolicach Wejherowa wyłączył transponder. W takiej sytuacji samolot „znika” z serwisów i system nie wyznacza nawet hipotetycznej trasy.



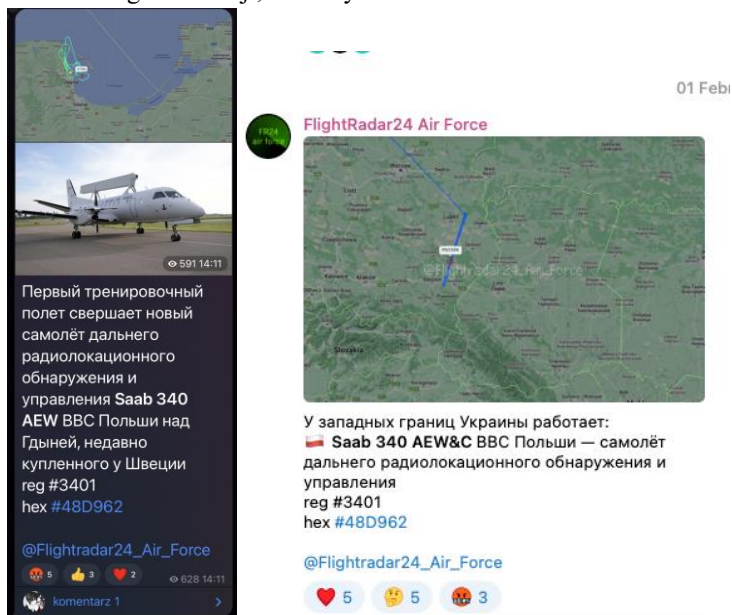
Rys. 12. Zapis lotu samolotu SAAB 340 AEW

Publikacja zdjęć na portalu X przez Sekretarza Stanu w Ministerstwie Obrony Narodowej Pawła Bejdę potwierdziła fakt przyjęcia przez Polskę tego samolotu ucinając spekulacje.



Rys. 13. Prezentacja samolotu SAAB 340 AEW

Od tego momentu był to jeden z częściej wypatrywanych i śledzonych samolotów. Praktycznie każdy ujawniony lot samolotu był odnotowany, np. przez telegramowy kanał FlightRadar 24 Air Force<sup>10</sup>. Nazwa tego kanału jest zbieżna z opisywanym serwisem, ale zbieżność jest myląca. Kanał zajmuje się „monitoringiem aktywności wojennego lotnictwa u granic Rosji, Ukrainy i Białorusi”.



Rys. 14. Informacja o pierwszym treningowym locie samolotu SAAB 340 AEW i działania samolotu przy granicy z Ukrainą.

<sup>10</sup> [https://t.me/Flightradar24\\_Air\\_Force](https://t.me/Flightradar24_Air_Force)

Kanał FlightRadar 24 Air Force praktycznie całodobowo publikuje informacje o aktywności samolotów identyfikowanych jako wywiadowcze nad terytorium Polski, krajów Bałtyckich i Bliskiego Wschodu.

Szczególnym punktem zainteresowania jest monitoring samolotów transportowych lądujących na lotnisku w Rzeszowie. Każdego miesiąca publikowane jest zestawienie wskazujące z jakich krajów wykonano loty.

Kanał nie jest bardzo popularny, ale publikacje z hashtagem Rzeszów powielane są na dziesiątkach kanałów wspierających wojnę przeciw Ukrainie. W ten sposób informacja dociera do szerokiego kręgu odbiorców.

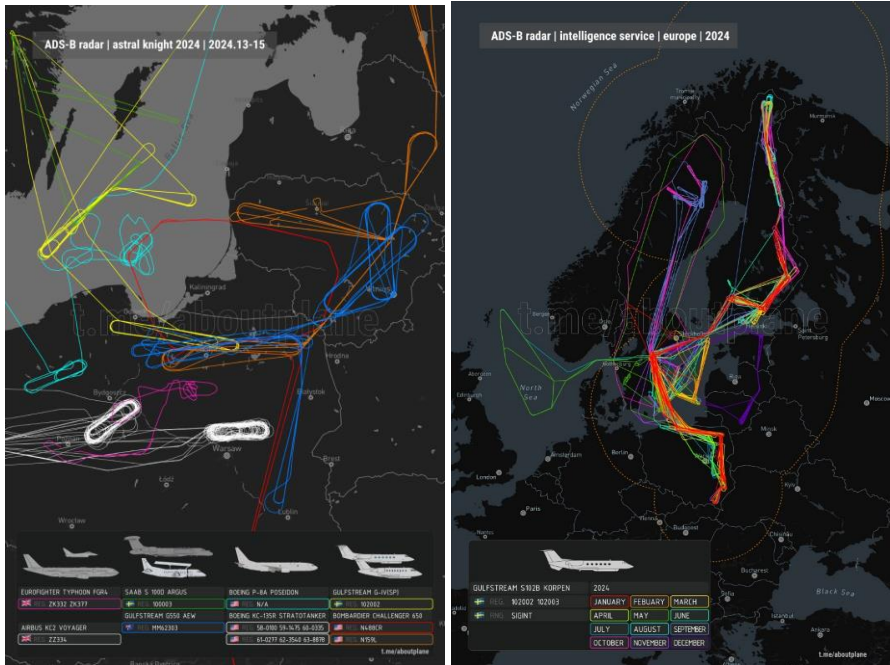


Rys. 15. Podsumowanie lotów transportowych na lotnisko w Rzeszowie w styczniu 2025 roku.

Jak widać z powyższego rysunku (Rys.15) statystyka lotów została wykonana wspólnie z kanałem Aboutplane<sup>11</sup>. Top kolejny niszowy kanał rosyjski specjalizujący się w analizowaniu aktywności samolotów wywiadowczych. Ich głównym produktem są publikowane co miesiąc statystyki i mapy aktywności głównie samolotów NATO.

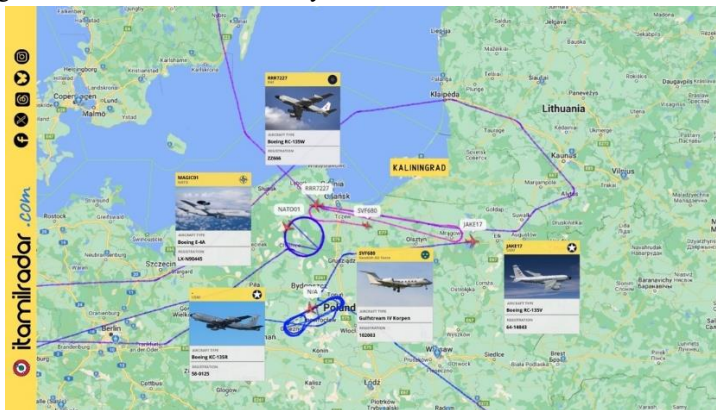
Najczęściej jest ono publikowane w osobnych mapach dotyczących Bałtyku i Okręgu Królewieckiego, Finlandii, basenu Morza Czarnego i Bliskiego Wschodu. Najczęściej oprócz tras lotu mapy zawierają podstawowe dane o samolocie i jego zadaniach.

<sup>11</sup> <https://tgstat.ru/channel/@aboutplane>



Rys. 16. Mapy aktywności samolotów wywiadowczych NATO.

Jednym z najciekawszych zachodnich źródeł monitoringu aktywności wojskowej jest strona ItaMilRadar<sup>12</sup>. Serwis istniejący od 2106 roku, pierwotnie skupiał się na działaniach na Morzu Śródziemnym. Dzisiaj działa w zasadzie globalnie i monitoruje lotnictwo NATO, Włoch, Grecji, Francji, Turcji, Rosji i USA. Chyba jako jedyny łączy monitoring lotnictwa z działaniami floty.



Rys. 17. Zestawienie aktywności nad Polską i wokół Okręgu Królewieckiego w dniu 27 listopada 2024.

<sup>12</sup> <https://www.itamilaradar.com>

Przykładem dezinformacji z wykorzystaniem danych o lotach może być sprawa rzekomej ucieczki z Izraela premiera tego kraju, tuż przed oczekiwanym atakiem odwetowym Iranu w kwietniu 2024 roku.

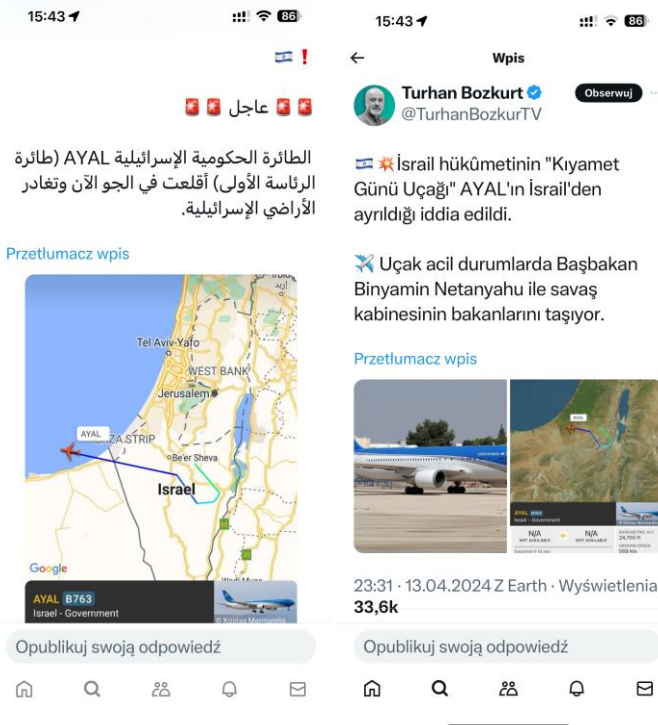


Rys. 18. Zapis lotu samolotu AYLAL 4X-ISR

Obserwatorzy serwisu FlightRadar zauważyli start z nieoznaczonego miejsca w Izraelu samolotu AYLAL 4X-ISR o nazwie „Skrzydła Syjonu” wykorzystywanego jako oficjalny samolot najwyższych władz Izraela i jednocześnie stanowisko dowodzenia, tzw. „Doomsday Plane”. Samolot był zwykle przechowywany w bazie Nevatim na pustyni Negev, w południowym Izraelu. Miejsce startu mogło wskazywać na zakłócenie systemu GNSS. Według mapy samolot przekroczył granicę egipską i nad Morzem Śródziemnym wyłączył transponder. Jeden tweet osoby zajmującej się analizą danych otwartych zawierający sugestię, że istnieje możliwość, iż Benjamin Netanyahu opuścił Izrael wystarczył, aby plotka rozeszła się na Bliskim Wschodzie, Turcji i Rosji.



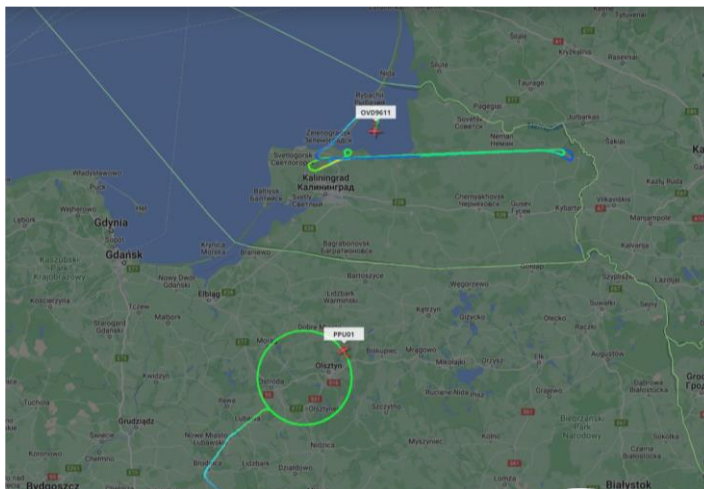
Rys. 19. Wiadomość sugerująca wylot premiera Izraela z kraju.



Rys. 20. Powielone przez arabskie i tureckie konta informacje o ucieczce premiera.

W tym wypadku sugestia rzucona przez analityka została podchwycona przez kanały propagandowe i rozeszła się niemalże jako potwierdzona informacja.

W przypadku analizy danych lotniczych, podobnie jak w ocenie innych rodzajów informacji, ważne jest, aby brać pod uwagę zarówno kontekst i potwierdzenie samej informacji.



Rys. 21. Aktywność samolotów inspekcji lotniczej.

Wiosną 2024 roku osoby monitorujące loty samolotów nad Polską i Okręgiem Królewieckim zaczęły wymieniać się informacjami o dziwnej (ich zdaniem) bo wykonywanej takim samym modelem samolotu Beechcraft King Air 350i aktywności po obu stronach granicy. Polski samolot PPU01<sup>13</sup> należy do Polskiej Agencji Żeglugi Powietrznej i pełni służbę kontrolno-pomiarową realizowaną przez inspekcję lotniczą PAŻP. Samolot OVD9611 należy do rosyjskiego odpowiednika Agencji i wykonuje zapewne podobne zadania. Oba samoloty zostały przygotowane do zadań w tej samej niemieckiej firmie<sup>14</sup>. Rosyjski samolot każdym swoim pojawieniem wywołuje w Rosji zainteresowanie, w Okręgu Królewieckim był nie pierwszy raz<sup>15</sup>. Prawdopodobnie przypadkowe wykonywanie czynności w tym samym czasie co w Polsce wywołało podejrzenia i komentarze.

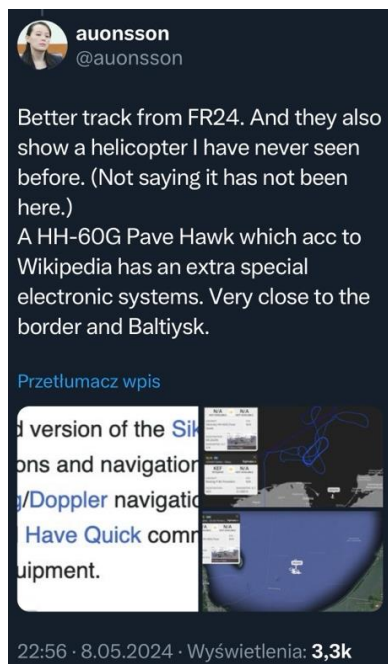
Podobne komentarze i fale zainteresowań wywołują pojawienia się nad Bałtykiem wcześniej niezauważonych wersji samolotów lub śmigłowców. W maju 2024 roku osoba publikująca w serwisie X pod pseudonimem „Auonsson”<sup>16</sup> poinformowała o zauważeniu blisko Mierzei Wiślanej helikoptera Armii USA w nietypowej wersji Sikorsky HH – 60G Pave Hawk.

<sup>13</sup> <https://www.pansa.pl/inspekcja/beechnraft-king-air-350/>

<sup>14</sup> <https://www.aerodata.de/en/>

<sup>15</sup> <https://makanom.livejournal.com/530582.html?>

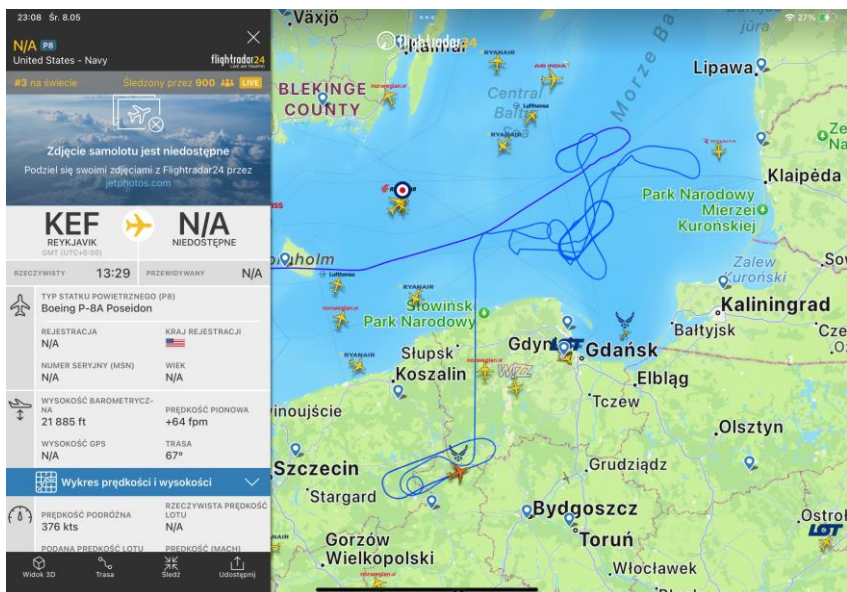
<sup>16</sup> <https://x.com/auonsson>



Rys. 22. Post na portalu X

Aunonsson jest osobą anonimową, a jej aktywność w mediach społecznościowych w całości dotyczy bezpieczeństwa lotów i żeglugi na Bałtyku.

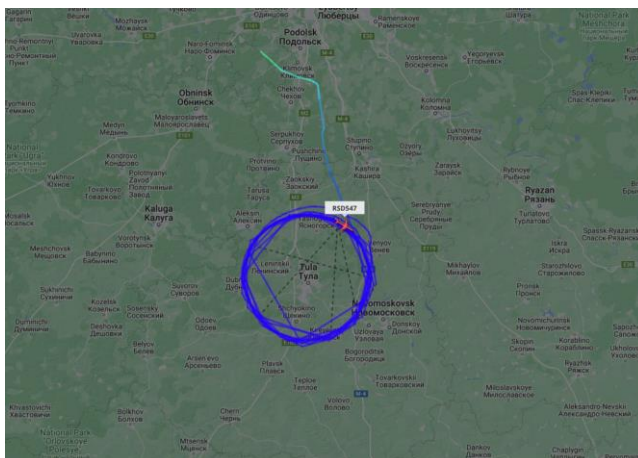
Helikopter Pave Hawk jest wykorzystywany do działań w trudnych warunkach, ale raczej ratunkowych, niż bojowych. Co ciekawe w tym samym czasie na Bałtyku służbę pełnił samolot Boeing P8A Poseidon przeznaczony do walki z okrętami podwodnymi. Samolot ten często pełni służbę nad Bałtykiem i nie wywołuje szczególnego zainteresowania.



Rys. 23. Aktywność samolotu Boeing P-8A Poseidon i helikoptera Sikorsky HH – 60G Pave Hawk.

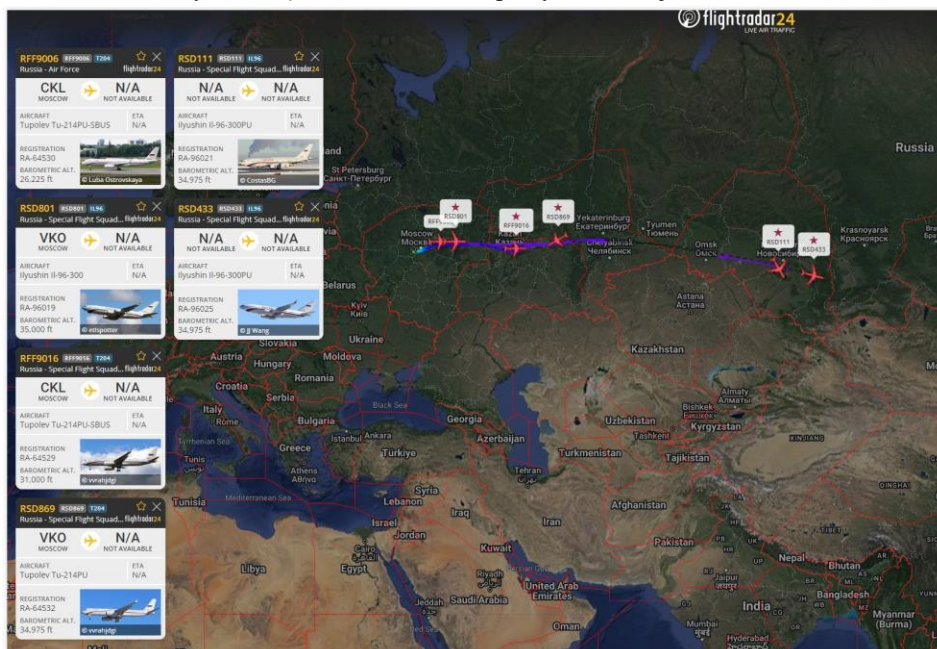
Dopiero szczegółowa analiza analogicznego serwisu pokazującego położenie statków wskazała możliwą interwencję związaną z jachtem pływającym pod niemiecką banderą. Oczywiście nie ma żadnego potwierdzenia takiej wersji, możliwe, że były to tylko rutynowe szkolenia lub inne czynności. Nie jest zadaniem tego artykułu dociekać, co wydarzyło się tego konkretnego dnia, ale ten przypadek pokazuje, jak monitorowane są aktywności w powietrzu i na morzu i jak prowokują do hipotez.

Jedną z częstszych podpowiedzi rosyjskiej wersji Google, po wpisaniu numeru samolotu, jest stwierdzenie „kto nim lata”. Rzeczywiście analitycy zajmujący się samolotami wykorzystywanymi w rosyjskiej administracji potrafią przypisać konkretne egzemplarze samolotów do ministerstw i osób. Większość widocznej w serwisach rosyjskiej floty lata w barwach specjalnej eskadry „Rosja”. Te samoloty należą do najczęściej obserwowanych w serwisach, a każda ich nietypowa aktywność oczywiście wzbudza komentarze.



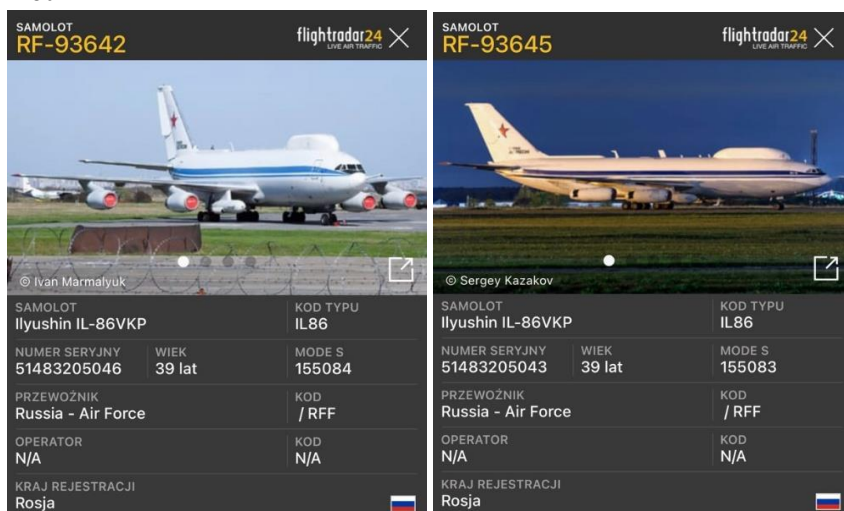
Rys. 24. Samolot Tupolew 214SR o numerze RA64527 krążący nad Tułą

Tak było też w przypadku samolotu Tupolew 214SR o numerze RA64527 krążącego nad Tułą. Wyjaśnienie okazało się bardzo łatwe – rosyjskie samoloty zwykle w nazwie zawierają informacje o swojej specjalności. W tym wypadku SR to „samolot retranslator”, czyli maszyna przeznaczona do zabezpieczenia specjalnej łączności. W tym samym czasie w Tule odbywało się forum z udziałem prezydenta Rosji.



Rys. 25. Samoloty eskadry „Rosja” w drodze do Chin w związku z wizytą W. Putina w Pekinie.

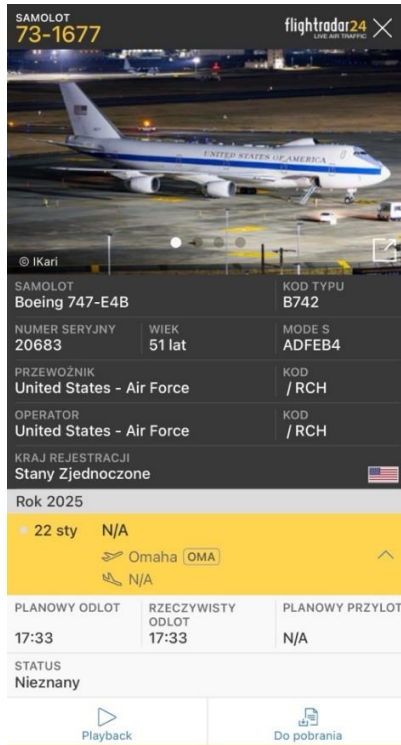
Obserwując samoloty delegacji rosyjskiej kierujące się z oficjalną wizytą do Pekinu można było postawić hipotezy co do składu delegacji i charakteru wizyty. Większość samolotów delegacji była w wersji PU, czyli „punkt dowodzenia”. Dodatkowo dwa samoloty były w wersji rozbudowanej SBUS, czyli „baza użytkownika strategicznego”<sup>17</sup>. Każdy z modeli samolotów jest zdublowany zapewne na wypadek awarii. Samoloty będące punktem dowodzenia strategicznego mają zapewnić możliwość kierowania państwem, także z powietrza. Tego typu samoloty nazywane są „doomsday planes”, czyli samolotami „czasów ostatecznych”. Są one przygotowane do gwarantowania ciągłości dowodzenia z powietrza przez wiele dni (oczywiście przy możliwości dotankowywania). Każdy lot tego typu samolotów wywołuje zainteresowanie. Po stronie rosyjskiej innym przykładem takiego samolotu jest Il 86 WKP (z rosyjskiego "ВКП" – "Воздушный командный пункт"), latający punkt dowodzenia. W 2022 roku pojawiły się informacje o planowanej zmianie prawie 40 letnich Il 86 i wprowadzenie na ich miejsce samolotów Il 80WKP.



Rys. 26. Rosyjskie latające punkty dowodzenia

W sieci brak jest informacji o lotach samolotów w wersji WKP po roku 2015. Prawdopodobnie ich starty odbywają się przy wyłączonych transponderach. W przeciwieństwie do rosyjskich, ich amerykańskie odpowiedniki Boeing 747 E4A trenują zwykle w sposób jawny, a ślady ich tras lotu można obserwować w serwisach.

<sup>17</sup> <https://www.konflikty.pl/aktualnosci/wiadomosci/drugi-214pu-sbus/>



Rys. 27. Samolot Boeing 747 E4A

Spory rezonans wywołało, pojawienie się w jednym momencie dwóch samolotów tego typu<sup>18</sup>. Oczywiście jest, że załogi samolotów muszą ćwiczyć w powietrzu, ale w dzisiejszych niespokojnych czasach każda aktywność jest zarówno monitorowana, jak i komentowana.



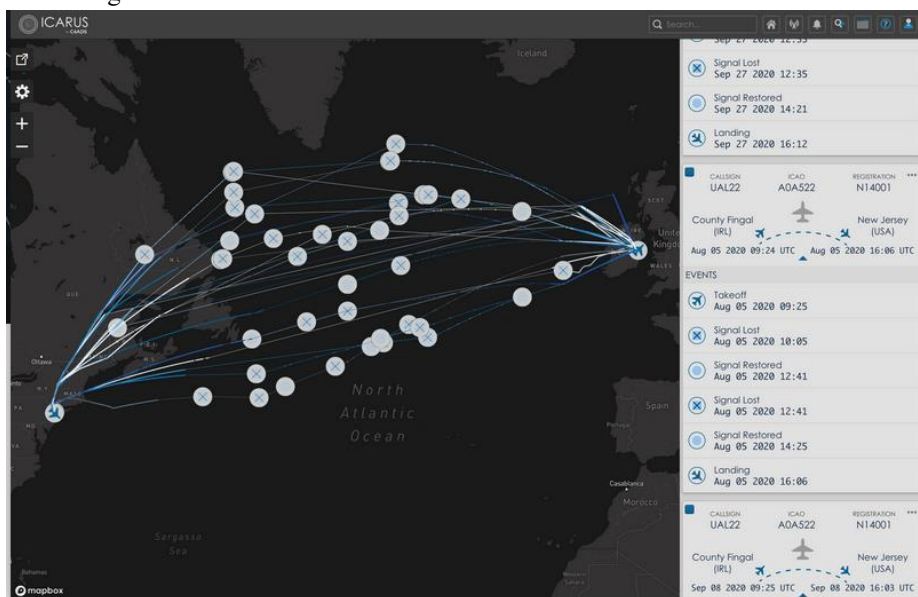
Rys. 27. Aktywność dwóch samolotów Boeing 747 E4A nad terytorium USA

<sup>18</sup> <https://khoradio.com/doomsday-planes-flying-over-missouri/>

## WYKORZYSTANIE DANYCH NA TEMAT LOTÓW

Oprócz wcześniej wymienionych serwisów, które gwarantują ograniczony czasowo dostęp do danych (w zależności od opłacanego abonamentu), istnieje organizacja **OpenSky Network**<sup>19</sup> zajmująca się zbieraniem, przechowywaniem oraz udostępnianiem danych związanych z ruchem lotniczym. Działa jako otwarty system, który gromadzi informacje o lotach samolotów, wykorzystując technologię ADS-B (Automatic Dependent Surveillance-Broadcast). Celem OpenSky Network jest udostępnienie danych o ruchu lotniczym społeczności naukowej, badawczej oraz szerokiego gronu użytkowników, takich jak deweloperzy, organizacje monitorujące bezpieczeństwo, a także pasjonaci lotnictwa.

Dane pobrane z **OpenSky Network** są wykorzystywane chociażby w śledztwach dziennikarskich. Innym narzędziem analitycznym jest rozwijane przez **Global Investigative Journalism**<sup>20</sup> i **C4ADS** (Center for Advanced Defense Studies)<sup>21</sup> narzędzie **Icarus Flights**<sup>22</sup>



Rys. 28. Icarus Flight, zrzut ze strony produktu

Ciekawym przykładem analizy lotów konkretnego samolotu jest historia rosyjskiego Il62M o numerze RA 86559, który został zauważony na zdjęciach satelitarnych wykonanych w sierpniu 2023 roku w Pjongjangu. Samolot był przypisywany jako pozostający w dyspozycji ministra obrony narodowej Rosji. Od tamtego momentu jest jedną z częściej obserwowanych maszyn. Jego loty poprzedziły

<sup>19</sup> <https://opensky-network.org/>

<sup>20</sup> <https://gijn.org/>

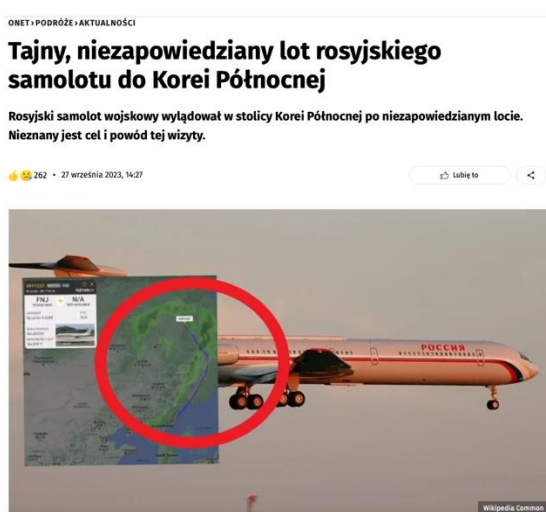
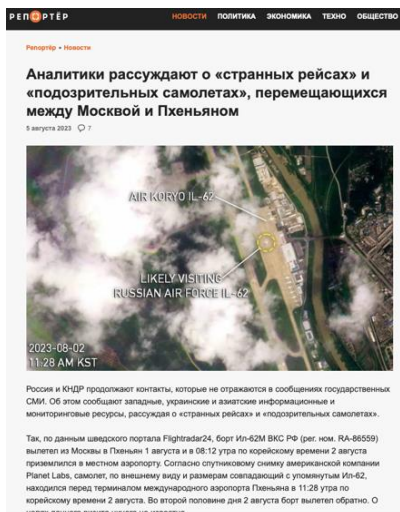
<sup>21</sup> Przykład śledztwa na temat lotów samolotów związanych z autorytarnym prezydentem Gwinei Równikowej

<sup>22</sup> <https://icarus.flights/>

wizytę ówczesnego ministra Szojgu w Korei Północnej, która z kolei skutkowałą pomocą militarną tego państwa<sup>23</sup>.

Rys. 28. Doniesienia prasowe na temat lotów IŁ 62M RA 86559

Samolot ma w sieci dobrze udokumentowaną historię, wiemy, że w przeszłości był



samolotem prezydenckim wykorzystywanym chociażby do wizyty w Finlandii.



Rys. 29. IŁ 62M RA 86559 w 2005 roku jako samolot prezydencki

<sup>23</sup> <https://www.polityka.pl/tygodnikpolityka/swiat/2221664,1,szojgu-w-korei-pln-witany-jak-gwiazda-rocka-rosja-sklad-a-oferte-na-co-liczy-w-zamian.read>




Ponownie zwrócono uwagę na ten samolot w styczniu 2024 roku za pośrednictwem posta na portalu X opublikowanego przez anonimowego „obserwatora militarnej aktywności” o pseudonimie MenchOsint<sup>24</sup>. Poniższy wpis (Rys. 30) miał wskazywać, że rosyjskie ministerstwo obrony prowadzi aktywną politykę w Afryce i przejmuje dawne kontrakty i strefy wpływów Grupy Wagnera. Z racji powiązania samolotu z osobistym wykorzystaniem przez ministra wskazywano na wizytę na wysokim szczeblu.





Rys. 30. Zrzut ekranu z portalu X


Samolot IŁ 62M RA 86559 jest nadal aktywny, jego podróże związane są z obszarami zainteresowania i interesów militarnych Rosji. Ostatnia aktywność to loty do Damaszku w Syrii, w związku z negocjacjami z nowym rządem syryjskim, wyłonionym po upadku reżimu Assada.


<sup>24</sup> <https://x.com/menchosint>

11:48   



SAMOLOT **RA-86559** flightradar24  LIVE AIR TRAFFIC






© Huangyijiang 



SAMOLOT Ilyushin Il-62M		KOD TYPU IL62
NUMER SERYJNY 2153258	WIEK 32 lata	MODE S 15521F
PRZEWOŹNIK Russia - Air Force		KOD / RFF
OPERATOR Russia - Air Force		KOD / RFF
KRAJ REJESTRACJI Rosja 		

Rok 2025

- 28 sty **RFF8910** RFF8910
  -  Damascus **DAM**
  -  Moscow **CKL**

PLANOWY ODLOT 18:55	RZECZYWISTY ODLOT 18:55	PLANOWY PRZYLOT 23:20
STATUS Wylądował 23:20		CZAS LOTU 04:26

 Playback    
  **RFF8910** Dane lotu    
  Do pobrania

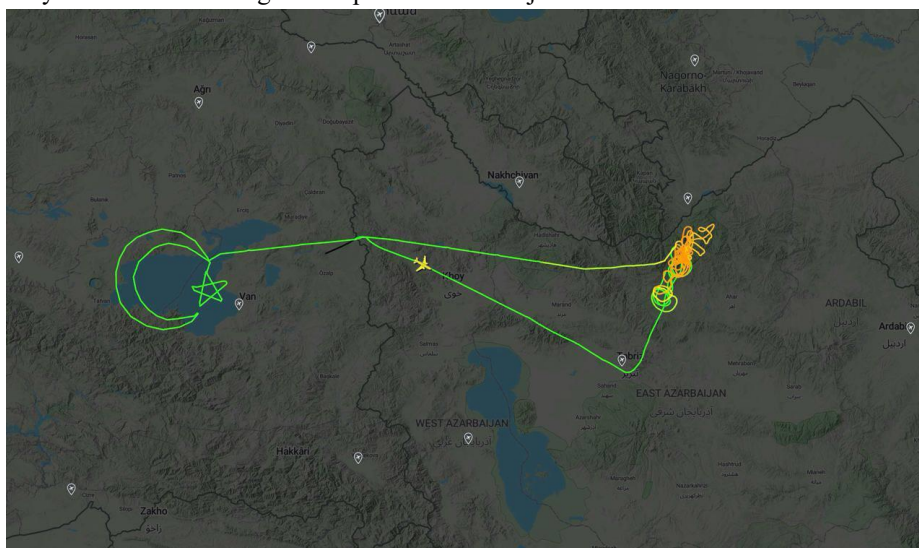
- 28 sty **RFF8909** RFF8909
  -  N/A
  -  N/A

Rys. 31. Zapis lotu IŁ 62M RA 86559 do Damaszku

Jaskrawym przykładem wykorzystania danych lotniczych jest sprawa poszukiwania szczątków helikoptera prezydenta Iranu który rozbił się w górzystym, niedostępnym terenie w dniu 19 maja 2024 roku<sup>25</sup>. Służby irańskie pomimo zaangażowania dużych sił i środków bezskutecznie przeszukiwały rejon prawdopodobnego upadku. Działając pod

<sup>25</sup> <https://www.pap.pl/aktualnosci/katastrofa-smiglowca-z-prezydentem-iranu-ebrahim-raisi-nie-zyje-wideo>

presją przyjęto ofertę wykorzystania w akcji poszukiwawczej tureckiego drona Bayraktar, o nazwie własnej Akinci. Maszyna sterowana zdalnie z Turcji sprawdziła rejon przeszukiwany przez służby naziemne, następnie przemieściła się na północ w niezbadany rejon, obniżyła lot i mimo fatalnych warunków pogodowych ujawniono szczątki helikoptera. Akcja poszukiwawcza była śledzona w sieci przez miliony użytkowników – na samym portalu FlightRadar 24 było ich prawie 3 miliony<sup>26</sup>. Strona turecka niezwłocznie przekazała lokalizację miejsca, irańskie służby ruszyły na pomoc, a operator drona prowadził je w kierunku granicy. Akcja okazała się gigantycznym sukcesem, tak dużym, że operator drona kierował nim w taki sposób, że ślad zapisał się w systemie w kształcie godła Republiki Tureckiej.



Rys. 32. Zapis akcji poszukiwawczej prowadzonej przez dron Bayraktar Akinci

Odpowiedź oficjalnej propagandy Iranu była natychmiastowa i całkowicie zaprzeczająca, aby Bayraktar przyczynił się jakkolwiek sposobem w odnalezieniu szczątków helikoptera. Stanowisko to powtórzył chociażby publikujący w języku rosyjskim dziennikarz propagandowy Haijal Muazzin<sup>27</sup>.

<sup>26</sup> <https://www.flightradar24.com/blog/turkish-akinci-iran/>

<sup>27</sup> <https://www.xayalmuazzin.com/>


🇮🇷 Дневник иранского журналиста
👁️ 12,6K edytowano 09:32

”
🇮🇷 🇹🇷 Дневник иранского журналиста
➡️

”
Минобороны Турции: Для поиска вертолета президента Ирана и



”
🇹🇷 🇮🇷 В прошлую ночь турецкий беспилотник «Akinci», который был направлен на помощь Ирану, не смог обнаружить никаких результатов в поисках и вернулся.

/#Иран #Турция/

✔️ @khayalpressa313

Rys. 33. Informacja o rzekomym fiasku misji poszukiwawczej Akinci

W odpowiedzi władze tureckie opublikowały na oficjalnych kanałach pełny zapis misji. Oczywiście wydaje się fakt, że publikacja w języku rosyjskim i perskim miała ułatwić dotarcie do odbiorców w obu krajach i przeciwdziałać oficjalnej propagandzie.

✂️ 7 часов и 27-минутный поиск турецким БПЛА AKINCI упавшего вертолёта президента Ирана Раиси

”
20:00: Иранское министерство иностранных дел запрашивает вертолёт для поисково-спасательной операции с ночным видением у Министерства национальной обороны (МНО) Турции. МНО предлагает deployment of Bayraktar AKINCI БПЛА в качестве стратегического класса, а также вертолёт.

20:20: Иранские чиновники принимают предложение, и МНО даёт указание Генеральному штабу готовиться.

22:30: МНО издаёт приказ о пересечении границы для вооружённого БПЛА AKINCI A6, который уже находился в воздухе.

23:00: Пересечение границы отменяется, так как иранские власти не одобрили вооружённый Bayraktar AKINCI.

23:18: Безоружный БПЛА AKINCI A5 взлетает из Бэгмена.

00:13: БПЛА пересекает границу из региона Ван.

”
00:45: AKINCI A5 прибывает в зону поиска и ведёт полёт на высоте 30 000 футов.

02:22: Непогода и трудности с получением съёмки с большой высоты приводят к тому, что БПЛА постепенно снижается до 9000 футов, где обнаруживается первый источник тепла.

02:37: Кадры с Bayraktar Akinci передаются иранским властям.

04:30: Иранские спасатели прибывают в район поисков.

05:46: Спасатели обнаруживают обломки вертолёта.

05:50: Иранские чиновники благодарят Министерство обороны и просят вывести БПЛА, так как в район заходят другие воздушные суда.

06:01: AKINCI A5 начинает обратный путь, поднимаясь на высоту.

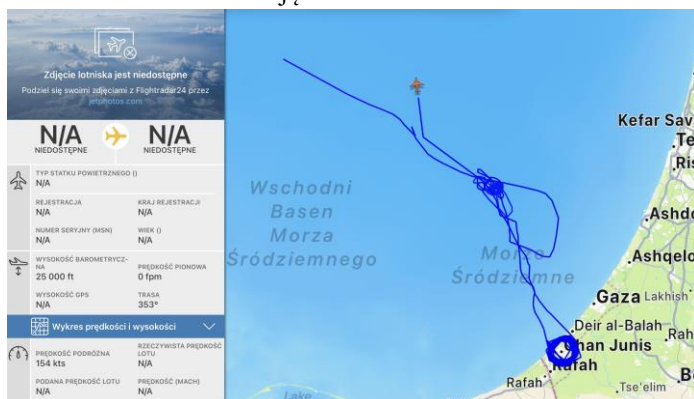
06:45: БПЛА возвращается в воздушное пространство Турции.

Rys. 34. Oficjalny komunikat władz Turcji na temat przebiegu misji Bayraktar Akinci.

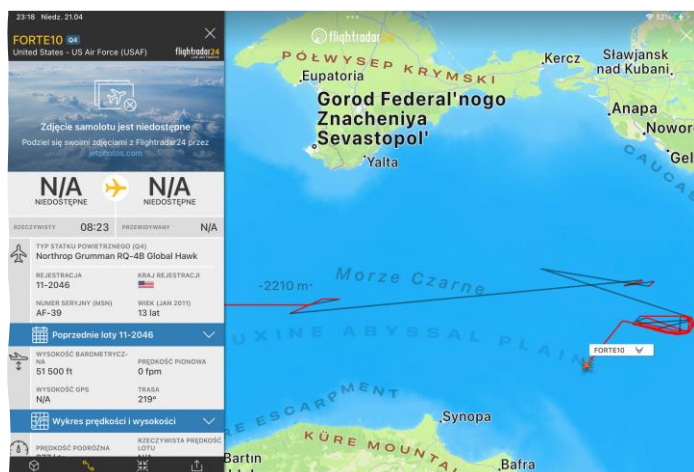
## Wpływ zakłóceń systemów GNSS na ruch lotniczy

Osoby analizujące ruch lotniczy wielokrotnie spotykają się z anomaliami w wizualizacji lotów. Znajdujące się w powietrzu aparaty zdają się nagle wykonywać dziwne, ostre manewry, a zapisy wyglądają chaotycznie. Często także tracimy dostęp do fragmentów zapisu lotu. Dzieje się tak wtedy gdy samolot znajdzie się w obszarze działania urządzenia zagłuszającego GPS (ang. **GPS jamming**). Jest kilka metod zagłuszania systemów. Dzisiaj najczęściej źródłem zagłuszania są systemy wojskowe, a sama metoda

jest traktowana jako element obrony przeciwlotniczej. Zakłada się, że zakłócony sygnał utrudni rakiecie lub atakującemu dronowi dotarcie do celu.



Rys. 34. Zakócenia sygnału GPS nad Izraelem w czasie operacji w Strefie Gazy



Rys. 35. Lot drona rozpoznawczego Forte 10.

W Polsce notujemy wysoki stan zakłóceń przynajmniej od grudnia 2023 roku, kiedy to wystosowano nawet komunikat NOTAM<sup>28</sup> informujący o problemie. Analitycy zajmujący się tematyką wskazują na lokalizację źródeł zakłóceń w Okręgu Królewieckim<sup>29</sup>.

<sup>28</sup> NOTAM (Notice to Airmen) to komunikat, który informuje lotników o warunkach lub sytuacjach, które mogą mieć wpływ na bezpieczeństwo lotów. NOTAM-y są używane do przekazywania ważnych informacji dotyczących przestrzeni powietrznej, lotnisk, tras lotów, zmian w procedurach, a także o wszelkich innych zagrożeniach, które mogą wpłynąć na operacje lotnicze.

<sup>29</sup> <https://x.com/auonsson/status/1776701617842073956/photo/1>

Informacje o obszarze i poziomie zakłóceń zbierane są na podstawie analizy danych ADSB i publikowane w serwisie gsjam.org. Mapy w tym serwisie pojawiają z minimum dobowym opóźnieniem i wskazują poziom zakłóceń.

Wracając do incydentu z samolotem SU 24MR zauważmy, że według komunikatu do naruszenia polskiej przestrzeni powietrznej doszło „na skutek awarii systemu nawigacyjnego samolotu Su-24MR”<sup>30</sup>. Mapa za dzień 11 lutego 2025 roku potwierdza silne zakłócenia sygnału GPS nad większością Zatoki Gdańskiej. Pozostaje oczywiście pytanie, na ile miały one wpływ na system nawigacyjny rosyjskiego samolotu Su-24MR.

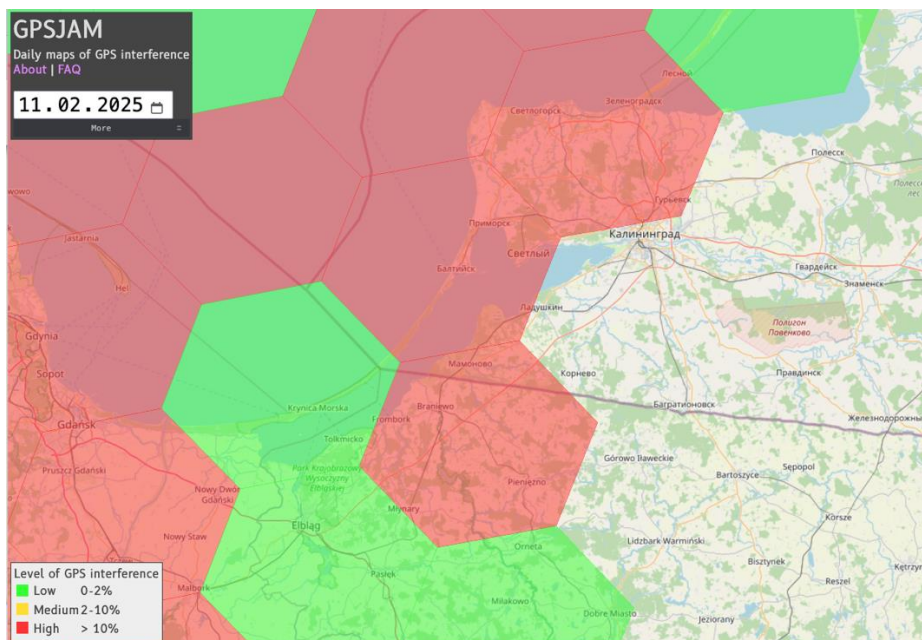
NOTAM C1142/23 Expired ●

C1142/23 NOTAMN  
Q) EPWW/QAFXX/IV/B0 /E /000/999/5202N01855E999  
A) EPWW B) 2312251730 C) 2312270700 EST  
E) ANOMALIES IN GNSS SIGNAL MAY BE EXPECTED IN AREA NORTH OF LINE  
DEFINED BY POINTS:  
1. 5131N01448E  
2. 5117N02338E.

FIR	Warszawa (EPWW)
Begin	Dec 25, 2023 17:30 UTC
End	Dec 27, 2023 07:00 UTC
Traffic	IFR/VFR
Scope	En-route
Purpose	PIB entry, Significant
Radius	999 NM

Rys. 36. NOTAM informujący o zakłóceniach systemu GPS nad Polską w grudniu 2023 roku

<sup>30</sup> <https://wiadomosci.wp.pl/naruszenie-polskiej-przestrzeni-powietrznej-jest-komunikat-wojska-7124155644635936a>

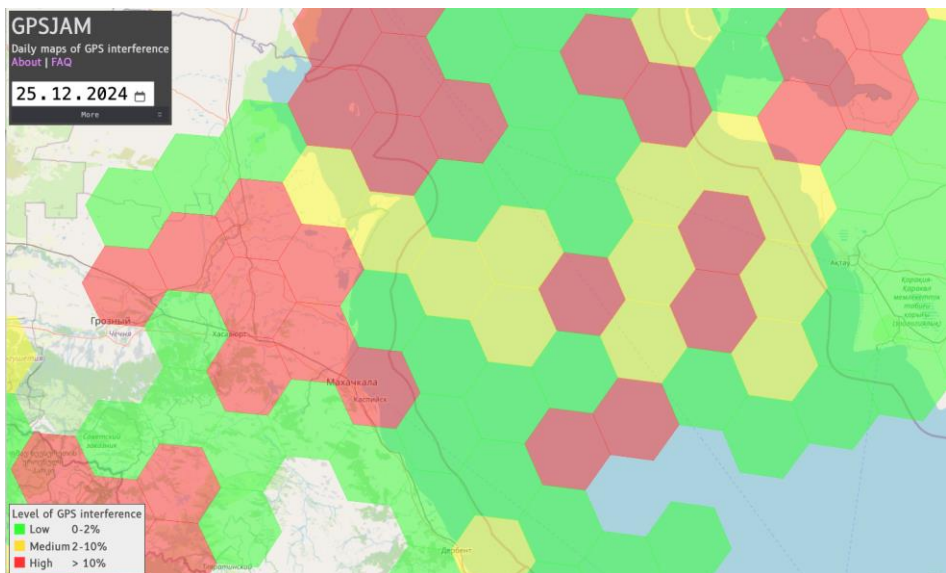


Rys. 37. Mapa z serwisu gpsjam.org dokumentująca zakłócenia w dniu 11.02.2025.

Silne zakłócenia sygnału GPS wpływają negatywnie na loty samolotów. W przypadku samolotów komunikacyjnych bywa, że zakłócenie jest powodem przerwania lotu i lądowania na innym niż docelowe lotnisku. Tak wydarzyło się, np. 11 czerwca 2024 roku w Finlandii, gdzie z powodu właśnie zakłóceń, rejsowy samolot nie mógł wylądować na znajdującym się w pobliżu rosyjskiej granicy lotnisku Joensuu i powrócić do Helsinek<sup>31</sup>.

Wdaje się także, że silne zakłócenia miały wpływ na przebieg wydarzeń poprzedzających katastrofę opisywanego na wstępie artykułu samolotu Embraer E190AR o numerze rejestracyjnym 4K-AZ65.

<sup>31</sup> <https://yle.fi/a/74-20106889>



Rys. 38. Mapa z serwisu gpsjam.org dokumentująca zakłócenia w dniu 25.12.2024 nad Czeczenią i Morzem Kaspijskim

Analiza zakłóceń nad rejonem Kaukazu w dniu katastrofy potwierdza ich wysoki poziom. Możliwe więc, że pilot uszkodzonego samolotu miał dodatkowy argument, aby nie lądować w górzystych portach lotniczych Rosji i podjął decyzję o locie przez morze do Aktau. Oczywiście do tej decyzji skłaniała także kwestia położenia kazachskiego lotniska, które znajduje się na równinie, ale jak widzimy tam warunki nawigacyjne były zdecydowanie lepsze.

Jeśli porównamy mapę zapisu danych lotu tego samolotu opublikowaną w przytaczanym już raporcie serwisu Flightradar24, to zauważymy, że wiarygodne dane lotu dotyczą tylko początkowej i ostatniej fazy. Silne zakłócenia sprawiły, że trasa jest niepełna i hipotetyczna.



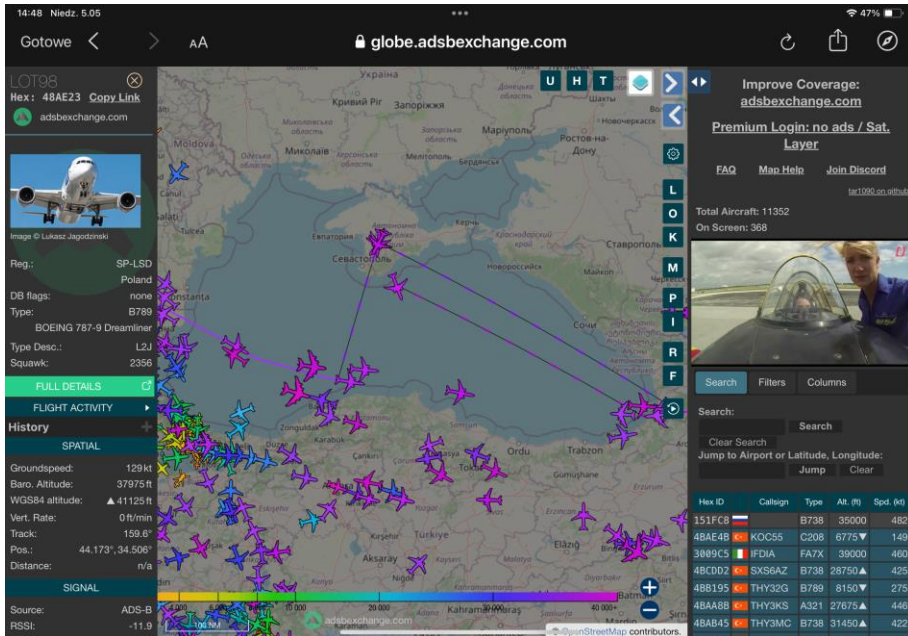
Rys. 39. Mapa lotu Embraer E190AR o numerze rejestracyjnym 4K-AZ65.

Na mapie pojawia się jeszcze jedno sformułowanie – błędne dane związane ze spoofingiem. Czym jest GPS spoofing? **GPS spoofing** to metoda zakłócania sygnałów GPS, mająca na celu wprowadzenie w błąd urządzeń korzystających z tych sygnałów, takich jak **smartfony, systemy nawigacyjne w pojazdach czy systemy stosowane w lotnictwie**. Spoofing polega na **generowaniu fałszywych sygnałów GPS**, które są wysyłane do odbiorników, przekonując je, że znajdują się one w innym miejscu, niż w rzeczywistości. Sama idea GPS spoofingu pojawiła się co najmniej w 2017 roku w Zatoce Perskiej, gdzie w błąd wprowadzono systemy nawigacyjne statków<sup>32</sup>. Do dzisiaj na Bliskim Wschodzie spoofing jest szeroko stosowany<sup>33</sup>. Przykładem jest Izrael, który zabezpieczając się przed atakiem Iranu „wirtualnie przeniósł” Telawiw do sąsiedniego Libanu. W pewnym momencie na mapach lotniczych samoloty Izraelskie lądowały i startowały z lotniska w Bejrucie. Był to jasny sygnał, że ataki, np. wyposażonych w nawigację dronów zamiast Izraela dosięgną Libanu.

Spoofing równie szeroko jest wykorzystywany do obrony przeciwlotniczej, np. na Krymie. Co pewien czas pojawiają się pytania o samoloty komunikacyjne przelatujące lub operujące nad Krymem. To właśnie efekt spoofingu.

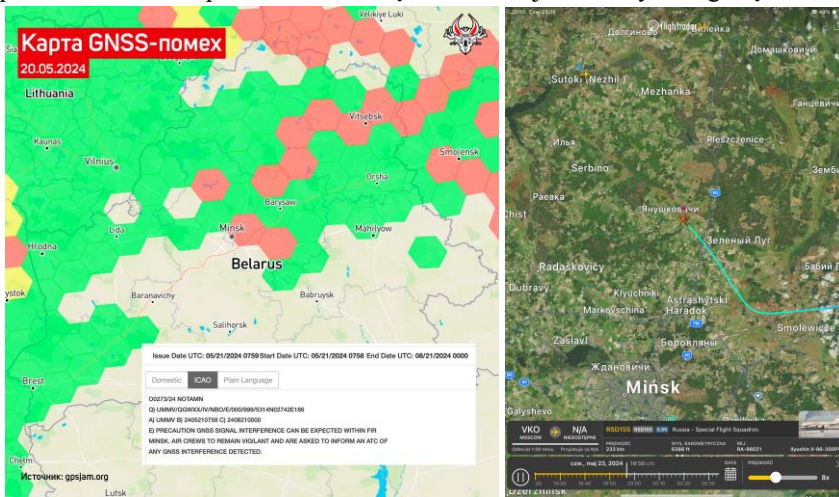
<sup>32</sup> <https://www.ww3.maritrac.com/post/electronic-interference-in-the-persian-gulf>

<sup>33</sup> <https://www.gpsworld.com/israeli-air-base-identified-as-alleged-source-of-gps-disruptions-in-mideast/>



Rys. 40. Samolot PLL LOT rzekomo przelatujący nad okupowanym Krymem.

Spoofing bywa także wykorzystany do wprowadzenia w błąd przy locie samolotu oficjalnej delegacji. Tak wydarzyło się na Białorusi w maju 2024 roku, gdy kraj ten odwiedził prezydent Rosji. Wcześniej wydano oficjalny NOTAM o możliwych problemach z systemami nawigacyjnymi. A samolot prezydencki według mapy serwisu FlightRadar24 wylądował w ... szczerym polu. W tym przypadku nie tylko wyłączono transponder, ale także wprowadzono w błąd, co do miejsca rzeczywistego lądowania.



Rys. 41. Mapy zakłóceń GPS i lądowania rosyjskiego samolotu prezydenckiego.

## PODSUMOWANIE

Analiza ruchu lotniczego ma ogromne znaczenie we współczesnych dochodzeniach otwartoźródłowych. Wymaga jednakże zrozumienia szeregu czynników związanych z lotami, konstrukcją samolotów i systemami zbierania danych. W artykule na kilku przykładach starałem się zasygnalizować wagę zagadnienia. Podsumowując warto wymienić serwisy ułatwiające dostęp do danych bieżących lub historycznych. Kilka z nich wymieniłem już w tekście, ale przypomnę je raz jeszcze. Zbierają one dane z systemu ADS-B i oferują wizualizację ruchu lotniczego w czasie rzeczywistym:

### 1. FlightRadar24

- Adres: <https://www.flightradar24.com>
- FlightRadar24 to jedna z najpopularniejszych platform do śledzenia lotów na całym świecie. Korzysta z systemu ADS-B, a także innych źródeł, takich jak radar i MLAT (Multi-Lateration), aby zapewnić dokładne dane o położeniu samolotów. Oferuje interaktywną mapę, na której można śledzić loty w czasie rzeczywistym, a także uzyskać szczegółowe informacje o poszczególnych maszynach (np. typ samolotu, prędkość, wysokość, trasa).
- FlightRadar24 oferuje zarówno bezpłatną wersję, jak i płatne subskrypcje, które zapewniają dostęp do bardziej zaawansowanych funkcji i danych historycznych.

### 2. PlaneFinder

- Adres: <https://www.planefinder.net>
- PlaneFinder to kolejna strona, która umożliwi śledzenie lotów na żywo przy użyciu danych z systemu ADS-B. Oferuje mapę z interaktywnym widokiem lotów w czasie rzeczywistym i szczegółowe informacje o samolotach. Można uzyskać dane o położeniu samolotu, jego prędkości, wysokości, trasie lotu oraz innych parametrach.
- PlaneFinder również oferuje aplikacje mobilne do śledzenia lotów, a także umożliwia dostęp do historycznych danych na podstawie zarejestrowanych tras.

### 3. ADSBExchange

- Adres: <https://www.adsbexchange.com>
- ADSBExchange to platforma, która specjalizuje się w gromadzeniu i udostępnianiu danych ADS-B. W odróżnieniu od niektórych innych serwisów, ADSBExchange nie filtruje żadnych danych, co oznacza, że użytkownicy mogą uzyskać dostęp do pełnej, surowej bazy danych o lotach na całym świecie. Jest to szczególnie popularne wśród entuzjastów lotnictwa i pasjonatów, którzy chcą mieć dostęp do jak najwięcej szczegółowych informacji.
- Platforma oferuje również możliwość śledzenia statków powietrznych w czasie rzeczywistym na mapie oraz analizowania danych historycznych.

#### 4. RadarBox

- Adres: <https://www.radarbox.com>
- RadarBox to kolejna popularna platforma śledzenia lotów, która wykorzystuje dane ADS-B, radar i inne technologie. Oferuje interaktywną mapę lotów, a także dane na temat położenia samolotów, tras, prędkości, wysokości, a także informacji o ich numerach rejestracyjnych. RadarBox ma opcję subskrypcji premium, która zapewnia dodatkowe funkcje i dane historyczne.

#### 5. OpenSky Network

- Adres: <https://opensky-network.org>
- OpenSky Network to projekt non-profit, który udostępnia dane o ruchu lotniczym, w tym dane ADS-B. Dzięki tej platformie użytkownicy mogą śledzić loty, analizować dane dotyczące przestrzeni powietrznej oraz korzystać z narzędzi analitycznych. OpenSky gromadzi dane na całym świecie i udostępnia je zarówno profesjonalistom, jak i entuzjastom lotnictwa.

#### 6. FlightAware

- Adres: <https://www.flightaware.com>
- FlightAware jest jedną z największych platform do śledzenia lotów, która również korzysta z technologii ADS-B do śledzenia samolotów w czasie rzeczywistym. Strona oferuje interaktywne mapy, a także dostęp do szczegółowych danych o lotach, w tym prędkości, wysokości i trasie. FlightAware oferuje zarówno bezpłatny, jak i płatny dostęp do swoich usług.

#### 7. SkyVector

- Adres: <https://skyvector.com>
- SkyVector to narzędzie używane głównie przez pilotów do planowania tras lotów. Oferuje mapy lotnicze oraz wizualizacje ruchu lotniczego w czasie rzeczywistym, w tym dane ADS-B. Choć głównie skierowane na planowanie lotów, SkyVector umożliwia również śledzenie samolotów w czasie rzeczywistym.

#### 8. FlightStats

- Adres: <https://www.flightstats.com>
- FlightStats to platforma śledzenia lotów, która wykorzystuje różne źródła, w tym ADS-B, do monitorowania ruchu lotniczego. Oferuje dane o położeniu, opóźnieniach i innych informacjach dotyczących lotów.

Podane usługi i strony pozwalają użytkownikom na śledzenie lotów, analizowanie danych o ruchu lotniczym, a także oferują dostęp do dodatkowych funkcji, takich jak możliwość filtrowania samolotów według różnych parametrów (np. numer lotu, typ samolotu, położenie itp.). W zależności od platformy, można uzyskać dostęp do danych w czasie rzeczywistym oraz do informacji historycznych. Oprócz źródeł informacji

wymienić należy także serwis Aircraft Recognition Guide<sup>34</sup>, który w przystępny sposób pomaga w identyfikacji typów i modeli samolotów. Podstawy analizy ruchu lotniczego omówione są także w książce autorstwa Rae Baker „Prawdziwa głębia OSINT. Odkryj wartość danych Open Source Intelligence” wydanej w Polsce przez Helion. Artykuł naturalnie nie wyczerpuje tematu, a książka stanowi jedynie próbę spojrzenia na zagadnienie z punktu widzenia analizy informacji.

## **BIBLIOGRAFIA**

1. <https://gijn.org/>
2. <https://icarus.flights/>
3. <https://khemoradio.com/doomsday-planes-flying-over-missouri/>
4. <https://makanom.livejournal.com/530582.html?>
5. <https://opensky-network.org/>
6. [https://t.me/Flightradar24\\_Air\\_Force](https://t.me/Flightradar24_Air_Force)
7. <https://tgstat.ru/channel/@aboutplane>
8. <https://wiadomosci.wp.pl/naruszenie-polskiej-przestrzeni-powietrznej-jest-komunikat-wojska-7124155644635936a>
9. <https://www.aa.com.tr/ru/мир/крушение-самолета-embraer-190-в-актау-версии-потерпевших-пассажиров-и-аналитиков/3434860>
10. <https://www.adsbexchange.com>
11. <https://www.adsbhub.org/>
12. <https://www.aerodata.de/en/>
13. <https://www.aircraftrecognitionguide.com/>
14. <https://www.flightradar24.com/blog/azerbaijan-airlines-e190-crashes-near-aktau/>
15. <https://www.flightradar24.com/blog/turkish-akinci-iran/>
16. <https://www.gpsworld.com/israeli-air-base-identified-as-alleged-source-of-gps-disruptions-in-mideast/>
17. <https://www.itamilradar.com>
18. <https://www.konflikty.pl/aktualnosci/wiadomosci/drugi-214pu-sbus/>
19. <https://www.pansa.pl/inspekcja/beechnraft-king-air-350/>
20. <https://www.pap.pl/aktualnosci/katastrofa-smiglowca-z-prezydentem-iranu-ebrahim-raisi-nie-zyje-wideo>
21. <https://www.polityka.pl/tygodnikpolityka/swiat/2221664,1,szojgu-w-korei-pln-witany-jak-gwiazda-rocka-rosja-sklada-oferte-na-co-liczy-w-zamian.read>
22. <https://www.polska-zbrojna.pl/home/articleshow/41759?t=Wszystkie-misje-AWACS-a>
23. <https://www.radarbox.com/>
24. <https://www.wv3.maritrace.com/post/electronic-interference-in-the-persian-gulf>
25. <https://www.xayalmuazzin.com/>

---

<sup>34</sup> <https://www.aircraftrecognitionguide.com/>

26. <https://x.com/auonsson>
27. <https://x.com/auonsson/status/1776701617842073956/photo/1>
28. <https://x.com/DowOperSZ>
29. <https://x.com/menchosint>
30. [https://x.com/team\\_luftwaffe](https://x.com/team_luftwaffe)
31. <https://yle.fi/a/74-20106889>
32. [www.pilotmall.com](http://www.pilotmall.com)

# WALKA Z ANALIZĄ – WYBRANE MECHANIZMY OCHRONNE MALWARE I SPOSOBY ICH NEUTRALIZACJI

## FIGHT AGAINST CODING ANALYSIS - SELECTED MALWARE PROTECTION MECHANISMS AND WAYS TO NEUTRALIZE THEM

**Kamil KOŁODZIEJCZYK<sup>1</sup>**

**Streszczenie:** Artykuł przedstawia techniki antysandboxowe i antydebugingowe stosowane przez złośliwe oprogramowanie, takie jak wykrywanie bibliotek wirtualizacyjnych, analiza kluczy rejestru czy weryfikacja połączeń sieciowych. Omówiono również metody ich neutralizacji, w tym zmianę logiki funkcji, modyfikację parametrów i zastępowanie kodu instrukcjami NOP. Celem jest zrozumienie mechanizmów unikania analizy i skutecznych sposobów ich obejścia.

**Słowa kluczowe:** analiza złośliwego oprogramowania, antydebuging, malware, techniki unikania analizy, mechanizmy obronne malware.

**Summary:** The study presents anti-sandbox and anti-debugging techniques used by malware, such as detecting virtualization libraries, analyzing registry keys, or verifying network connections. It also discusses methods for neutralizing these mechanisms, including modifying function logic, altering parameters, and replacing code with NOP instructions. The goal is to understand avoidance mechanisms and effective ways to bypass them.

**Keywords:** malware analysis, anti-debugging, malware, evasion techniques, malware defense mechanisms.

### WSTĘP

W obliczu rosnącej liczby zagrożeń w cyberprzestrzeni złośliwe oprogramowanie (malware) rozwija techniki, które pozwalają skutecznie unikać wykrycia i utrudniać pracę specjalistom ds. bezpieczeństwa, jak również i samym użytkownikom. Twórcy „wirusów” nie tylko koncentrują się na infekowaniu systemów, ale także na wdrażaniu mechanizmów obronnych, które chronią ich szkodliwe dzieła przed analizą i neutralizacją.

Celem artykułu jest przybliżenie najczęściej stosowanych technik antysandboxowych i antydebugingowych, które umożliwiają malware przetrwanie w środowiskach kontrolowanych przez analityków. Techniki te pozwalają złośliwemu

---

<sup>1</sup> Sekcja Informatyki Śledczej, Zarząd Specjalny, Centralne Biuro Zwalczenia Cyberprzestępczości, kamil.kolodziejczyk@cbzc.policja.gov.pl.

oprogramowaniu rozpoznać, czy działa w sztucznym środowisku (np. wirtualnej maszynie lub sandboxie) lub wykryć obecność narzędzi diagnostycznych, takich jak debugery. Dzięki temu malware może podejmować działania obronne – opóźnić wykonanie szkodliwego kodu, ukrywać swoje funkcje lub całkowicie przerywać działanie, jeśli wykryje, że jest analizowane.

W pracy przedstawiono zarówno ogólne zasady działania technik unikania sandboxów i debuggerów, jak i konkretne przykłady ich implementacji w programach. Omówiono także praktyczne metody neutralizacji tych mechanizmów, w tym modyfikację logiki kodu, zmianę parametrów oraz zastępowanie fragmentów kodu instrukcjami NOP. W artykule zaprezentowano również narzędzia wykorzystywane w procesie analizy, takie jak debugery i edytory hexadecymalne, oraz przygotowano prosty skrypt w Pythonie automatyzujący proces modyfikacji kodu binarnego. Analiza ta pozwala zrozumieć, dlaczego techniki obronne malware stanowią wyzwanie dla analityków i jak można im przeciwdziałać, aby skuteczniej zwalczać cyberzagrożenia.

## TECHNIKI OCHRONNE

Sandbox – jest to izolowane środowisko uruchomieniowe, które służy między innymi do bezpiecznego testowania i analizy podejrzanych programów, w tym złośliwego oprogramowania (malware). Głównym jego celem jest umożliwienie obserwacji zachowania programu w kontrolowanych warunkach bez ryzyka, że jego działanie wpłynie na rzeczywisty system operacyjny lub sieć. Sandbox tworzy wirtualne środowisko, które emuluje rzeczywisty system operacyjny, często z ograniczonym dostępem do zasobów sprzętowych i sieciowych.

Twórcy złośliwego oprogramowania zdają sobie sprawę, że sandboxy są skutecznym narzędziem do analizy ich projektów. W rezultacie implementują techniki antysandboxowe, które pozwalają rozpoznać, czy program działa w sztucznym środowisku. Jeśli malware wykryje sandbox, może:

- przerwać swoje działanie,
- ograniczyć wykonywane operacje, by wyglądać na nieszkodliwe,
- opóźnić działanie, by zmylić analityków,
- wykonać zupełnie inną – nieszkodliwą wersję kodu.

Sandboxy są kluczowym elementem analizy malware, ale ich skuteczność zależy od zdolności do ukrycia swojej tożsamości przed badanym oprogramowaniem. Stąd „wyścig zbrojeń” między twórcami malware, a analitykami bezpieczeństwa trwa nieustannie.

Jedną z najprostszych, a zarazem skutecznych technik wykorzystywanych przez złośliwe oprogramowanie do wykrywania środowisk sandboxowych jest sprawdzanie obecności charakterystycznych dla nich bibliotek w systemie, takich jak:

- VBox\*.dll – powiązana z VirtualBox oraz

- vm\*.dll – biblioteki wykorzystywane przez VMware (np. vmGuestLib.dll, vmhgfs.dll).

Malware przeszukuje system operacyjny w poszukiwaniu plików DLL związanych z popularnymi platformami wirtualizacji dla instalacji VirtualBox: VBoxGuest.dll, VBoxSF.dll czy VBoxService.dll oraz VMware – biblioteki z prefixem vm, takie jak np. vmGuestLib.dll. Obecność tych bibliotek wskazuje, że mamy do czynienia z konkretną platformą wirtualizacyjną.

Na rysunku numer 1 został przedstawiony fragment kodu wykorzystującego bibliotekę systemową FindFirstFileW do wyszukiwania plików w katalogu C:\Windows\System32. Jeśli poszukiwane biblioteki (np. VBoxGuest.dll) zostaną znalezione, malware może wykryć, że działa w środowisku wirtualnym i zmodyfikować swoje zachowanie.

```
sub_140001950 proc near

    phkResult= qword ptr -288h
    var_278= qword ptr -278h
    FindFileData= _WIN32_FIND_DATAW ptr -268h
    var_18= qword ptr -18h

; __unwind { // __GSHandlerCheck
sub     rsp, 2A8h          ; Integer Subtraction
mov     rax, cs:__security_cookie
xor     rax, rsp          ; Logical Exclusive OR
mov     [rsp+2A8h+var_18], rax
lea     rdx, [rsp+2A8h+FindFileData] ; lpFindFileData
lea     rcx, aCWindowsSystem ; "C:\\Windows\\System32\\VBox*.dll"
call    cs:FindFirstFileW ; Indirect Call Near Procedure
cmp     rax, 0FFFFFFFFFFFFh ; Compare Two Operands
jz     short loc_14000198B ; Jump if Zero (ZF=1)
```

Rys. 4. Przykład kodu sprawdzającego obecność bibliotek VBox.dll

Na rysunku numer 2 zaprezentowany został fragment kodu przedstawiający ponownie detekcję bibliotek VMware poprzez wyszukiwanie plików vm\*.dll w katalogu C:\Windows\System32 za pomocą funkcji FindFirstFileW. Jeśli biblioteki charakterystyczne dla VMware zostaną znalezione, malware może wykryć, że działa w środowisku wirtualnym i podjąć odpowiednie kroki.

```
loc_14000198B:          ; lpFindFileData
lea     rdx, [rsp+2A8h+FindFileData]
lea     rcx, aCWindowsSystem_0 ; "C:\\Windows\\System32\\vm*.dll"
call    cs:FindFirstFileW ; Indirect Call Near Procedure
cmp     rax, 0FFFFFFFFFFFFh ; Compare Two Operands
jz     short loc_1400019AA ; Jump if Zero (ZF=1)
```

Rys. 5. Przykład kodu sprawdzającego obecność bibliotek vm\*.dll

Innym sposobem jest wykorzystanie specyficznych wpisów w rejestrze systemu Windows, jako sposób na wykrycie środowisk wirtualnych. Klucze rejestru pozostawione

przez oprogramowanie wirtualizacyjne są jednym z najbardziej charakterystycznych śladów, które pozwalają malware rozpoznać, że działa w wirtualnym środowisku.

```
loc_1400019AA:
lea   rax, [rsp+2A8h+var_278] ; Load Effective Address
mov   [rsp+2A8h+phkResult], rax ; phkResult
mov   r9d, 1 ; samDesired
xor   r8d, r8d ; ulOptions
lea   rdx, SubKey ; "SYSTEM\\ControlSet001\\Services\\VBoxSF"
mov   rcx, 0FFFFFFF80000002h ; hKey
call  cs:RegOpenKeyExW ; Indirect Call Near Procedure
test  eax, eax ; Logical Compare
jnz   short loc_1400019DC ; Jump if Not Zero (ZF=0)
```

Rys. 6. Fragment kodu przedstawiający implementację techniki antysandboxowej polegającej na detekcji klucza rejestru dla VirtualBox

Rysunek numer 3 przedstawia technikę antysandboxową opartą na detekcji środowiska VirtualBox za pomocą klucza rejestru systemu Windows. Główna funkcja, którą wykorzystano, to RegOpenKeyExW (odpowiedzialna za otwarcie wskazanego klucza rejestru). Kod najpierw przygotowuje parametry wymagane do wywołania tej funkcji. Klucz rejestru, który jest sprawdzany, to SYSTEM\ControlSet001\Services\VBoxSF, charakterystyczny dla maszyn wirtualnych VirtualBox. Wskaźnik na ten klucz zostaje załadowany do rejestru rdx. Główna gałąź rejestru, od której zaczyna się operacja, to HKEY\_LOCAL\_MACHINE, zaadresowana w rejestrze rcx. W rejestrach r9d i r8d zapisano dodatkowe parametry: minimalny poziom dostępu i brak opcji specjalnych podczas otwierania klucza. Po przygotowaniu parametrów następuje wywołanie funkcji RegOpenKeyExW. Wynik działania tej funkcji jest zapisany w rejestrze eax i natychmiast sprawdzany za pomocą instrukcji test eax, eax. Jeśli wartość w eax wynosi zero, oznacza to, że klucz rejestru został znaleziony. W przeciwnym przypadku następuje przeskoczenie do innej części kodu.

Rysunek numer 4 przedstawia fragment kodu z tą samą techniką, co w przypadku VirtualBox, jednak zamiast wykrywać klucze związane z VirtualBox, malware sprawdza obecność klucza charakterystycznego dla VMware: SYSTEM\ControlSet001\Services\VMTools.

```
loc_1400019DC:
lea   rax, [rsp+2A8h+var_278] ; Load Effective Address
mov   [rsp+2A8h+phkResult], rax ; phkResult
mov   r9d, 1 ; samDesired
xor   r8d, r8d ; ulOptions
lea   rdx, aSystemControls_0 ; "SYSTEM\\ControlSet001\\Services\\VMTool"...
mov   rcx, 0FFFFFFF80000002h ; hKey
call  cs:RegOpenKeyExW ; Indirect Call Near Procedure
test  eax, eax ; Logical Compare
jnz   short loc_140001A0E ; Jump if Not Zero (ZF=0)
```

Rys. 7. Fragment kodu przedstawiający implementację techniki antysandboxowej

Inną interesującą techniką jest sprawdzanie czasu od momentu uruchomienia systemu operacyjnego. Środowiska sandboxowe są zazwyczaj nowo uruchamianymi maszynami wirtualnymi. Jeśli malware wykryje, że system działa krócej niż określony czas, może uznać, że znajduje się w środowisku wirtualnym i nie wykonać swojego szkodliwego kodu.

Fragment kodu zaprezentowany na rysunku numer 5 ilustruje tę technikę. Funkcja GetTickCount64 zwraca liczbę milisekund, które upłynęły od momentu uruchomienia systemu. Wynik tej funkcji jest przechowywany w rejestrze rax. W funkcji: `cmp [rsp+38h+var_18], 86400` – wartość uzyskana w poprzednim kroku jest porównywana z liczbą 86400. Ta liczba odpowiada 24 godzinom (86400 sekund = 24 godziny). Jeśli wartość czasu działania systemu jest mniejsza niż 24 godziny, kod wykonuje skok warunkowy za pomocą instrukcji `jnb` (jump if not below), co oznacza, że program kontynuuje wykonanie tylko wtedy, gdy upłynęło przynajmniej 24 godziny.

```
sub    rsp, 38h          ; Integer Subtraction
call   cs:GetTickCount64 ; Indirect Call Near Procedure
xor    edx, edx         ; Logical Exclusive OR
mov    ecx, 3E8h
div    rcx              ; Unsigned Divide
mov    [rsp+38h+var_18], rax
cmp    [rsp+38h+var_18], 86400 ; Compare Two Operands
jnb    short loc_1400017BB ; Jump if Not Below (CF=0)
```

Rys. 8. Fragment kodu przedstawiający implementację techniki opóźnienia wykonania malware

Kolejną ciekawą techniką jest weryfikowanie przez złośliwe oprogramowanie dostępu do sieci internet. Sandboxy często działają w środowiskach izolowanych od internetu lub z ograniczonym dostępem do sieci, aby zapewnić bezpieczeństwo analizy. Złośliwe oprogramowanie wykorzystuje to ograniczenie, próbując nawiązać połączenie z konkretnymi, znanymi domenami, takimi jak `update.microsoft.com`. Domeny te są powszechnie dostępne w normalnych warunkach, więc ich niedostępność może być dla malware sygnałem, że działa w sandboxie. Ta technika jest prostym, ale skutecznym sposobem na odróżnienie rzeczywistego środowiska od wirtualnego i utrudnia pełną analizę zachowania malware.

Rysunek numer 6 przedstawia tego typu rozwiązanie. Ten fragment kodu przedstawia sposób, w jaki złośliwe oprogramowanie wykorzystuje funkcję `InternetCheckConnectionA` do weryfikacji obecności aktywnego połączenia z internetem i dostępności konkretnej domeny – w tym przypadku `http://update.microsoft.com`. Adres URL jest przekazywany do funkcji jako parametr, która następnie próbuje ustalić czy system może nawiązać połączenie z podaną lokalizacją sieciową. Jeśli połączenie z domeną `http://update.microsoft.com` jest możliwe, funkcja zwraca wynik pozytywny, co może być dla malware sygnałem, że działa w normalnym, rzeczywistym środowisku

użytkownika. W przeciwnym przypadku, jeśli połączenie nie zostanie ustanowione, złośliwe oprogramowanie może podejrzewać, że działa w izolowanym środowisku analitycznym, takim jak sandbox, które często blokuje lub symuluje dostęp do internetu. W tym kodzie widać, że przygotowywane są odpowiednie parametry dla funkcji – adres URL zostaje załadowany do odpowiedniego rejestru, a flagi wymuszają rzeczywistą próbę połączenia, pomijając ewentualną pamięć podręczną systemu. Malware analizuje wynik tej operacji, co pozwala mu dostosować swoje zachowanie w zależności od dostępności sieci. Brak dostępu do wskazanej domeny może skutkować wstrzymaniem szkodliwej aktywności, co ma na celu zmylenie analityków i utrudnienie pełnej analizy złośliwego oprogramowania. Technika ta bazuje na powszechności dostępu do domen takich jak update.microsoft.com, które w normalnym środowisku są niemal zawsze dostępne. Dzięki temu malware może w prosty sposób zidentyfikować sytuacje, w których działa w sztucznie ograniczonym środowisku, charakterystycznym dla systemów analitycznych.

```

lea   rcx, aHttpUpdateMicr ; "http://update.microsoft.com"
mov   rdi, rcx
mov   rsi, rcx
mov   ecx, 1Ch
rep   movsb                ; Move Byte(s) from String to String
xor   r8d, r8d             ; dwReserved
mov   edx, 1               ; dwFlags
lea   rcx, [rsp+0D8h+szUrl] ; lpszUrl
call  cs:InternetCheckConnectionA ; Indirect Call Near Procedure

```

Rys. 9. Fragment kodu przedstawiający implementację techniki detekcji dostępu do sieci

Następną, frustrującą i najczęściej spotykaną funkcją utrudniającą analizę jest Sleep(). Jest ona idealnym rozwiązaniem na automatyczne sandboxy. Środowiska takie zazwyczaj mają ograniczony czas analizy, aby szybko wykrywać zagrożenia i minimalizować zużycie zasobów. Malware, wprowadzając celowe opóźnienia w swoim działaniu, próbuje „przeczekać” ten ograniczony czas. Dzięki temu szkodliwy kod może uniknąć swojego wykonania w sandboxie, ponieważ analiza kończy się, zanim malware zdąży ujawnić swoją szkodliwą funkcjonalność. Funkcja ta może być także myląca dla niedoświadczonego analityka, który uruchamia próbkę na krótki czas bez wcześniejszej analizy kodu. Ponieważ przez pośpiech może on nie doczekać do momentu wykonania tej najważniejszej, złośliwej części kodu.

Rysunek numer 7 prezentuje zastosowanie tego rozwiązania. Analiza kodu pozwala na wykrycie zastosowania krótkiego opóźnienia (5 sekund), które może być częścią większej sekwencji wstrzymań, mającej na celu zwiększenie łącznego czasu oczekiwania. W bardziej zaawansowanych przypadkach opóźnienia mogą być znacznie dłuższe bądź dynamicznie obliczane co dodatkowo utrudnia analitykom przewidzenie zachowania malware.

```

mov   ecx, 5000            ; dwMilliseconds
call  cs:Sleep             ; Indirect Call Near Procedure

```

Rys. 10. Fragment kodu przedstawiający implementację funkcji Sleep()

Innym rodzajem technik jest wykrywanie uruchomienia programu w debuggerze. Debugger to narzędzie programistyczne używane do analizy i debugowania (poprawiania) programów komputerowych. Umożliwia deweloperom oraz analitykom śledzenie działania programu w czasie rzeczywistym, identyfikowanie błędów, analizę logiki działania oraz monitorowanie wartości zmiennych, pamięci i innych aspektów wewnętrznego funkcjonowania aplikacji. W kontekście analizy malware, debugger jest nieocenionym narzędziem, które pozwala analitykom na:

- obserwowanie zachowania złośliwego oprogramowania bez jego pełnego wykonania,
- zatrzymywanie wykonywania szkodliwego kodu w kluczowych momentach, aby zrozumieć jego logikę,
- zmieniać dane lub kod na żywo, aby zobaczyć, jak malware reaguje na modyfikacje.

Złośliwe oprogramowanie może wykrywać obecność debuggera za pomocą specjalnych funkcji API systemowych, takich jak `IsDebuggerPresent`, sprawdzając określone flagi systemowe lub monitorując czas wykonania programu (np. przy opóźnieniu wywoływanym przez debugera). Jeśli malware wykryje debuger, często zmienia swoje zachowanie, aby utrudnić analizę.

Rysunek numer 8 przedstawia procedurę o nazwie `Check_debugger`, która implementuje technikę antydebuggingową mającą na celu wykrycie obecności debuggera i odpowiednie zareagowanie, jeśli zostanie on wykryty. Na początku programu rezerwowane jest miejsce na stosie, a następnie za pomocą instrukcji odczytywana jest struktura Thread Environment Block (TEB). Jest to obiekt w systemie Windows, który przechowuje różne informacje o bieżącym wątku, w tym flagę wskazującą, czy proces jest debugowany. Kod odczytuje wartość flagi z odpowiedniego pola TEB i sprawdza, czy wskazuje ona na obecność debuggera. Jeśli flaga nie jest ustawiona, program przechodzi do sekcji, w której kończy procedurę bez żadnych dalszych działań. Natomiast gdy flaga wskazuje na obecność debuggera, program wykonuje kolejne kroki mające na celu poinformowanie użytkownika lub analityka o wykryciu tego narzędzia. W tym celu wywoływana jest funkcja `MessageBoxW`, która wyświetla komunikat z tytułem "*Abort!*" i treścią "*Debugger Detected*". Po pokazaniu tego komunikatu program natychmiast kończy swoje działanie, wywołując funkcję `ExitProcess`, co uniemożliwia dalsze badanie jego działania. W przypadku, gdy debugger nie zostanie wykryty, procedura po prostu kończy swoje wykonanie, przywracając stos do pierwotnego stanu i wracając do głównego kodu programu.

Całość ilustruje typową technikę antydebuggingową, w której malware monitoruje systemowe struktury pamięci w celu rozpoznania, czy jest analizowane, a w razie wykrycia narzędzi takich jak debugger podejmuje działania defensywne, takie jak

zakończenie procesu. Ten mechanizm jest prosty, ale bardzo skuteczny w utrudnianiu dynamicznej analizy przez analityków.

```

Check_debugger proc near

var_18= qword ptr -18h

sub    rsp, 38h
mov    rax, gs:60h
mov    [rsp+38h+var_18], rax
mov    rax, [rsp+38h+var_18]
movzx  eax, byte ptr [rax+2]
test   eax, eax
jz     short loc_140001786

mov    r9d, 10h           ; uType
lea    r8, Caption       ; "Abort!"
lea    rdx, Text         ; "Debugger Detected"
xor    ecx, ecx          ; hWnd
call   cs:MessageBoxW
mov    ecx, 9            ; uExitCode
call   cs:ExitProcess

loc_140001786:
add    rsp, 38h
retn
Check_debugger endp

```

Rys. 11. Fragment procedury implementujący technikę antydebuggingową

## OBEJŚCIE MECHANIZMÓW OCHRONNYCH W MALWARE

Dla analityków bezpieczeństwa kluczowe jest umiejętnie radzenie sobie z omawianymi zabezpieczeniami. Neutralizacja tych funkcji pozwala na odsłonięcie prawdziwego zachowania złośliwego oprogramowania i skuteczną analizę jego potencjalnych zagrożeń. W tej części omówione zostaną trzy praktyczne techniki obejścia mechanizmów ochronnych:

1. Zmiana logiki funkcji
2. Modyfikacja parametrów/zmiennych funkcji
3. Wypełnienie „NOP-ami”

Jednym z najprostszych i najczęściej stosowanych sposobów na obejście funkcji omawianych funkcji jest zmiana logiki programu poprzez modyfikację instrukcji warunkowych. W kodzie mogą być zastosowane następujące warunki:

- jne (jump if not equal) - instrukcja jne wykonuje skok do wskazanego adresu, jeśli flaga zerowa (ZF) nie jest ustawiona, co oznacza, że wynik ostatniej operacji nie był równy zero. Jest to często stosowane w celu wykonania alternatywnego bloku kodu, gdy dwie wartości porównywane ze sobą są różne.

- je (jump if equal) - instrukcja je wykonuje skok do wskazanego adresu, jeśli flaga zerowa (ZF) jest ustawiona, co oznacza, że wynik ostatniej operacji był równy zero. W praktyce sygnalizuje to, że dwie wartości porównywane były sobie równe.
- jnz (jump if not zero) - skok, jeśli flaga zerowa (ZF) nie jest ustawiona, co oznacza, że wynik ostatniej operacji był różny od zera. Jest to odpowiednik jne.
- jz (jump if zero) - skok, jeśli flaga zerowa (ZF) jest ustawiona, co oznacza, że wynik ostatniej operacji był równy zero. Jest to odpowiednik je.
- jnle (jump if not less or equal) - skok, jeśli flaga zerowa (ZF) nie jest ustawiona oraz flaga znaku (SF) nie różni się od flagi nadmiaru (OF). Oznacza to, że wynik ostatniego porównania jest większy.
- jnl (jump if not less) - skok, jeśli flaga znaku (SF) nie różni się od flagi nadmiaru (OF). Oznacza to, że wynik ostatniego porównania jest większy lub równy.
- jnge (jump if not greater or equal) - skok, jeśli flaga znaku (SF) różni się od flagi nadmiaru (OF). Oznacza to, że wynik ostatniego porównania jest mniejszy.
- jng (jump if not greater) - skok, jeśli flaga zerowa (ZF) jest ustawiona lub flaga znaku (SF) różni się od flagi nadmiaru (OF). Oznacza to, że wynik ostatniego porównania jest mniejszy lub równy.

Instrukcje te umożliwiają sterowanie przepływem programu w zależności od wyników operacji porównania lub innych logicznych warunków. Są one kluczowe w logice programów, w tym mechanizmów zabezpieczających.

Rozważmy fragment kodu, w którym program sprawdza obecność debuggera za pomocą warunku, a następnie podejmuje odpowiednie działania. Instrukcja warunkowa, taka jak jne (jump if not equal), jest kluczowym elementem, który decyduje, czy program ma kontynuować działanie, czy przejść do sekcji obsługi debuggera.

```
test eax, eax      ; Sprawdzenie flagi debuggera
jne DebuggerDetected ; Skok do obsługi debuggera, jeśli wykryto
```

Rys. 12. Fragment kodu sprawdzający obecność debuggera

Instrukcja jne sprawdza, czy wynik operacji (wartość w eax) różni się od zera. Jeśli tak, wykonuje skok do etykiety DebuggerDetected, gdzie program reaguje na obecność debuggera, np. wyświetla komunikat lub kończy działanie.

Aby oszukać program i zmusić go do "myślenia", że debuggera nigdy nie wykryto, można zmienić instrukcję jne (skok przy braku równości) na je (skok przy równości). Po tej modyfikacji program zachowa się, jakby debuggera nie było, niezależnie od rzeczywistego wyniku sprawdzenia

```
test eax, eax      ; Sprawdzenie flagi debuggera
je DebuggerDetected ; Skok do obsługi debuggera, jeśli wykryto
```

Rys. 13. Zmodyfikowany fragment kodu sprawdzający obecność debuggera

Po tej zmianie program zawsze przejdzie do kolejnych instrukcji, ignorując debuggera, nawet jeśli jest obecny. W ten sposób funkcja antydebuggingowa staje się nieskuteczna, a analityk może kontynuować badanie zachowania programu.

Modyfikacja parametrów lub zmiennych używanych w funkcjach jest kolejnym skutecznym sposobem na obejście mechanizmów antysandboxowych. Polega na edycji wartości, które są kluczowe dla działania funkcji sprawdzających środowisko, tak aby zmienić ich logikę lub wprowadzić dane, które nie mają wpływu na analizę. Przeanalizujemy to na przykładzie zmiany nazwy pliku VBox\*.dll (charakterystycznego dla VirtualBox) na MMox\*.dll, które nie istnieje.

Rozważmy przedstawiony na rysunku numer 11 fragment kodu, w którym malware wykorzystuje funkcję FindFirstFileW do wyszukiwania plików VBox\*.dll w katalogu systemowym, aby sprawdzić obecność VirtualBox. W tym przypadku nazwa VBox\*.dll jest kluczowym parametrem, który decyduje o wykryciu sandboxa.

```
lea rcx, aCWindowsSystem ; Załadowanie ścieżki "C:\\Windows\\System32\\VBox*.dll"  
call FindFirstFileW      ; Sprawdzenie, czy plik istnieje  
cmp rax, -1             ; Porównanie wyniku  
jz SandboxDetected     ; Skok, jeśli plik znaleziono
```

Rys. 14. Fragment kodu wykorzystującego funkcję FindFirstFileW do wyszukiwania plików VBox\*.dll

Aby wyłączyć funkcjonalność tego sprawdzenia, można zmienić ciąg znaków VBox\*.dll na inny, np. MMox\*.dll, który nie istnieje w środowisku VirtualBox (ani w innych systemach). Zmiana ta powoduje, że funkcja FindFirstFileW zawsze zwraca wartość wskazującą brak pliku, nawet w środowiskach wirtualnych. Powyższą zmianę zaprezentowano na rysunku numer 12.

```
lea rcx, aCWindowsSystem ; Załadowanie ścieżki "C:\\Windows\\System32\\MMox*.dll"  
call FindFirstFileW      ; Sprawdzenie, czy plik istnieje  
cmp rax, -1             ; Porównanie wyniku  
jz SandboxDetected     ; Skok, jeśli plik znaleziono
```

Rys. 15. Zmodyfikowany fragment kodu wykorzystującego funkcję FindFirstFileW do wyszukiwania plików MMox\*.dll

W ten sposób nawet jeśli malware działa w środowisku VirtualBox, funkcja FindFirstFileW nie wykryje charakterystycznych bibliotek, ponieważ modyfikacja parametru zmienia kryterium wyszukiwania.

Zastąpienie instrukcji kodu operacjami NOP (ang. No Operation) to jedna z najprostszych i najszybszych metod wyłączania mechanizmów antydebuggingowych. Instrukcja NOP nie wykonuje żadnej operacji i jedynie przesuwa wskaźnik instrukcji do następnej pozycji, nie zmieniając stanu procesora. Dzięki temu możemy "zneutralizować" wybrane fragmenty kodu bez konieczności modyfikacji jego logiki.

W przypadku funkcji InternetCheckConnectionA, stosowanej przez malware do weryfikacji połączenia z internetem, neutralizacja jej działania poprzez wypełnienie

instrukcjami NOP jest skutecznym sposobem na obejście mechanizmu wykrywania sandboxów. Usunięcie tej funkcjonalności sprawia, że malware działa tak, jakby połączenie internetowe zawsze było dostępne. Rysunek numer 13 przedstawia fragment kodu weryfikujący dostęp do sieci internet.

```
lea rcx, aHttpUpdateMicr ; Załadowanie adresu URL "http://update.microsoft.com"
xor r8d, r8d ; Ustawienie opcji dwReserved na 0
mov edx, 1 ; Ustawienie flagi dwFlags na 1 (realna weryfikacja połączenia)
call InternetCheckConnectionA ; Wywołanie funkcji
test eax, eax ; Sprawdzenie wyniku (0 = brak połączenia, 1 = dostępne)
jz NoInternet ; Skok, jeśli brak połączenia
```

*Rysunek 16. Fragment kodu wykorzystującego funkcję InternetCheckConnectionA do weryfikacji połączenia z siecią Internet*

W tym przypadku, jeśli funkcja zwróci wynik negatywny (brak połączenia), malware przechodzi do obsługi tego stanu (np. kończy swoje działanie lub ukrywa funkcje).

Aby zneutralizować działanie tego mechanizmu, można zastąpić kluczowe instrukcje wywołujące funkcję InternetCheckConnectionA oraz analizujące jej wynik instrukcjami NOP. Po takiej modyfikacji malware ignoruje wynik sprawdzenia i zawsze przechodzi do dalszego kodu, zakładając, że połączenie internetowe jest dostępne. Rysunek numer 14 przedstawia fragment takiego kodu.

```
nop ; Usunięcie załadowania adresu URL
nop ; Usunięcie ustawienia opcji dwReserved
nop ; Usunięcie ustawienia flagi dwFlags
nop ; Usunięcie wywołania funkcji InternetCheckConnectionA
nop ; Usunięcie sprawdzenia wyniku
nop ; Usunięcie skoku na brak połączenia
```

*Rys. 17. Fragment kodu zastąpionego instrukcjami NOP*

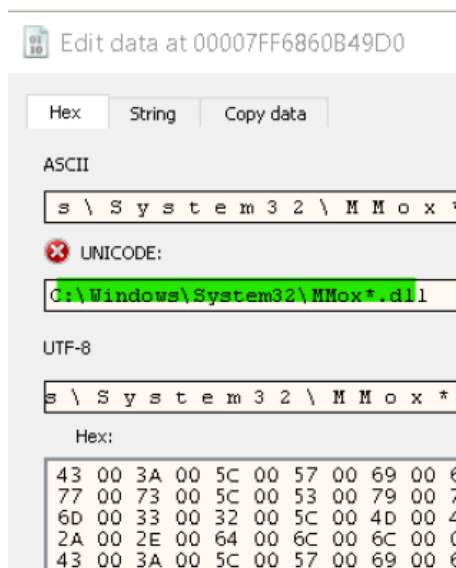
Zastąpienie instrukcji NOP to jedna z najprostszych i najszybszych technik wyłączenia zabezpieczeń, szczególnie przydatna w przypadku prostych mechanizmów antydebuggingowych. Niemniej jednak należy zachować ostrożność – nadmierne użycie NOP może prowadzić do utraty dostępu do innych części programu lub zakłócić jego działanie. Z tego powodu technika ta najlepiej sprawdza się jako rozwiązanie tymczasowe, które pozwala na szybkie obejście zabezpieczeń i kontynuację analizy.

## **METODY WPROWADZANIA ZMIAN**

Wprowadzenie zmian w kodzie złośliwego oprogramowania jest kluczowym etapem analizy, pozwalającym neutralizować mechanizmy antydebuggingowe i lepiej zrozumieć logikę działania programu. Dzięki odpowiednim technikom, takim jak modyfikacja logiki instrukcji, zamiana parametrów funkcji czy zastępowanie kodu instrukcjami NOP, analitycy mogą skutecznie obejść zabezpieczenia malware. W tym podrozdziale omówione zostaną praktyczne zastosowania zmiany, wykorzystując

narzędzia takie jak debugger x32.dbg, edytory hex oraz skrypty automatyzujące proces modyfikacji kodu.

1. Za pomocą debuggera - w debugerze (np. x64dbg) możemy znaleźć miejsce w pamięci, w którym przechowywany jest ciąg znaków VBox\*.dll, i zastąpić go np. ciągiem MMox\*.dll. Ważne, aby ciąg miał tę samą długość lub był odpowiednio dostosowany (np. wypełniony znakami null \0).



Rys. 18. Zmiana parametrów funkcji w x32dbg

2. Za pomocą hex edytora - w pliku binarnym można wyszukać ciąg znaków ASCII VBox\*.dll i zmienić go na MMox\*.dll. Warto pamiętać, że zmiana musi być dokładna, aby zachować strukturę danych w pliku. Taką zmianę można wykonać np. w edytorze: hexedit. Po otwarciu pliku należy odnaleźć konieczny do zmiany ciąg znaków (ctrl+s), a następnie zastąpić go odpowiednią wartością pamiętając o zachowaniu długości ciągu znaków.
3. Za pomocą kodu patchującego – istnieje opcja stworzenia krótkiego skryptu (np. w Pythonie), który to automatycznie zmienia odpowiednią wartość w pamięci lub pliku. Należy pamiętać, że w plikach binarnych (np. plikach wykonywalnych) dane są przechowywane w sposób bardzo uporządkowany, w formie kodu maszynowego, który procesor interpretuje bezpośrednio. Każdy bajt (czyli jedna wartość w systemie szesnastkowym) w pliku ma swoje miejsce i znaczenie w strukturze programu. Zmiana długość ciągu znaków w tym pliku, zmieni również pozycję bajtów, które następują po nim, co może prowadzić do uszkodzenia pliku. Rysunek numer 16 przedstawia prosty przykład skryptu podmieniającego wartości parametrów wraz z warunkiem sprawującym długość ciągu znaków.

```

def patch_file_simple(file_path, search_str, replace_str):
    # Sprawdza dlugosc znakow
    if len(search_str) != len(replace_str):
        print(f"Błąd: Ciągi '{search_str}' i '{replace_str}' muszą mieć tę samą długość!")
        return

    # Otwiera plik w trybie do odczytu binarnego
    with open(file_path, "rb") as file:
        data = file.read() # Wczytaj całą zawartość pliku

    # Zamienia wyszukiwany tekst na nowy
    patched_data = data.replace(search_str.encode(), replace_str.encode())

    # Zapisuje zmodyfikowany plik, jeśli coś się zmieniło
    with open(file_path, "wb") as file:
        file.write(patched_data)
    print(f"Zmieniono '{search_str}' na '{replace_str}' w pliku {file_path}")

file_path = "sample_binary.exe" # Ścieżka do pliku
search_str = "VBox*.dll"       # Ciąg znaków do znalezienia
replace_str = "MMox*.dll"      # Ciąg znaków na który zamienić

# Wywołanie funkcji
patch_file_simple(file_path, search_str, replace_str)

```

Rys. 19. Przykładowy skrypt Python podmieniający wartość VBox\*.dll na MMox\*.dll

## PODSUMOWANIE

W dynamicznie rozwijającej się cyberprzestrzeni techniki antysandboxowe i antydebugingowe są skutecznymi narzędziami w arsenale twórców złośliwego oprogramowania. Ich implementacja pozwala malware nie tylko ukrywać swoje szkodliwe działanie, ale również unikać analizy i wykrycia przez analityków bezpieczeństwa. W artykule omówiono najczęściej stosowane metody unikania analizy, takie jak detekcja środowisk wirtualnych, opóźnianie działania, weryfikacja połączenia z internetem czy rozpoznawanie debuggera.

Przedstawione techniki obejmowania mechanizmów ochronnych w malware - zmiana logiki funkcji, modyfikacja parametrów oraz zastąpienie instrukcji operacjami NOP są kluczowymi narzędziami w arsenale analityków. Choć każda z tych metod ma swoje ograniczenia, ich umiejętne zastosowanie pozwala zneutralizować część zabezpieczeń i skutecznie przeprowadzić analizę.

Artykuł ukazuje również, jak za pomocą debuggerów, edytorów hexadecymalnych i automatycznych skryptów można wprowadzać modyfikacje w złośliwym kodzie, aby lepiej zrozumieć jego mechanizmy. Dla analityków bezpieczeństwa kluczowe jest ciągle doskonalenie umiejętności w zakresie wykrywania i neutralizacji takich technik, co przyczynia się do zwiększenia skuteczności ochrony systemów przed cyberzagrożeniami.

Współczesne zagrożenia wymagają nie tylko znajomości technik ofensywnych stosowanych przez cyberprzestępców, ale również kreatywności w znajdowaniu i eliminowaniu ich mechanizmów obronnych. Dlatego walka z analizą malware pozostaje wyścigiem zbrojeń, w którym każde nowe odkrycie jest krokiem ku lepszemu zabezpieczeniu użytkowników i systemów.

## **BIBLIOGRAFIA**

1. Jurczyk M., Coldwind G. i in., Praktyczna inżynieria wsteczna. Metody, techniki i narzędzia, PWN, 2016.
2. Sikorski M., Honig A., Praktyczna Analiza Malware Przewodnik po usuwaniu złośliwego oprogramowania, PWN, 2021.

# ZABEZPIECZANIE DANYCH ULOTNYCH W SYSTEMACH WINDOWS

## VOLATILE DATA COLLECTION FROM WINDOW SYSTEM

Grzegorz TWOREK <sup>1</sup>

**Streszczenie:** Niniejszy rozdział podsumowuje wykład oraz warsztaty przeprowadzone podczas konferencji naukowej „Przestępczość Teleinformatyczna XXI” odbywającej się w maju 2024 na Akademii Marynarki Wojennej im. Bohaterów Westerplatte w Gdyni.

**Słowa kluczowe:** incydent, dane ulotne, Windows, SysInternals, dowód.

**Summary:** This chapter summarizes the lecture and workshop conducted during the academic conference “ICT Crime XXI” held in May 2024 at the Bohaterów Westerplatte Naval Academy in Gdynia.

**Keywords:** incident, ephemeral data, Windows, SysInternals, evidence.

Opracowanie skupia się na praktycznym scenariuszu typowym dla zabezpieczania danych podczas incydentów bezpieczeństwa informacji, co w praktyce oznacza zbieranie danych zgodnie z wolą administratora lub co najmniej uprawnionego użytkownika danego komputera.

Od strony teoretycznej, zabezpieczanie danych opisane zostało w wielu opracowaniach, z których na szczególną uwagę zasługuje dokument RFC3227 Guidelines for Evidence Collection and Archiving (Brezinski & Killalea, 2002). Dokument ten opisuje między innymi Order of Volatility, czyli kolejność, w jakiej potencjalnie użyteczne w informatyce śledczej dane znikają z badanego systemu, tak w wyniku jego normalnego działania, jak i w wyniku przeprowadzonych działań mających zabezpieczyć materiał dowodowy.

Przedstawione w czasie konferencji podejście stanowi pewne uproszczenie, wynikające ze względów praktycznych oraz z ograniczenia zakresu działań wyłącznie do systemów Windows. Przekłada się to na ułatwione zastosowanie praktyczne, co było świadomym założeniem.

W przypadku zabezpieczania danych w systemach Windows, zastosować można podział, w którym użyteczne i potencjalnie możliwe do pozyskania dane przechowywane są w pamięci masowej w sposób, który pozwala na dostęp do nich wyłącznie na podstawie nośnika, również po wyłączeniu komputera, oraz na dane, które w momencie wyłączenia komputera traczone są bezpowrotnie (dane ulotne). Co istotne, w przypadku danych

---

<sup>1</sup> Microsoft, grzegorz.tworek@stderr.pl.

ulotnych nie chodzi wyłącznie o zawartość pamięci RAM. Choć faktycznie to pamięć RAM odpowiada za realizację mechanizmów związanych z danymi ulotnymi i choć to charakter pamięci RAM powoduje, że jej zawartość staje się niedostępna po wyłączeniu komputera, to analiza danych wyłącznie na podstawie binarnej kopii pamięci (zrzutu pamięci) jest niezwykle trudna, czasochłonna i w praktyce bardzo ograniczona. Pozyskany w ten sposób materiał będzie zazwyczaj niekompletny. Dla ilustracji podać można przykład pamięci podręcznej protokołu DNS (DNS Cache). Oczywiście takie dane znajdują się w pamięci RAM, jednak wydobyć ich ze zrzutu pamięci będzie znacząco trudniejsze niż pozyskanie w wyniku zapytania zrealizowanego przy pomocy mechanizmów API (funkcji `DnsQuery_W()` wykorzystywanej na przykład przez polecenie „`ipconfig /displaydns`”) w systemie, który działa i komunikuje się z operatorem.

Dane nieulotne (zapisane na dyskach) są stosunkowo wygodnym materiałem dowodowym. Mogą być analizowane wielokrotnie, przez różnych ekspertów, lokalnie oraz zdalnie, również po pewnym czasie wynikającym na przykład z pozyskania nowych informacji lub opracowania nowych technik badawczych. Praktycznym ograniczeniem jest jedynie objętość pamięci masowej użytej do przechowania obrazów dysków. W przypadku danych ulotnych (z wyjątkiem bardzo wygodnych pod tym względem maszyn wirtualnych), analiza wykonywana może być tylko do czasu restartu komputera, który zazwyczaj wynika z presji właściciela systemu, chcącego jak najszybciej przywrócić jego zgodne z oczekiwaniami funkcjonowanie. Oznacza to, że dane ulotne zabezpieczone zostać powinny sprawnie, w sposób prawidłowy oraz (o ile to możliwe) powtarzalny, aby ułatwić ich analizę oraz porównanie między systemami.

Znacząca część danych ulotnych dostępna jest dzięki wbudowanym w system narzędziom, również pracującym w wierszu poleceń, co ułatwia zapisywanie ich wyników do plików tekstowych. Pozostałe potencjalnie użyteczne dane wymagają aplikacji niedostępnych w systemie operacyjnym, często jednak wystarczy ograniczenie się wyłącznie do narzędzi Sysinternals, dystrybuowanych i podpisanych cyfrowo przez Microsoft. Teoretycznie, możliwe jest pozyskanie niemal wszystkich danych ulotnych przy pomocy skryptów PowerShell, ale w praktyce podejście takie wydaje się bezzasadne. Skuteczne skrypty są zbyt skomplikowane, aby wprowadzać je ręcznie, co oznacza, że i tak konieczne jest posłużenie się zewnętrznym nośnikiem, podobnie jak w przypadku gotowych narzędzi. Ponadto, sposób działania PowerShell powoduje automatyczne zapisywanie wielu danych na dysku, co potencjalnie może uszkodzić (zatrzeć) inne wartościowe dane, zanim zostaną zebrane. Narzędzia firm trzecich służące do analizy danych skonstruowane zazwyczaj są w taki sposób, aby zminimalizować ich negatywny wpływ na inne potencjalnie użyteczne obszary.

Podczas użycia narzędzi Sysinternals, wskazane jest zachowanie ostrożności wynikające ze sposobu ich działania. W szczególności należy zwrócić uwagę na dwa aspekty:

1. Użycie każdego narzędzia wymaga manualnego lub automatycznego zaakceptowania umowy licencyjnej. Zaakceptowanie takie odnotowywane jest w rejestrze, co z kolei może prowadzić do fałszywie pozytywnych wyników, jeżeli później (również w wyniku analizy danych nieulotnych) wykonane zostanie badanie pod kątem użycia tych narzędzi.
2. Część narzędzi występuje w wersji 32 oraz 64 bit. Wersje 32 bit są tak naprawdę połączeniem narzędzi 32 oraz 64 bit, a ich użycie na 64 bitowym systemie powoduje, że z pliku binarnego wypakowywana jest wersja 64 bit, która następnie jest uruchamiana jako proces potomny. Oznacza to, że wersje 32 bit dla zebrania tych samych danych muszą wykonać znacząco bardziej złożone działania, potencjalnie niszczące więcej śladów, które nie zostały jeszcze zabezpieczone. Ponieważ w chwili obecnej większość systemów to systemy 64 bit, należy przyjąć, że do pozyskiwania danych ulotnych powinno się używać wyłącznie 64 bitowych narzędzi Sysinternals.

Omawiając konkretne dane ulotne, których zebranie może być zasadne w praktycznych scenariuszach obsługi incydentu, wymienić należy przede wszystkim:

- 1) Listę procesów wraz z załadowanymi bibliotekami przy pomocy polecenia: "tasklist /v > raport01.txt" oraz "tasklist /m > raport02.txt" lub zewnętrznym narzędziem "listdlls64.exe -v -accepteula > raport03.txt". Zalecenie użycia zewnętrznego narzędzia wynika z faktu, że pozyskanie listy procesów systemowym narzędziem tasklist jest ograniczone w dwóch obszarach:
  - a) Wymienione są tylko nazwy bibliotek a nie pełne ścieżki do nich
  - b) Standardowa wersja narzędzia niepoprawnie identyfikuje biblioteki załadowane do procesów 32 bit.
- 2) Zawartość cache dns "ipconfig /displaydns > raport04.txt". Cache DNS zawiera również wpisy z pliku hosts, nawet jeżeli dana nazwa nie była nigdy rozwiązywana przez badany system. Należy na to zwrócić uwagę podczas analizy.
- 3) Zawartość cache arp: "arp -a > raport05.txt".
- 4) Listę połączeń sieciowych: "netstat -ano > raport06.txt".
- 5) Zawartość środowiska: "set > raport07.txt". Środowisko teoretycznie jest indywidualną cechą każdego procesu i może się między procesami różnić, jednak w praktyce różnica ta nie zmienia sposobu analizy dla faktycznie spotykanych przypadków.
- 6) Listę certyfikatów root: "certutil -store root > raport08.txt".
- 7) Listę kont: "wmic netlogin > raport09.txt". Narzędzie WMIC może zostać usunięte z przyszłych (lub testowych) wersji systemu, w chwili obecnej jest jednak wszędzie dostępne.
- 8) Listę sesji "klist sessions > raport10.txt".

- 9) Klucze BitLocker: "manage-bde.exe -protectors -get c: >> raport11.txt" i analogicznie dla każdego woluminu w systemie. Dane zapisywane w pliku należy traktować jak dane wrażliwe.

Jeżeli wchodzi w grę użycie narzędzi Sysinternals, dodatkowo można pozyskać:

- 10) Uchwyty do obiektów: "handle64.exe" -a -accepteula > raport12.txt".  
11) W trakcie badania warto zarejestrować również łatwo dostępne dane, które są możliwe do pozyskania z obrazów dysków, jednak są istotnie trudniej dostępne, takie jak: czas systemowy, nazwę komputera, czy czas startu komputera.

Teoretycznie, zrzut pamięci (dump) również jest sposobem zabezpieczenia danych ulotnych, jednak należy rozważyć, czy koszt jego przechowywania jest usprawiedliwiony. Typowe zrzuty pamięci mają objętość wielu gigabajtów i są kilka rzędów wielkości obszerniejsze niż wszystkie pozostałe dane ulotne. Jeżeli przechowywanie zrzutów nie jest problemem, to warto również je wykonać, nawet jeżeli ich analiza nie jest objęta przyjętym zakresem prac.

W trakcie prowadzonych przez wiele lat działań związanych z obsługą incydentów, użyteczne okazało się zautomatyzowanie procesu zbierania wszystkich możliwych do zidentyfikowania danych ulotnych. W tym celu stworzone zostało narzędzie Volatile Data Collector. Narzędzie to jest publikowane na licencji GPL 3.0 i jest dostępne pod adresem <https://github.com/gtworek/VolatileDataCollector> wraz z przykładowym raportem oraz kodem źródłowym w języku C. Wszystkie omawiane w niniejszym opracowaniu dane ulotne zbierane są automatycznie a narzędzie działa w taki sposób, aby w jak najmniejszym stopniu uszkadzać niezbrane jeszcze dane.

## **BIBLIOGRAFIA**

1. <https://github.com/gtworek/VolatileDataCollector>
2. RFC3227 Guidelines for Evidence Collection and Archiving (Brezinski & Killalea, 2002)

**OPRACOWANIE WPŁYWU KORZYSTANIA ZE SMARTFONÓW PRZEZ  
UCZNIÓW PAŃSTWOWYCH SZKÓŁ PODSTAWOWYCH NA TERENIE  
GMINY MIASTA KRAKÓW.**

A STUDY ON THE IMPACT OF MOBILE PHONE USAGE BY STUDENTS OF  
PUBLIC PRIMARY SCHOOLS IN THE MUNICIPALITY OF KRAKOW.

**mgr Paulina TUREK**

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie

**prof. dr hab. Piotr DELA**

Uniwersytet Kaliski

**Streszczenie:** Artykuł omawia wpływ telefonów komórkowych na środowisko szkolne, analizując zarówno korzyści, jak i wyzwania związane z ich użytkowaniem. Autorzy artykułu zwraca uwagę na często odmienny punkt widzenia nauczycieli i uczniów względem wprowadzenia zakazu korzystania z telefonów w szkołach. Artykuł po raz pierwszy uwzględnia tak młodą grupę internautów z krakowskich szkół, zestawiając ich odpowiedzi z odpowiedziami nauczycieli. Wnioski artykułu wskazują na potrzebę wprowadzenia koniecznych regulacji, które zadbają o dobrostan psychiczny, fizyczny i społeczny uczniów a także o bezpieczeństwo nauczycieli.

**Słowa kluczowe:** cyberbezpieczeństwo, telefon, szkoła, dobrostan, smartfon

**Summary:** The article discusses the impact of mobile phones on the school environment, analyzing both the benefits and challenges associated with their use. The author highlights the often differing perspectives of teachers and students regarding the introduction of a ban on the use of phones in schools. The article, for the first time, includes such a young group of internet users from Krakow's schools, comparing their responses with those of teachers. The findings of the article indicate the need to introduce necessary regulations that ensure the mental, physical, and social well-being of students as well as the safety of teachers.

**Keywords:** cybersecurity, mobile phone, school, well-being, smartphone

## WSTĘP

Po zachłyśnięciu się zaletami, które płyną z nowych technologii w edukacji, przyszedł czas na reelekcję poprzedzoną licznymi obserwacjami. Niestety, faza zachwytu przerodziła się w fazę obaw i wątpliwości spowodowanych telefonami z dostępem do Internetu przynoszonymi do szkół. Na dobre rozgorzała dyskusja czy telefony są konieczne i niezbędne w procesie edukacji. Najnowszy Raport UNESCO [19] podaje, że dobre, bezstronne dowody na wpływ technologii edukacyjnej są rzadkością. Istnieje niewiele solidnych dowodów na dodatkową wartość cyfrowej technologii w edukacji. Pojawia się też termin "uzależnienie od smartfonów" (SPA), aby opisać zachowania uzależnieniowe związane z używaniem smartfonów oraz związane z nimi fizyczne i psychospołeczne upośledzenia [9].

Nowe technologie wcześniej pojawiają się w krajach lepiej rozwiniętych i z tych krajów, również szybciej płyną obserwacje i wnioski. Problem jest trudny i skomplikowany, więc nie wszystkie kraje są jednomyślne ale można zaobserwować jednoznaczną tendencję do wprowadzania ograniczeń z korzystania z telefonów na terenie szkoły.

Francja od 2025 roku bezwzględnie zakazuje używania telefonów komórkowych w szkołach podstawowych i gimnazjach. Uczniowie będą musieli oddawać telefony do depozytu, dopiero po zakończonych zajęciach, będą mogli je odebrać. Zakaz obowiązuje również w szkołach w całej Holandii. Włochy zakazały korzystania z telefonów komórkowych i urządzeń mobilnych w przedszkolach, szkołach podstawowych oraz gimnazjach, dodatkowo zabroniono również korzystania z tych urządzeń w celach dydaktycznych. Podobne rozwiązania wprowadził rząd Węgier. Najbardziej restrykcyjnym krajem wydaje się Australia. To pierwszy kraj na świecie, który zakazał korzystania z mediów społecznościowych osobom, które nie ukończyły 16 lat. Od 2020 uczniowie w szkole podstawowej nie mogą posiadać telefonów komórkowych podczas całego pobytu w szkole. A uczniowie szkoły średniej muszą mieć telefony wyłączone i schowane poza zasięgiem wzroku. Pojawiają się również połowiczne rozwiązania. W Belgii, zakaz korzystania ze smartfonów obowiązuje uczniów szkół podstawowych i średnich na razie tylko we francuskojęzycznych regionach oraz w Brukseli. W Hiszpanii zakaz wprowadziły niektóre regiony autonomiczne. W Finlandii zakaz używania telefonów obejmuje uczniów w Helsinkach. Zakaz, wprowadzają również kolejne stany w USA.

W Polsce, Niemczech, Danii, Szwajcarii, Portugalii i Chorwacji nie ma przepisów ogólnokrajowych regulujących tę kwestię. W Polsce dyrektorzy szkół mają możliwość włączenia odpowiednich zapisów do statutu. Rozwiązanie to jest szeroko krytykowane przez gremia szkolne, gdyż nie daje wsparcia w skutecznym egzekwowaniu zakazu korzystania z telefonów w szkole [16].

Celem przeprowadzonych badań jest dostarczenie wskazówek dla dyrektorów szkół, nauczycieli, rodziców i decydentów, poprzez stworzenie optymalnych regulacji i strategii dotyczących wykorzystania technologii w edukacji oraz w podjęciu

odpowiednich kroków mających na celu dobro i ochronę dzieci. W artykule przedstawiono problemy badawcze, które odnoszą się do kontekstu społecznego, edukacyjnego i technologicznego a także zdrowia psychicznego dzieci i młodzieży. Poruszone zostały również kwestie dotyczące regulacji i ich skuteczności egzekwowania zakazu korzystania z telefonów w szkole.

Zaprezentowane wyniki badań pokazują w jakich punktach zgadzają się ze sobą nauczyciele i uczniowie, a w jakich wprost przeciwnie. Jak obie te grupy postrzegają korzyści i zagrożenia płynące z możliwości korzystania z telefonów w szkole.

W niniejszym artykule przedstawiono wyniki badań, które po raz pierwszy zostały przeprowadzone na grupie tak młodych użytkowników telefonów w szkole. Badania przeprowadzono na grupie 1.043 uczniów klas 4-8 szkół podstawowych oraz grupie nauczycieli (201 osób) z krakowskich szkół. Odpowiedzi młodych respondentów zostały skonfrontowane z obserwacjami nauczycieli.

## **STAN BADAŃ**

W niniejszym artykule określenie „telefon” nie odnosi się tylko do urządzenia, z którego można dzwonić. Autorzy wymiennie będzie używać słowa telefon i smartfon jako urządzeń mobilnych, elektronicznych, na stałe podłączonych do Internetu.

O ile zagadnieniu problematycznego używania Internetu przez dzieci i młodzież od smartfonów poświęcono wiele artykułów, już od pierwszej dekady 2000 roku, to temat korzystania z telefonów przez uczniów w szkołach, pojawia się w literaturze dopiero w drugiej dekadzie 2000 roku, gdy telefony zaczynają pojawiać się na przerwach i lekcjach. Pierwsza fala zakazów zostaje wprowadzona pod koniec lat 80. XX wieku w Stanach Zjednoczonych Ameryki Północnej, kiedy wiele sektorów szkolnych zaczęło wprowadzać przepisy mające na celu uniemożliwienie uczniom korzystania z telefonów komórkowych i pagerów w szkołach [19]. Dziewięć lat po wprowadzeniu na rynek iPhone'a pojawiają się głosy, że używanie urządzeń mobilnych w klasie, może być rozpraszające i szkodliwe. Zostają zauważone: częste rozproszenie po tym gdy pojawiają się powiadomienia na ekranie, niepoprawne zachowania a także nieuczciwość akademicka. Zachowania te, są korelowane ze spadkiem umiejętności myślenia poznawczego, interakcji społecznych i zmniejszeniem czasu koncentracji, finalnie z używaniem urządzeń mobilnych w klasie i gorszymi ocenami [4].

Równocześnie w 2019 roku greccy naukowcy z Ionian University [11] publikują artykuł pt.: Smartphones at Schools? Yes, Why not? W którym dowodzą, że telefony komórkowe są uważane za odpowiednie narzędzie do procesu nauczania ze względu na ich mały rozmiar, przenośność, przystępność cenową, dostępność, potencjał do angażowania użytkowników wszędzie i w każdej chwili, a także ich zdolność do wspierania szybkiej interakcji multimedialnych aplikacji. Podkreślają również, że możliwość tworzenia własnych treści jest bardzo istotna dla wzmocnienia kreatywności uczniów i nauczycieli.

W 2021 roku autorzy *Cell Phones, Student Rights, and School Safety: Finding the Right Balance* [17], jako jedni z pierwszych, zauważają konieczność znalezienia równowagi w korzystaniu przez uczniów z telefonów komórkowych w szkołach. Podkreślają, że jest to trudne wyzwanie, które wymaga podejścia całej społeczności, w tym rodziców, nauczycieli, rad szkolnych, ministerstw edukacji i szerszej świadomości społecznej na temat wpływu telefonów komórkowych na osiągnięcia i dobrostan młodzieży.

Natomiast badania przeprowadzone na Tajwanie [20] wśród klas piątych i szóstych szkoły podstawowej wykazały, że uczniowie z grupy intensywnego użytkowania smartfonów przewyższali akademicko tych z grupy niskiego użytkowania smartfonów. Z tą opinią polemizuje artykuł pt. „Do we need a digital school uniform? Arguments for and against a smartphone ban in schools” autorstwa Christian Montag i Jon D. Elhai [14]. Naukowcy zauważają, że często wielkości efektów nie są duże, ale jednak można dostrzec w wynikach badań utratę produktywności u osób „uzależnionych” od smartfonów/mediów społecznościowych oraz niższe oceny u osób z wyższym obiektywnym użyciem smartfonów. Badacze podkreślają, że zakazy używania smartfonów mogą być szczególnie istotne dla najmłodszych uczniów uczęszczających do szkół podstawowych oraz dla tych w okresie dojrzewania. Raport UNESCO z 2023 roku tylko potwierdza tezę, że jedynie technologia, która ma wyraźną rolę we wspieraniu nauki, może być dozwolona w szkole [19]. Podejście to podzielają nauczyciele, psychologowie i dyrektorzy krakowskich szkół na konferencji pt. „O czym marzą dziewczynki a czego się boją? Dbamy o zdrowie psychiczne krakowskich uczennic” [16].

W *Smartphones and Learning: Evaluating the Focus of Recent Research* [8] pojawia się stwierdzenie, że w literaturze pokazane i obecne są, korzystne zastosowania smartfonów, jednak są one znacznie mniej powszechne i rzadziej cytowane. W przeglądzie literatury poświęconej smartfonom i korzystaniu z nich przez dzieci w szkołach podstawowych [3], autorzy udowadniają, że dzieci biorące udział w zadaniach matematycznych lub edukacyjnych z wykorzystaniem urządzeń mobilnych osiągały lepsze wyniki w zakresie umiejętności liczenia lub czytania i pisania, niż te używające innego urządzenia (np. laptopa lub komputera stacjonarnego) lub niekorzystające z żadnego urządzenia (działania klasowe jak zwykle). Badacze z Wielkiej Brytanii oraz Tanzanii podkreślają jednak, by te wyniki interpretować ostrożnie, gdyż zadania i warunki klasowe różniły się dość znacznie, dlatego potrzebne są dalsze badania, aby lepiej zrozumieć potencjalny wpływ urządzeń mobilnych na uczniów w szkołach. Autorzy [8] nie są zwolennikami tezy, że smartfony powinny być zakazane w środowiskach edukacyjnych, ale podkreślają, że temat dotyczy uczniów, którzy mają zdrowy i umiarkowany związek ze smartfonem. Pojawia się jednak zasadnicze pytanie, które brzmi: Jak wygląda zdrowy i umiarkowany związek ucznia ze smartfonem? Tutaj, zauważają konieczność pogłębienia badań. Podobny dysonans poznawczy, wyróżniają względem uczniów i ich telefonów, także Christian Montag i Jon D. Elhai [14]. Wskazują na dowody badawcze, które pokazują, że korzystanie ze smartfona jest związane z

lepszym samopoczuciem, ale równocześnie to samo badanie wykazało, że większe natężenie korzystania ze smartfona koreluje z gorszym samopoczuciem.

W Nowej Zelandii w 2024 roku przeprowadzono badania [5] na grupie nauczycieli i uczniów. Obie grupy były za regulacją używania telefonów komórkowych na poziomie szkoły, ale równocześnie były też mniej przychylnie całkowitemu zakazowi. Powody dla bardziej rygorystycznych regulacji dotyczących używania telefonów komórkowych w szkołach zauważają natomiast badacze z Australii w pracy Evidence for and against banning mobile phones in schools: A scoping review [2]. Dowodzą, że telefony w szkołach przynoszą uczniom trudności w nauce, zakłócenia w czasie odpoczynku oraz służą jako narzędzie do ściągania podczas egzaminów. Badanie wskazało powody dla bardziej rygorystycznych regulacji dotyczących używania telefonów komórkowych w szkołach. Tematykę używania telefonów w szkołach zbiorczo podsumowuje Raport UNESCO z 2023 roku [19]. Badanie wykazało, że telefony komórkowe rozpraszają uczniów w nauce. Nawet samo posiadanie telefonu komórkowego w pobliżu z przychodzącymi powiadomieniami jest wystarczające, aby uczniowie tracili uwagę na zadaniu, które mają wykonywać. Pojawiają się także obawy dotyczące prywatności danych i bezpieczeństwa (aplikacje zbierają dane użytkowników) oraz dobrostanu, które stanowią podstawę debat na temat używania niektórych technologii w szkołach, szczególnie przez uczniów w młodym wieku. Sara Abrahamsson z Norweskiego Instytutu Zdrowia Publicznego w swojej pracy formułuje wniosek, że zakaz korzystania z telefonów komórkowych w szkołach to najlepsza, darmowa profilaktyka dla zachowania dobrego zdrowia psychicznego uczniów, zwłaszcza dziewcząt. Ten aspekt potwierdzają również badania dr Romana Soleckiego [18] oraz Raport z Konferencji pt. „O czym marzą dziewczynki?..” [16] Zakaz używania telefonów w szkole znacząco zmniejsza problemy ze zdrowiem psychicznym szczególnie u dziewcząt, a akty agresji - u obu płci [1]. Ponadto, badaczka zauważa, że poprawiają się średnie ocen dziewcząt i wzrasta ich prawdopodobieństwo uczęszczania do akademickiej szkoły średniej. W 2024 roku Jonathan Haidt, amerykański psycholog społeczny, wydaje pozycję pt. „The Anxious Generation..”[7], która rozgrzewa temat telefonów w szkołach do czerwoności. Początkowo zwolennik smartfonów, po przeprowadzonych badaniach formułuje cztery normy, które jego zdaniem powinny zostać wdrożone dzięki współpracy polityków, nauczycieli, rodziców i samych dzieci. Nr 1: korzystanie ze smartfonów możliwe dopiero od szkoły średniej. Nr 2: zakaz korzystania z social mediów przed 16. rokiem życia. Z takim działaniem zgadza się 74% krakowskich nauczycieli (45% - tak, 29% - zdecydowanie tak). Nr 3: korzystania ze smartfonów w szkołach – stanowczo zabronione. Nr 4: więcej swobodnej i wolnej zabawy, więcej odpowiedzialności dla dzieci i młodzieży w rzeczywistym świecie [7]. Za większą niezależnością w realnym świecie dla dzieci zagłosowało 86% nauczycieli (29% - tak, 47% - zdecydowanie tak). Zważywszy na fakt, że część nauczycieli jest również rodzicami, wydaje się to być ważny argument prowadzący do dobrostanu dzieci.

Zgodnie z Raportem UNESCO [19] prawie jedno na cztery kraje wprowadzają zakazy używania smartfonów w szkołach w przepisach lub politykach. Zakazy są bardziej powszechne w Azji. Zarówno Bangladesz, jak i Singapur zakazują używania smartfonów na lekcjach, ale nie w szkołach. Francja zakazuje używania smartfonów, chyba że są wykorzystywane ściśle do celów pedagogicznych lub wspierania dzieci z niepełnosprawnościami. Niektóre kraje dla odmiany, zakazały używania konkretnych aplikacji w środowiskach edukacyjnych z powodu obaw dotyczących prywatności. Dania i Francja zabroniły korzystania z Google Workspace, podczas gdy Niemcy zakazały produktów Microsoft w niektórych stanach. W Stanach Zjednoczonych niektóre szkoły i uniwersytety zaczęły zakazywać TikToka [19]. W Polsce, szkoły, zazwyczaj jednak tylko prywatne, posiadają szafki czy pudła na telefony dzieci. Najczęstsza i tym samym najmniej skuteczna forma obowiązująca w szkołach publicznych, to – wyłączony telefon, który podczas pobytu w szkole powinien znajdować się w plecaku ucznia. Ministerstwo Edukacji Narodowej, decyzję odnośnie korzystania z telefonów w szkołach zostawiło – dyrektorom szkół, którzy jedynie w statucie mogą dokonać odpowiedniego zapisu a następnie egzekwować zakaz. W efekcie, dyrektorzy szkół zostają sami na „polu walki” z uczniami a często także – rodzicami. Jak wynika z Raportu „O czym marzą dziewczynki?...” [16] nauczyciele i dyrektorzy krakowskich szkół marzą o ogólnym ujednoczeniu zapisów. Od kilku lat pojawiają się inicjatywy prowadzone przez fundacje, min. Instytut Spraw Obywatelskich, które monitorują sytuację oraz popierając ją wynikami badań, apelują do władz o wprowadzenie ogólnopolskiego zakazu korzystania z telefonów w szkołach. Ograniczenie, oczywiście, ma wyłączać sytuacje edukacyjne czy ratujące życie (wsparcie medyczne dla uczniów chorych np. na cukrzycę). 2 grudnia 2024 roku Rafał Górski, prezes zarządu Instytutu Spraw Obywatelskich, prowadzący kampanię obywatelską „Ratuj dzieci!” wraz z ośmioma profesorami, terapeutami i dyrektorem szkoły podstawowej wystosowali „Apel VIP do minister Barbary Nowackiej w sprawie smartfonów” [6]. Aktywiści zwrócili się do minister z apelem o wprowadzenie jednolitych zasad higieny cyfrowej dotyczących używania telefonów komórkowych i innych urządzeń ekranowych w żłobkach, przedszkolach i szkołach podstawowych. Uważają, że zasady powinny dotyczyć zarówno dzieci, młodzieży, jak i personelu placówek. Opowiadają się za centralną, rządową, regulacją. Wskazują na fakt, iż brak jednolitych zasad higieny cyfrowej naraża dzieci na lawinowy wzrost negatywnych skutków. Organizatorzy konferencji „UWAGA! Smartfon” [12] zorganizowanej po raz pierwszy w 2022 roku również szukali odpowiedzi na pytania: jak technologia wpływa na społeczeństwo?, czy smartfony ułatwiają rodzicielstwo? jakie rozwiązania powinny stosować szkoły, aby radzić sobie z nadużywaniem elektroniki?

Problem zakazu korzystania z telefonów w szkołach w Polsce, wydaje się więc być dość nowy i mało opracowany w literaturze. Natomiast na co dzień dla nauczycieli [16] i świadomych rodziców, jest to temat palący już od dobrych kilku lat. Pierwsze, lokalne, badania przeprowadził w 2017 roku Instytut Badawczy przygotowując Raport z Korzystania z urządzeń elektronicznych oraz z Internetu przez dzieci i młodzież [10].

Zostały zrealizowane badania z dziećmi, młodzieżą oraz nauczycielami z Krakowa, na temat korzystania z telefonów komórkowych, tabletów, komputerów, Internetu, mediów społecznościowych, gier komputerowych i konsolowych. We wnioskach znalazło się podsumowanie, które podkreśla, że już w roku 2017 telefon komórkowy jest najbardziej popularnym urządzeniem elektronicznym z którego im starsza młodzież, tym częściej korzysta podczas lekcji. O zagrożeniach wynikających ze zbyt intensywnego korzystania z Internetu przeczytamy zarówno w Raporcie autorstwa dr Romana Soleckiego [18] jak i w Raporcie Nastolatki 3.0 [15]. Znajdziemy tam informacje, że w 2023 roku prawie co trzeci nastolatek (31%) wykazuje się wysokim natężeniem wskaźników problematycznego użytkowania Internetu (PUI), a ośmiu na stu – bardzo wysokim (8,3%, wzrost względem 2020 r. o 5,1 pp.) [15]. Dr Roman Solecki zwraca uwagę, że zbyt intensywne korzystanie z Internetu przez uczniów, szczególnie wtedy, gdy zaczyna zastępować realne kontakty rówieśnicze, wykazuje związek z takimi zaburzeniami psychicznymi, jak depresja i uzależnienie. Zdaniem autora, kluczem do dobrostanu psychicznego, fizycznego i społecznego młodych ludzi jest poczucie sensu życia, które jest jednym z najsilniejszych czynników chroniących przed zaburzeniami i uzależnieniem [18]. Jednak żaden z powyższych raportów nie porusza problemu korzystania z telefonów w szkołach. Temat ten został dostrzeżony i omówiony przez pedagogów, psychologów, nauczycieli i dyrektorów krakowskich szkół podczas warsztatów i konferencji pt. „O czym marzą dziewczynki a czego się boją. Dbamy o zdrowie psychiczne krakowskich uczennic” zorganizowanej przez Urząd Miasta Krakowa i Fundację Try IT na Wydziale Informatyki Akademii Górniczo-Hutniczej. Nauczyciele chcą pomagać swoim uczniom, jednak potrzebują konkretnego wsparcia ze strony rodziców i instytucji. Chcą wsparcia na trzech poziomach: współpraca szkoła – rodzice, kształtowanie świadomości i krytycznego myślenia wśród uczniów a przede wszystkim rozwiązań instytucjonalnych na wyższym szczeblu o które to, apeluje właśnie Rafał Górski [6]. Systemowy zakaz korzystania ze smartfonów w szkołach w całej Polsce (poza sytuacjami edukacyjnymi i monitorującymi zdrowie ucznia), wydaje się być koniecznością w osiągnięciu celu – zdrowia psychicznego, fizycznego i społecznego młodego pokolenia.

## **METODOLOGIA**

W badaniu wzięły udział następujące grupy z krakowskich szkół podstawowych: uczniowie: klas czwartych: 288 ankiet; piątych: 410 ankiet; szóstych: 97 ankiet; siódmych: 163 ankiet; ósmych: 88 ankiet. Nauczyciele: przeprowadzono 186 ankiet, w tym wychowawcy: 72 ankiety; psychologowie: 3 ankiety; pedagodzy: 11 ankiet; dyrektorzy, wicedyrektorzy: 13 ankiet. Sumarycznie w badaniu wzięło udział 1.046 uczniów oraz 211 nauczycieli z krakowskich szkół podstawowych.

Badania były prowadzone metodą ankiety online. Ankiety były samodzielnie wypełniane przez respondentów. Były anonimowe i całkowicie dobrowolne. Dzieci wypełniały ankietę na lekcji informatyki pod opieką nauczyciela, którego rola sprowadzała się do zaprezentowania tematyki badania, zachęcenia do wzięcia udziału w

badaniu, ewentualnie do wyjaśnienia wątpliwości, które mogły pojawić się podczas uzupełniania ankiety.

Ankieta dla nauczycieli stanowiła odrębne narzędzie badawcze. Niektóre z pytań dla nauczycieli celowo pokrywała się z pytaniami dla dzieci. Tak przygotowane narzędzia pozwalają na wspólną analizę odpowiedzi respondentów.

## **ANALIZA SZCZEGÓŁOWA**

### ***Charakterystyka badanych***

Do badania zostały zaproszone dzieci, które brały udział w warsztatach z cyberbezpieczeństwa pt. „Cyfrowy Świat” finansowanych przez Urząd Miasta Krakowa a organizowanych przez Fundację Try IT. W ankiecie wzięły udział 503. dziewczynki i 543. chłopców. W tych samych szkołach poproszono o udział w ankiecie również nauczycieli.

### ***Korzystanie z telefonów przez dzieci***

Największa grupa respondentów deklaruje, że pierwszy telefon komórkowy otrzymała w wieku ośmiu lat (239 osób, tj. 23%). Kolejno: dziewięciolatkowie (233 osoby, tj. 22%) i siedmiolatkowie (211 dzieci, tj. 20%). 166 osób (16%) przyznało, że swój pierwszy smartfon otrzymało poniżej 7. roku życia. A tylko 6 osób (1%) zadeklarowało, że telefon komórkowy otrzymało po 12. roku życia. Grupa 21. dzieci (2%) w chwili wypełniania ankiety nie miała jeszcze swojego telefonu. Wyniki ankiety pokrywają się z danymi zaprezentowanymi w Raporcie NASK Natolatki 3.0 [15], które wskazują, że średni wiek otrzymania pierwszego telefonu z dostępem do Internetu wynosi 8 lat i 5 miesięcy. Dzieci jednak już we wcześniejszym wieku korzystają ze smartfonów, najczęściej są to telefony rodziców. 80% respondentów podaje taką odpowiedź. Korzystając z telefonów rodziców dzieci oglądały bajki i filmy (70%), grają w gry (61%), słuchają muzyki (33%) a 39% dzieci używało telefonów do dzwonienia.

### ***Zasady korzystania z telefonów komórkowych przez dzieci w domu***

Na pytanie „Czy masz ustawiony przez rodziców limit dzienny na telefonie?” 43% dzieci odpowiedziało: „Nie, nie mam żadnego limitu”. Drugą grupą pod względem ilości głosów, jest grupa dzieci, która deklaruje, że ma ustalony limit czasu na telefonie i go przestrzega – 39% respondentów. Dwie najmniejsze pod względem liczebności głosów grupy deklarują: „Tak, mam ustalony limit ale go nie przestrzegam” – 4% i „Nie mam telefonu z Internetem” – 3%. Podobnie prezentują się dane Raportu NASK Nastolatki 3.0 [15] „Ponad połowa nastolatków (53%) twierdzi, że ich rodzice nie ustalają żadnych zasad dotyczących korzystania z Internetu w zakresie czasu i dostępu do treści”. Na pytanie czy i w jaki sposób rodzice kontrolują czas dzieci spędzony w Internecie, największa grupa respondentów odpowiada, że kontrola odbywa się poprzez aplikację (42%). Natomiast druga grupa pod względem liczebności głosów odpowiada, że „Rodzice nie kontrolują mojego czasu w Internecie” (27%). Kolejne dwie grupy deklarują, że albo odkładają lub wyłączają telefon (9%) lub też rodzice zabierają im telefon (9%). „Blisko co czwarty młody internauta uważa, że wprowadzona przez jego rodziców

kontrola w zakresie czasu korzystania z Internetu (28,8%) oraz dostępu do treści w Internecie (28,9%) jest nieskuteczna” [15]. Jeśli chodzi o czas spędzany w Internecie ankietowana grupa krakowskich uczniów deklaruje: godzinę lub dwie (43%). Kolejna grupa (28%), że od 2-3 godzin. Następnie 12% uczniów przyznaje się do trzech, czterech godzin dziennie. 8% dzieci deklaruje – ponad 4 godziny a 9% cały czas ma ze sobą telefon i nie kontroluje czasu. Internet jest dla nich przyjemnością i rozrywką, której trudno się oprzeć i z której trudno jest dobrowolnie zrezygnować.

### ***Zasady korzystania z telefonów komórkowych przez dzieci w szkole. Oczami uczniów i nauczycieli.***

Wg Raportu NASK „Nastolatki 3.0” [15] prawie co trzeci uczeń ma możliwość korzystania z urządzeń mobilnych (smartfon, tablet, laptop) na terenie szkoły podczas przerw lekcyjnych. W krakowskiej ankiecie, uczniom zadano pytanie: „Czy w Twojej szkole jest zakaz używania telefonów?” Trzy najpopularniejsze odpowiedzi brzmią: „Tak, ale mało kto go przestrzega” (40%), „Tak, ale na lekcjach za zgodą nauczyciela można korzystać” (30%), „Tak i uczniowie go przestrzegają” (24%). Co ciekawe, jest grupa uczniów (2%), która nie wie czy w szkole obowiązuje taki zakaz. Nauczyciele przyznają, że korzystanie z Internetu w szkole jest możliwe. 64% nauczycieli odpowiada, że uczniowie mogą z niego korzystać w trakcie lekcji za zgodą nauczyciela (np. ćwiczenia, testy online). Ale tylko 30% uczniów zaznaczyło taką opcję. Trudno domniemywać z czego wynika aż tak duża rozbieżność odpowiedzi. Może z faktu, że uczniowie nie zawsze pamiętają jak przebiegają poszczególne lekcje, co na nich było omawiane i w jaki sposób. Nauczyciel opracowując temat, przygotowuje się do lekcji i świadomie planuje metody dydaktyczne. Podobnie rozmiągają się odpowiedzi nauczycieli i uczniów odnośnie skutecznego egzekwowanie zakazu korzystania z telefonów przez uczniów w szkole. Najliczniejsza grupa nauczycieli (47%) twierdzi, że nauczyciele starają się go egzekwować, a dzieci odpowiadają: „Tak, jest zakaz, ale mało kto go przestrzega” (40%). Kilka osób (2%) nawet przyznało, że przestrzeganie zasad „w naszej szkole jest niemożliwe”. 29% nauczycieli wyznaje, że egzekwowanie jest możliwe ale jest bardzo trudne. Podobne obserwacje mają autorzy Cell Phones, Student Rights, and School Safety: Finding the Right Balance [17], którzy podkreślają, że wprowadzenie zakazu korzystania z telefonów w szkole jest trudnym zadaniem, bo wymaga współpracy całej społeczności, w tym rodziców, nauczycieli, rad szkolnych, ministerstw edukacji oraz szerszej świadomości społecznej na temat wpływu telefonów komórkowych na osiągnięcia i dobrostan młodzieży. A autorzy krakowskiego Raportu [10] dodają, że należy młodzieży zapewnić atrakcyjną alternatywę podczas przerw oraz wprowadzić skuteczne, systemowe zasady korzystania z telefonów w szkołach.

Twórcy ankiety zapytali dzieci co sądzą na temat zakazu korzystania z telefonów w szkole. Czy ten pomysł im się podoba? 15% uczniów przyznało, że zdecydowanie jest za wprowadzeniem takiego ograniczenia w szkole. Natomiast 24% jest zdecydowanie przeciw. Sumaryczna grupa skłaniająca się do niechęci wprowadzenia zakazu („zdecydowanie przeciw”, „raczej przeciw”) jest prawie dwukrotnie większa i liczy 50%.

Ich przeciwnicy, zwolennicy wprowadzenia zakazu („zdecydowanie tak”, „chyba tak”), liczy tylko 32%. Jest też grupa niezdecydowanych („nie wiem”) – 18% uczniów. Wydaje się, że wyniki badań krakowskich uczniów bardzo korespondują z wynikami uczniów z Nowej Zelandii [5], którzy nie skłaniali się do całkowitego zakazu korzystania z telefonów w szkole ale jednak większość uczestników uważała, że uczniowie nie powinni mieć telefonów podczas zajęć lekcyjnych, mając na uwadze naukę i względy bezpieczeństwa. Zwracając uwagę na dużą grupę dzieci (40%), która przyznaje, że zakaz nie jest w szkole respektowany przez samych uczniów, trudno zaproponować skuteczne rozwiązanie. Można przychylić się do propozycji badaczy Raportu [10], i zapewnić dzieciom atrakcyjne przerwy w postaci organizacji gier planszowych, piłkarskich czy gry w ping-ponga. Ta rozrywka, może przyczynić się do integracji i atrakcyjnego spędzania czasu, gdyż same dzieci przyznają, że „telefon pozwala mi unikać ludzi i nie czuć się głupio” (25%) oraz że „telefon jest lekarstwem na nudę” (45%). Nauczyciele potwierdzają, że uczniowie często uciekają do Internetu od swoich realnych problemów. Tak uważa 92% ankietowanych nauczycieli („tak” – 49%, „zdecydowanie tak” – 43%). Problem ten został również dostrzeżony przez krakowskich pedagogów na konferencji pt.: „O czym marzą dziewczynki..?” [16].

Zapytana kadra pedagogiczna o to, czy są zwolennikami zakazu korzystania z telefonów w szkole, wypowiedziała się skrajnie przeciwnie niż dzieci. Aż 90% odpowiedziało – „tak”, tylko 6% - „nie”. Nauczyciele (46%) uważają, że dzięki wprowadzeniu zakazu korzystania z telefonów w szkołach, uczniowie mają mniej problemów ze zdrowiem psychicznym. 77% nauczycieli (42% - „tak”, 35% - „zdecydowanie tak”) uważa, że uzależnienie od telefonów ma związek z depresją, lękiem i ADHD. Ale już nie popierają tak zdecydowanie tezy, że „jest to darmowe narzędzie do osiągnięcia zdrowia psychicznego dzieci i młodzieży” (30%). Jest to teza Sary Abrahamsson z Norweskiego Instytutu Zdrowia Publicznego [1]. Natomiast ponad połowa (57%) uważa, że „jest to metoda na zmniejszenie ilości uczniów uzależnionych od Internetu”. Spora grupa (49%) obserwuje, że „uczniowie wydają się spokojniejsi”. Nauczyciele zostali poproszeni o wymienienie innych, ich zdaniem ważnych, korzyści płynących z ograniczeń korzystania z telefonów w szkole. Najczęstszymi odpowiedziami są: większa integracja z kolegami i koleżankami (rozwijanie kompetencji interpersonalnych) oraz lepsza koncentracja podczas lekcji, mniejsze pobudzenie i rozproszenie. Dzieci bez telefonu, w sposób naturalny szukają aktywizujących sposobów na nudę. Na te aspekty zwrócił uwagę Michelle Fitzula w jednej z pierwszej publikacji [4] poświęconej telefonom w szkołach. Wskazuje: rozproszenie, niepoprawne zachowania a także nieuczciwość akademicką. Eliminując telefony ze szkoły, można mieć nadzieję na poprawę wymienionych problemów. Obie grupy przyznają, że dzięki zakazowi korzystania z telefonów czują się bezpieczniej w szkole. Nauczyciele: 27%, nie chcą być nagrani ani sfotografowani przez uczniów, a uczniowie: 33%, potwierdzają że ma miejsce mniej agresji.

Zapytano dzieci, czy ich zdaniem telefon w szkole im przeszkadza czy pomaga. Odpowiedzi dzieci są prawie równomiernie podzielone pomiędzy trzy możliwe odpowiedzi: „tak”, „nie”, „trudno powiedzieć”. Wydaje się jakby uczniowie, szkół podstawowych biorących udział w ankiecie, nie widzieli większych korzyści z wprowadzenia zakazu korzystania z telefonów w szkołach. Nie widzą związku pomiędzy korzystaniem z telefonów w szkole a lepszą integracją z klasą (30%), lepszym skupieniem się na lekcjach (29%), ochroną przed uzależnieniem od Internetu (27%) czy ochroną wzroku (17%). Tylko 38% przyznaje, że bez telefonu ma lepsze wyniki w nauce.

Wyraźnie większa natomiast jest grupa, która przyznaje, że dzięki telefonom częściej się śmieje (60%). Może to wynikać z faktu, że młodzież Internet traktuje jako świetną zabawę i rozrywkę, dlatego najczęściej ogląda śmieszne i zabawne filmiki i rolki [16].

W odpowiedzi na pytanie: „Do czego używasz telefonu w szkole?” pojawiły się cztery główne pozycje: „robimy na lekcjach zadania/quizy na telefonie” – „czasami” (41%), „w ogóle nie używam telefonu w szkole” – 38%, „do kontaktu z rodzicami” – „tak, dość często” (35%), „korzystam na przerwie, żeby sprawdzić informacje” – 13% „tak, dość często”. Na podstawie udzielonych przez uczniów odpowiedzi można wnioskować, że nie korzystają w sposób niedozwolony z telefonów ani na przerwie ani na lekcji. W tym pytaniu odpowiedzi nauczycieli i uczniów zbiegają się ze sobą. W grupie nauczycieli pojawiły się dwa stwierdzenia, które zdobyły największą ilość głosów: „uczeń korzystał z telefonu na lekcji do celów edukacyjnych za zgodą nauczyciela” (55% - „zdecydowanie tak”), „uczeń kontaktował się z rodzicami” (52% - „zdecydowanie tak”). Są to jak najbardziej poprawne zachowania dzieci.

Uczniowie zauważyli jednak również kilka niestosownych zachowań uczniów i nauczycieli z użyciem telefonu. Pierwsze trzy to: „ktoś wyrzucił cię z grupy np. na WhatsAppie” (41%), „nauczyciel zabrał uczniowi telefon” (39%), „ktoś zrobił ci zdjęcie” (31%). Pedagodzy, również zaobserwowali niepokojące sytuacje w szkole. Ich obserwacje w dużej mierze pokrywają się z tymi, które zaznaczyli uczniowie. „Uczeń nagrał innych uczniów” (46%), „uczeń nagrał/zrobił zdjęcie nauczyciela bez jego zgody” (35%), „uczeń wyrzucił innego z grupy np. na WhatsAppie” (30%), „uczeń wykorzystał materiały innego ucznia bez jego zgody” (26%), „uczeń oglądał filmiki pokazujące przemoc fizyczną” (22%). Zdarzyło się także, że nauczyciel odebrał telefon uczniowi. 22% nauczycieli przyznaje, że taka sytuacja miała miejsce. Kompromitujące lub obraźliwe wiadomości uczniów widziała lub dostała, grupa 26% nauczycieli („zdecydowanie tak”). 10% nauczycieli widziało, że „uczeń oglądał pornografię”. Stosunkowo niewielka skala odpowiedzi pozytywnych, daje nadzieję na fakt, że sytuacje takie nie są powszechne. Z własnego doświadczenia nauczyciele dodatkowo opisują w ankiecie min. takie sytuacje: *„dziewczynka nagrała siebie podczas kąpieli i umieściła nagranie w sieci, puszczenie filmików pornograficznych na lekcjach zdalnych, bez pozwolenia nauczyciela zabranie telefonu na zieloną szkołę, obrażanie innych uczniów na portalach społecznościowych, uczeń hejtował innych uczniów, korzystanie z Internetu podczas sprawdzianu, nagrywanie instastory z wycieczki szkolnej, nagrywanie lekcji, obraźliwie wpisy o nauczycielach,*

*udostępnianie wizerunku ucznia i założenie mu fałszywego konta na Facebooku, uczeń "podszył" się pod innego w grupie klasowej na Whatsappie, rodzice uczniów hejtują się wzajemnie na założonych przez siebie forach*". Konflikty między dziećmi przeniosły się do sieci, na grupy do komunikatorów. Nagminnie zdarza się, że uczniowie wyrzucają się z grup np. na WhatsAppie, co potwierdza największa ilościowo grupa uczniów ankietowanych. Dorosłym, poprzez ich brak obecności w grupie, trudno grupy kontrolować i zaprowadzić w nich zasady oraz reguły, przez co dzieci na komunikatorach czują się mniej bezpieczne. Temat ten podsumowuje Raport „Dziewczynki i komunikatory”[13]. Problem hejtu w sieci wydaje się być najpoważniejszy i najtrudniejszy dla uczniów szkół podstawowych.

### ***Internet i jego wpływ na uczniów, rodziców i szkoły.***

Nauczyciele zostali poproszeni o wybranie tez z którymi się zgadzają. W tej grupie pytań, odpowiedzi znalazły się głównie w zakresie „tak” i „zdecydowanie tak”. Tylko dwie odpowiedzi wyraźnie uplasowały się w zakresie „nie”, „raczej nie”, „trudno powiedzieć”. Nauczyciele nie mają zdania na temat czy „zakaz używania telefonów w szkole ma pozytywny wpływ zwłaszcza dla dziewczynek” – „trudno powiedzieć” (49%). Tę samą ilość głosów (49%) otrzymała teza: „Zakaz używania telefonów w szkole ma pozytywny wpływ zwłaszcza dla dziewczynek”.

Na pierwsze miejsce wysuwa się natomiast potrzeba obowiązkowej edukacji dla dzieci w zakresie cyberbezpieczeństwa. Tak uważa 96% pytaných nauczycieli (31% - „tak”, 65% - „zdecydowanie tak”). Na drugim miejscu plasuje się teza, zgodnie z którą „nauczyciele postrzegają rodzinę jako klucz do cyfrowego bezpieczeństwa dzieci” (94%; 32% - „tak”, 62% - „zdecydowanie tak”). Do osiągnięcia tego celu konieczna jest współpraca szkoły z rodzicami. Największa grupa nauczycieli (41%) twierdzi, że „szkoła ma wsparcie w rodzicach”. Aż 72% nauczycieli zauważa, że „rodzice oczekują pomocy ze strony szkoły”. A ponad 52% ankietowanych potwierdza współpracę rodziców z wychowawcą, pedagogiem szkolnym. Teza numer trzy brzmi: „telefony wpływają na problemy z małą motoryką, ubogim słownictwem, wycofaniem w kontaktach rówieśniczych”, tak uważa 93% ankietowanych nauczycieli (32% - „tak”, 61% - „zdecydowanie tak”). Kolejne: „poprzez zaangażowanie w social media, dzieci omijają pozytywne doświadczenia z życia realnego” twierdzi 91% nauczycieli (45% – „tak”, 46% - „zdecydowanie tak”). W edukacji rodziców poprzez warsztaty i spotkania, nauczyciele upatrują dużego wsparcia dla dzieci (88%; 41% - „tak”, 47% - „zdecydowanie tak”). Grono pedagogiczne (88%, „tak” i „zdecydowanie tak”), dobrego sposobu w walce z uzależnieniem czy niekontrolowanym korzystaniem z telefonu upatruje w „regularnej aktywności fizycznej, która ma najsilniejszy efekt ochronny przed pogorszeniem funkcji poznawczych”. Stworzenie zespołów współpracujących (nauczyciele, rodzice, eksperci, rząd) jest ważne dla 76% ankietowanych (46% - „tak”, 30% - „zdecydowanie tak”). „Szkoły powinny przejąć inicjatywę cyberedukacji i w tym otrzymać wsparcie od rządu” tak uważa 67% ankietowanych (44% - „tak”, 23% - „zdecydowanie tak”).

### ***Czy i jakiego wsparcia oczekują nauczyciele od instytucji samorządowych?***

W tej sekcji odpowiedzi: „raczej tak” i „zdecydowanie tak”, bardzo wyraźnie wybrzmiały. Można zauważyć, że odpowiedzi: „nie”, „raczej nie”, „trudno powiedzieć”, właściwie nie występują. „Jednolite zasady dla wszystkich szkół np. dotyczące korzystania z telefonów”: 60% - „zdecydowanie tak”, 30% - „raczej tak”. „Opracowanie procedur reakcji szkoły na nieodpowiednie zachowania w sieci (np. hejt) i skuteczne wyciąganie konsekwencji”: 68% - „zdecydowanie tak”, 26% - „raczej tak”. „Edukacja prawna w zakresie przestępstw internetowych”: 66% - „zdecydowanie tak”, 29% - „raczej tak”. „Zaangażowanie przedstawicieli służb (np. policji) w działania profilaktyczne podejmowane w szkole”: 71% - „zdecydowanie tak”, 26% - „raczej tak”. „Jednolite narzędzia z zakresu profilaktyki opracowane przez ekspertów”: 62% - „zdecydowanie tak”, 33% - „raczej tak”. „Wyposażenie szkół w sprzęt (komputery/tablety) umożliwiający bezpieczne korzystanie z Internetu w szkole”: 66% - „zdecydowanie tak”, 22% - „raczej tak”.

### **WNIOSKI I REKOMENDACJE**

Przeprowadzone badania jako pierwsze badają tak młodych użytkowników Internetu oraz zestawiają ich głosy z opiniami nauczycieli w kwestii korzystania z telefonów w szkole. W podsumowaniu zostają silnie podkreślone potrzeby i oczekiwania nauczycieli, które pozwolą im zadbać o dobrostan cyfrowy ich samych, ale przede wszystkim – dzieci. Zostają również uwzględnione potrzeby rodziców. Tylko dzięki współpracy szkoła – rodzic – dziecko, można zapewnić bezpieczny rozwój młodego pokolenia.

W kwestii wprowadzenia zakazu korzystania z telefonów w szkole, dzieci i dorośli mają odmienne zdanie na ten temat. 90% nauczycieli jest zwolennikami zakazu korzystania z telefonów w szkołach ale tylko 15% uczniów zdecydowanie popiera ten pomysł. Aż 50% uczniów zadeklarowało „zdecydowanie jestem przeciw” i „raczej nie”. W zakazie korzystania z telefonów dzieci nie widzą znaczących korzyści, nauczyciele – wprost przeciwnie. Pedagodzy w zakazie upatrują metody do zmniejszenia ilości uczniów uzależnionych od Internetu (57%, zdecydowanie tak), uczniowie wydają się być spokojniejsi (50%, zdecydowanie tak), uczniowie mają mniej problemów ze zdrowiem psychicznym (46%, zdecydowanie tak). Odpowiedzi dzieci są bardzo równomiernie rozłożone pomiędzy trzy kolumny: tak, nie, trudno powiedzieć. Można domniemywać kilku powodów tak rozłożonych głosów. Pierwszy to brak wiedzy i świadomości dzieci, brak obserwacji u rówieśników wspomnianych problemów, niechęć by się przyznać, gdy ewentualnie takie problemy obserwuje się u siebie. Sytuacje w których uczniowie korzystają z telefonu w szkole. Tutaj odpowiedzi nauczycieli i uczniów bardzo się do siebie zbliżają patrząc na wykresy w zestawieniu. Najczęściej jest to kontakt z rodzicami (dzieci: 36%, nauczyciele: 52%), na lekcji do celów edukacyjnych za zgodą nauczyciela (dzieci: 28%, nauczyciele: 56%).

Największa grupa ankietowanych uczniów (43%) deklaruje, że z telefonu korzysta od 1-2 godzin dziennie. Kolejna (28%) że od 2-3 godzin. Zważywszy na fakt, że 43% dzieci przyznaje, że nie ma żadnych limitów w korzystaniu z telefonu a największą grupą ankietowanych są uczniowie piątej klasy (39%) można podejrzewać, że tak małe dzieci nie mają poczucia czasu i wyniki które podają względem czasu spędzanego w Internecie są zaniżone. Co potwierdzałyby odpowiedź dzieci: „Chyba spędzam za dużo czasu w telefonie” (23%). Mimo, że dzieci swój pierwszy telefon otrzymują najczęściej już w wieku 8 lat (23%), 9 lat (22%) i 7 lat (20%) bardzo cieszące są ich odpowiedzi w zakresie oceny ich własnej relacji ze smartfonem. Na stwierdzenie: „Wydaje mi się, że potrafię korzystać z telefonu i regulować swój czas” – 74% dzieci wybrało: „raczej tak”. Na stwierdzenie „Mogłabym/ mógłbym spędzić tydzień bez telefonu np. na wakacjach” – 70% dzieci odpowiedziało: „raczej tak”. Odpowiedzi tym bardziej cieszą, że dzieci do świata cyfrowego wchodzą już dużo wcześniej, min. korzystając z telefonów rodziców (80%). Część z nich (16%) ma już swój telefon w wieku poniżej 7 roku życia. Maluchy najczęściej oglądają bajki lub filmy (71%) oraz grają w gry (62%). Uwzględniając tak wczesny wiek dzieci, konieczna wydaje się również cyfrowa edukacja rodziców. Nauczyciele właśnie rodzinę postrzegają jako klucz do cyfrowego bezpieczeństwa dzieci (62%, „zdecydowanie tak”).

Należy wzmocnić wiedzę i świadomość rodziców na temat cyfrowych zagrożeń dzieci. Konieczne jest organizowanie dla nich dedykowanych konferencji, na których będą się mogli podzielić swoimi obserwacjami i problemami z ekspertami oraz uzyskać odpowiedzi. Telefon z dostępem do Internetu jest wspaniałym narzędziem, ale należy dzieciom przedstawiać korzyści i zagrożenia płynące z jego korzystania. Młodzież należy edukować i motywować by w świadomy sposób korzystała z Internetu, dbając o swój dobrostan fizyczny, psychiczny i społeczny. Uczniów należy zachęcać do aktywności fizycznej, która zdaniem nauczycieli (88%) ma najsilniejszy efekt ochronny przed pogorszeniem funkcji poznawczych. Należy ich wspierać dodatkowymi warsztatami i lekcjami z higieny cyfrowej oraz cyberbezpieczeństwa. Tak uważa 66% nauczycieli („zdecydowanie tak”). Nauczyciele sami siebie nie postrzegają jako ekspertów, nie czują się na tyle kompetentni by wprowadzać młodzież w cyfrowy świat. Należy wzmocnić nauczycieli poprzez dedykowane szkolenia, warsztaty i konferencje z zakresu cyberbezpieczeństwa. Nauczyciele chcą też zaangażowania przedstawicieli służb np. policji, w działania profilaktyczne podejmowane w szkole (72%, „zdecydowanie tak”). Od instytucji rządowych oczekują wsparcia systemowego i merytorycznego.

Konieczna jest edukacja i wsparcie zarówno dla nauczycieli, rodziców jak i dzieci. W realizacji tego celu, niezbędne są darmowe konferencje z zakresu cyberbezpieczeństwa dla dorosłych, osobne dla obu grup oraz ciekawe, interaktywne warsztaty dla dzieci, które pomogą świadomie i dobrowolnie wyeliminować korzystanie z telefonów w szkołach. Wielkim wsparciem dla dyrektorów i pracowników szkół, byłaby ustawa na szczeblu krajowym, która regulowała by tę kwestię.

## BIBLIOGRAFIA:

1. Abrahamsson Sara, "Smartphone Bans, Student. Outcomes and Mental Health, 2024.
2. Campbell Marilyn, Edwards Elizabeth J, Pennell Donna, Poed Shiralee, Lister Victoria, Gillett-Swan Jenna, Kelly Adrian, Zec Dajana, Nguyen Thuy-Anh, Evidence for and against banning mobile phones in schools: A scoping review, 2024.
3. Dorris Claire, Winter Karen, O'Hare Liam, Lwoga Edda Tandi, A systematic review of mobile device use in the primary school classroom and impact on pupil literacy and numeracy attainment: A systematic review, 2024.
4. Fitzula Michelle, "Using Mobile Devices in the Classroom, Stockton University, 2019.
5. Gath Megan E., Monk Lauren, Scott Amy, Gillon Gail, "Smartphones at School: A Mixed-Methods Analysis of Educators' and Students' Perspectives on Mobile Phone Use at School, 2024.
6. Górski Rafał, „Apel VIP do minister Barbary Nowackiej w sprawie smartfonów, Instytut Spraw Obywatelskich”, 2024. [<https://instytutsprawobywatelskich.pl/apel-vip-ow-w-sprawie-smartfonow-do-minister-barbary-nowackiej/>]
7. Haidt Jonathan, "The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness", 2024.
8. Hartley Kendall, Hoffman Bobby, Andújar Alberto, "Smartphones and Learning: Evaluating the Focus of Recent Research", 2023.
9. Horvath Juliane, Mundinger Christina, Schmitgen Mike M, Wolf Nadine D , Sambataro Fabio, Hirjak Dusan, Kubera Katharina M, Koenig Julian, Wolf Robert Christian, "Structural and functional correlates of smartphone addiction", 2020.
10. Instytut Badawczy IPC Sp. z o.o., „Raport z Korzystania z urządzeń elektronicznych oraz z Internetu przez dzieci i młodzież”, 2017.
11. Kaimara Polyxeni, Poulimenou Sofia Maria, Oikonomou Andreas, Deliyannis Ioannis, "Smartphones at Schools? Yes, Why not?", 2019.
12. Konferencja „UWAGA! Smartfon”, [<https://uwagasmartfon.pl/>]
13. KOSMOS dla dziewczynek, „Raport: Dziewczynki i komunikatory” [<https://kosmosdladziewczynek.pl/thinktank/raport-dziewczynek-dziewczynki-i-komunikatory>]
14. Montag Christian, Elhai Jon D., "Do we need a digital school uniform? Arguments for and against a smartphone ban in schools", 2023.
15. NASK Nastolatki 3.0, „Raport z ogólnopolskiego badania uczniów i rodziców”, 2023
16. Nowakowska-Głuszak Anna, Kozaczuk Urszula, Raport z konferencji "O czym marzą dziewczynki, a czego się boją? Dbamy o zdrowie psychiczne krakowskich uczennic", 2024; [<https://www.informatyka.agh.edu.pl/pl/dla-szkol/o-czym-marza-dziewczynki-a-czego-sie-boja-dbamy-o-zdrowie-psychiczne-krakowskich-uczennic/>]
17. Smale William T., Hutcheson Ryan, Russo Charles J., "Cell Phones, Student Rights, and School Safety: Finding the Right Balance", 2021.
18. Solecki Roman, „Raport z badania ankietowego kondycji psychicznej młodzieży”, 2023.
19. UNESCO Global Education Monitoring Report, 2023.
20. Wan Jen Chun, Hsieh Chia-Yen, Kung Shih-Hao, "The impact of smartphone use on learning effectiveness: A case study of primary school students", 2022.

## JAK UGOTOWAĆ ŻABĘ I UPOLOWAĆ JEDNOROŻCA?

Agnieszka CENZARTOWICZ<sup>1</sup>

**Streszczenie:** Rozdział zawiera instrukcję, która została napisana z przymrużeniem oka, aby uczulić, tak założycieli startupów, jak i funkcjonariuszy, na narzędzia powszechnie stosowane przez osoby, które pozorując działania inwestorskie wykorzystują dla różnych celów (w tym przestępczych) taki nowopowstały podmiot.

**Słowa kluczowe:** beneficjent rzeczywisty, compliance, oszustwo, błąd poznawczy.

### **Zastrzeżenie:**

*Poniższy artykuł powstał na podstawie zanonimizowanych doświadczeń autorki. Wszelkie podobieństwo do funkcjonujących na rynku podmiotów jest zamierzone. Artykuł ten dedykuje: UBO et consortes.*

*„Ja nie mam nic, ty nie masz nic, on nie ma nic – zaśmiał się głośno.  
-To razem właśnie mamy tyle, w sam raz tyle, żeby założyć wielką fabrykę.  
Cóż stracimy? Zarobić zawsze można.”  
Stanisław Reymont, Ziemia obiecana*

Struktura typowego startupu oparta na ograniczonych zasobach, ciągłym działaniu pod presją czasu, przez częstokroć niedoświadczonych założycieli czyni go podatnym na manipulacje. Quasi inwestorzy potrafią czerpać korzyści z tych słabości, stosując zarówno wyrafinowane strategie psychologiczne i pułapki prawne, jak i wykorzystując przy tym brak compliance w startupie. Celem ich działań jest przejęcie kontroli nad podmiotem, wyciągnięcie korzyści finansowych lub zasobów technologicznych, a czasem nawet wykorzystanie startupu do nielegalnych działań.

Niniejsza „instrukcja” nie ma na celu wskazania quasi inwestorowi (Tobie) kilku możliwości przejęcia startupu i pozostawienia założycieli z pełną odpowiedzialnością. Jej celem jest zilustrowanie tak założycielom startupu poszukującym kapitału jak i funkcjonariuszom, którzy być może zechcą Ci się kiedyś przyjrzeć, na co mają zwrócić uwagę w tego typu sprawach.

---

<sup>1</sup> SWC Group sp. z o.o., acenzartowicz@swclaw.pl.

## Startup to łatwy cel?

Założyciele startupu to wizjonerzy wierzący, że ich pomysł zmieni świat. Niestety, ten świat jest również pełen niedoświadczenia, presji finansowej i chaosu zarządzania. To doskonała okazja dla Ciebie, quasi inwestora, by do niego wkroczyć, stopniowo przejmując kontrolę nad marzeniami założycieli, aby przekształcić je w źródło własnych zysków.

Twoja strategia nie powinna polegać na otwartym przejęciu władzy. Pozostawmy to innym inwestorom. To gra, w której założyciele podejmują decyzje zgodne z Twoimi interesami, nawet tego nie zauważając. Wykorzystujesz ich naiwność, brak compliance<sup>2</sup>, psychologiczne słabości i luki prawne, aby stworzyć sytuację, w której „ich startup” staje się Twoim narzędziem do realizacji Twoich celów<sup>3</sup>.

### **1. Założyciele nie mają żadnego lub prawie żadnego doświadczenia biznesowego.**

Nie mają, bo są nimi często inżynierowie, technolodzy lub naukowcy, koncentrujący się na tworzeniu produktu, ignorujący aspekty prawne i finansowe. Brak wiedzy

o umowach inwestycyjnych, strukturach korporacyjnych, czy ochronie własności intelektualnej czyni ich niezwykle podatnymi na manipulacje.

- **Presja finansowa**

Startupy, szczególnie na wczesnym etapie, często mają bardzo ograniczone zasoby finansowe. To prowadzi do desperackiego poszukiwania inwestorów, co sprawia, że są skłonne zaakceptować niemal każdą ofertę bez dokładnej analizy jej możliwych konsekwencji.

- **Pułapka prawna**

Quasi inwestorzy mogą oferować finansowanie z klauzulami rozwodnieniowymi, które pozwalają im przejąć kontrolę nad firmą w przypadku problemów finansowych startupu.

- **Skupienie na technologii kosztem biznesu**

Założyciele często koncentrują się na rozwijaniu produktu, zaniedbując kwestie związane z ochroną własności intelektualnej, rejestracją patentów czy analizą prawną umów.

---

<sup>2</sup> Compliance (zgodność) to przestrzeganie przepisów prawa, standardów branżowych oraz wewnętrznych regulacji i procedur w organizacji. Obejmuje działania mające na celu zapewnienie, że podmiot działa zgodnie z obowiązującymi normami prawnymi, etycznymi i regulacyjnymi, minimalizując ryzyko prawne, finansowe i reputacyjne.

<sup>3</sup> Szymon Janiak w „Ciemna strona start-upów” (2023), podkreśla, że startupy często nie są świadome ryzyk wynikających z niekorzystnych zapisów w umowach inwestycyjnych. Z kolei Daniel Kahneman w „Pułapkach myślenia” (2011) wyjaśnia, jak błędy poznawcze sprawiają, że ludzie podejmują irracjonalne decyzje w stresujących sytuacjach. Te dwa elementy stanowią powinny fundament Twojej strategii.

- **Brak compliance**

Większość startupów nie wdraża procedur kontrolnych, takich jak audyt umów, transparentność przepływów finansowych, czy zabezpieczenie własności intelektualnej. To Twoje eldorado – możesz działać bez większego nadzoru i wprowadzać korzystne dla Ciebie klauzule, które pozostaną niezauważone.

- **Skupienie na wizji**

Założyciele wierzą, częstokroć niebezpiecznie, że ich produkt zmieni świat. Ta wiara sprawia, że ignorują ryzyka wynikające z umów inwestycyjnych czy decyzji finansowych.

- **Zależność od pożyczek**

Założyciele, chcąc uniknąć rozwodnienia udziałów, często wybierają pożyczki zamiast inwestycji kapitałowych. To narzędzie, które możesz wykorzystać, by przejąć firmę w przypadku problemów finansowych.

## 2. Jak SKUTEKZNIE manipulować założycielami startupów?

Quasi inwestorzy stosują różnorodne techniki, aby zdobyć kontrolę nad podmiotem, zarówno przez wpływ psychologiczny, jak i prawne pułapki. Jak subtelnie przejąć kontrolę nad startupem? Etap

- **Wejść jako wybawca *CALY UBRANY NA BIAŁO***

Twoja pierwsza rola to mentor, partner i sojusznik. Musisz wejść do startupu jako ktoś, kto wierzy w wizję jego założycieli i jest gotów ich wesprzeć w drodze do sukcesu definiowanego jako komercjalizacja wynalazku.

Bądź entuzjastą ich pomysłu. Proponuj wsparcie na własny koszt w uporządkowaniu kwestii prawnych i finansowych. Proponuj, ale nie narzucaj się.

**Buduj swój wizerunek w oparciu o sprzeczne lub nieprawdziwe informacje. Wykorzystuj niedomowienia. W celu zdobycia zaufania założycieli** kreuj się na skromnego eksperta w dziedzinie inwestycji, wspierając się dotychczasowymi osiągnięciami, publikując artykuły sponsorowane w mediach branżowych, w których przedstawiany jesteś jako lider danego rynku lub wręcz sugerując współpracę z dużymi podmiotami o uznanej renomie rynkowej.

Pamiętaj, że założyciele w dzisiejszych czasach to często przedstawiciele pokolenia wrażliwego na cierpienia tego świata, cenią uczciwość, transparentność i cnoty moralne - dając nowo poznany partnerom biznesowym, często nieuzasadniony, kredyt zaufania. Przedstaw się i kreuj na oazę uczciwości, transparentności i moralności. Najlepiej bądź konserwatywnym wyznawcą jednego z głównych nurtów religijnych, dobrym partnerem/ką, mężem, żoną, ojcem oraz społecznie zaangażowanym aktywistą/ką.

Założyciele działający pod presją czasu i będąc świadomymi braku kapitału, zobaczą w Tobie wybawcę. Będą wdzięczni za Twoją pomoc i otwarci na Twoje sugestie. To kluczowy moment, w którym przejmiesz kontrolę nad ich decyzjami, jednocześnie pozostawiając ich w przekonaniu, że to oni pozostają u sterów.

- **Psychologia jako narzędzie manipulacji**

Ludzie podejmują często decyzje pod wpływem emocji i stresu. Wykorzystaj to. Założyciele startupów są pełni ambicji, ale również stresu i obaw, co stwarza idealne warunki do manipulacji.

Najpierw wykorzystaj **efekt potwierdzenia**. Wzmocnij ich wiarę, że ich pomysł jest przełomowy, a Ty jesteś ich sprzymierzeńcem. Dzięki temu nie będą kwestionować Twoich intencji ani propozycji.

Następnie wykorzystaj **efekt aureoli**, by stworzyć wizerunek eksperta. Wspomnij o współpracy z wielkimi graczami w branży lub podaj przykłady innych startupów, które dzięki Tobie odniosły sukces. Założyciele nie będą kwestionować nawet najbardziej wyolbrzymionych historii, ponieważ zaufają Twojej reputacji.

**Presja czasu** to kolejne narzędzie. Wywieraj presję wskazując na Twoją ograniczoną dostępność. Strach przed stratą zmusza ludzi do szybkiego działania. W takiej sytuacji założyciele przestaną analizować warunki umowy, koncentrując się na „ratowaniu” spółki.

Wykorzystaj również **efekt utopionych kosztów**. Gdy założyciele zainwestują czas i pieniądze we współpracę z Tobą, trudno będzie im się wycofać. Będą bardziej skłonni akceptować Twoje warunki, nawet jeżeli stają się one coraz mniej korzystne.

Żeby efekt utopionych kosztów zadziałał prawidłowo, nie możesz dopuścić, aby w startup zainwestował jeszcze ktoś inny.

- **Wykorzystaj brak compliance jako przewagę**

Startupy, szczególnie te na wczesnym etapie rozwoju, rzadko wdrażają formalne procedury kontrolne. Brak audytu umów oznacza, że możesz wprowadzać klauzule, które formalnie wydają się standardowe, ale w rzeczywistości oddają Ci pełną kontrolę nad spółką.

Na przykład pozornie niewinne stwierdzeniem, że każda zmiana w strukturze udziałowej wymaga Twojej zgody uniemożliwia założycielom pozyskanie nowych funduszy bez Twojej aprobaty. Możesz to przedstawiać jako „powszechną praktykę w branży”, standard „z doliny”, etc.

Nieprzejrzyste przepływy finansowe w startupach pozwalają Ci wprowadzać pieniądze jako inwestycję, a następnie wyprowadzać je w formie fikcyjnych faktur lub honorariów. Wysokie koszty operacyjne startupów i brak procedur audytowych sprawiają, że takie działania są trudne do wykrycia.

Słabo chroniona własność intelektualna to najcenniejszy element Twojej strategii. Jeżeli startup posiada kod źródłowy, patenty lub technologie, możesz zarejestrować je na swoją spółkę, tłumacząc, że to uprości procesy. Gdy firma nie spełni warunków umowy, te aktywa staną się Twoje.

- **Konieczność skłócić założycieli i przejmij kontrolę nad narracją**

Podziel zespół założycielski, aby osłabić ich zdolność do wspólnego podejmowania decyzji. Zaczynij od faworyzowania jednej osoby.

Kiedy zespół jest podzielony, stajesz się jedynym stabilnym punktem odniesienia. Założyciele, zajęci wzajemnymi konfliktami, stają się mniej efektywni w podejmowaniu kluczowych decyzji. Możesz subtelnie podsycać napięcia, sugerując, że jeden z nich jest bardziej kompetentny lub zaangażowany od pozostałych. To nie tylko osłabi dynamikę zespołu, lecz również stworzy sytuację, w której każdy założyciel zwróci się do Ciebie jako mediatora lub arbitra. W praktyce zaczynasz kierować ich decyzjami, jednocześnie przedstawiając siebie jako stabilizatora chaosu, który sam stworzyłeś.

- **Sterowanie z cienia**

Twoim celem nie jest otwarte przejęcie władzy nad firmą, lecz stworzenie sytuacji, w której możesz kontrolować wszystkie istotne decyzje bez formalnej odpowiedzialności. Kluczowym narzędziem jest wprowadzenie odpowiednich zapisów w umowach inwestycyjnych, takich jak prawo weta.

Prawo weta pozwala Ci blokować każdą decyzję, która nie jest zgodna z Twoimi interesami. Możesz na przykład uniemożliwić firmie pozyskanie dodatkowego finansowania od innego inwestora, argumentując, że wprowadzi to chaos w strukturze kapitałowej. W rzeczywistości nie chcesz dopuścić do sytuacji, w której ktoś inny mógłby podważyć Twoją dominację.

- **Zawsze włączaj swoich doradców**

Quasi inwestorzy często sugerują, że korzystanie z ich prawnika, doradcy IT, księgowego „przyspieszy proces” i „zredukuje koszty”. W rzeczywistości taki prawnik bądź doradcę działa wyłącznie w interesie inwestora. W Twoim interesie, jako quasi inwestora, należy doprowadzenie do zmarginalizowania roli doradców założycieli lub samej spółki poprzez stopniowe kwestionowanie ich kompetencji, wyłączenie ich z dyskusji merytorycznych lub ciągle sugerowanie wsparcia w postaci kontaktu z Twoimi doradcami.

- **„Dłużej poczekają – bardziej pokochają.” Nigdy nie spiesz się z dostarczaniem dokumentów**

Quasi inwestorzy celowo przesyłają kluczowe dokumenty tuż przed terminem podpisania, licząc na to, że założyciele nie zdążą ich dokładnie przeanalizować. Gdyby jakimś cudem im to się jednak udało, warto dopilnować, aby w dokumentach znalazło się sporo drobnych błędów, co ułatwi odwrócenie uwagi założycieli od meritum.

**Pamiętaj, że to Ty wybierasz notariusza. Twój notariusz, Twój termin, TWOJA interpretacja umowy. Nie przesadz jednak. Notariusz to ostatecznie zawód zaufania publicznego, a zatem wybierz „elastycznego”, który w pragnieniu wsparcia Cię „trochę” naruszy prawo. Nie chcesz przecież doprowadzić do unieważnienia aktu.** Pamiętaj, że odpowiedzialność za błędy spoczywa na zarządzie. Jeżeli spółka napotka problemy finansowe, prawne lub operacyjne, to założyciele będą musieli tłumaczyć się przed sądem, inwestorami lub kontrahentami. Ty jako inwestor jesteś „czysty” – oficjalnie nie masz wpływu na bieżące zarządzanie.

- **Wykorzystaj startup jako narzędzie finansowe**

Startupy to nie tylko podmioty gospodarcze – to również idealne wehikuly finansowe. Możesz je wykorzystać do prania pieniędzy, unikania podatków lub zabezpieczania swoich interesów. Brak przejrzystych procedur w młodych firmach sprawia, że takie działania są trudne do wykrycia.

Pranie pieniędzy: możesz wprowadzać środki jako „inwestycje”, a następnie wyprowadzać je w formie fikcyjnych faktur za usługi doradcze, marketingowe lub technologiczne.

Optymalizacja podatkowa: jeżeli startup ma strukturę międzynarodową, możesz przenieść zyski do jurysdykcji o korzystnych stawkach podatkowych. W ten sposób minimalizujesz obciążenia podatkowe, jednocześnie legalizując swoje dochody.

Ukrywanie aktywów: jeżeli startup posiada wartościowe aktywa, takie jak patenty, kod źródłowy czy znaki towarowe, możesz przenieść je na spółki zależne zarejestrowane w rajach podatkowych. Dzięki temu aktywa są chronione przed wierzycielami i pozostają pod Twoją kontrolą.

- **Kontrola bez odpowiedzialności**

Twoim największym atutem jest możliwość sterowania firmą, bez ponoszenia formalnej odpowiedzialności. Dzięki odpowiednio skonstruowanym umowom inwestycyjnym możesz wymusić prawo weta na wszystkie kluczowe decyzje firmy, od nowych emisji udziałów po sprzedaż aktywów.

Jednocześnie założyciele nadal są formalnymi członkami zarządu. To oni podejmują decyzje i ponoszą odpowiedzialność za wszelkie problemy. Ty pozostajesz w cieniu jako „inwestor”, który jedynie wyraża swoją opinię.

- **Subtelne wyciskanie wartości**

Gdy już przejmiesz kontrolę nad startupem, możesz stopniowo wyprowadzać z niego wartość. Możesz to robić subtelnie, aby założyciele nie zdawali sobie sprawy z tego, co się dzieje, aż będzie za późno.

Jednym z narzędzi jest rozwodnienie udziałów. Wprowadzasz zapisy w umowach, które pozwalają Ci przejmować dodatkowe udziały w przypadku niespełnienia przez startup określonych celów finansowych. Na przykład: „Jeżeli przychody startupu nie osiągną 10 milionów złotych w ciągu roku, inwestor ma prawo objąć dodatkowe 20% udziałów.”

W praktyce, gdy spółka nie spełnia tych celów – co często jest wynikiem Twojej własnej manipulacji – stajesz się większościowym udziałowcem bez konieczności inwestowania dodatkowych środków.

### **3. Kiedyś w końcu założyciele zaczną się domyślać... i bronić.**

Poniżej otwarta lista pomysłów na działania obronne założycieli:

<b>Działanie założycieli</b>	<b>Uzasadnienie</b>	<b>Twoje ad vocem</b>
------------------------------	---------------------	-----------------------

<b>Zatrudnienie profesjonalnych doradców</b>	Każda umowa inwestycyjna powinna być analizowana przez niezależnego prawnika i księgowego, którzy reprezentują interesy startupu.	<b>- poleciłem i opłaciłem usługi prawnika dla dobra spółki.</b>
<b>Weryfikacja quasi inwestora post factum</b>	Przeprowadzenie lub zlecenie przeprowadzenia szczegółowej analizy historii inwestora, jego wcześniejszych projektów oraz opinii w środowisku startupowym.	<b>- przecież działamy w zaufaniu - głośne rozważanie odstąpienia od inwestycji na gruncie KSH</b>
Transparentność w decyzjach	wprowadzenie jasnych zasad współpracy i podejmowania decyzji wewnątrz zespołu założycielskiego. Transparentność zapobiega konfliktom oraz minimalizuje ryzyko podejmowania decyzji pod wpływem presji lub przez jedną osobę.	<b>- z pomocą wspierającego nas członka zespołu kwestionujemy sens takich działań oraz/lub wyrażamy oburzenie, przedstawiając chęć wprowadzenia takich zasad jako brak zaufania i podważenie naszej dobrej wiary</b>
Ochrona własności intelektualnej	Ochrona własności intelektualnej (patenty, znaki towarowe i inne kluczowe zasoby technologiczne) na wczesnym etapie działalności firmy.	<b>- oferujemy się z pomocą</b>
....		

Podsumowując jako quasi inwestor musisz przyjąć subtelny strategię opierającą się na precyzji i bezwzględny wykorzystaniu słabości Twojego celu. Budujesz zaufanie, manipulujesz błędami poznawczymi, skłócasz zespół założycielski i wykorzystujesz brak compliance, aby przejąć nad nim kontrolę. Sterujesz startupem z cienia, jednocześnie pozostawiając formalną odpowiedzialność na barkach zarządu. Korzystasz z luk prawnych, by przejąć aktywa, minimalizować podatki i legalizować pieniądze.

Wszystko to musisz robić powoli, konsekwentnie i subtelnie, aby założyciele nie zdawali sobie sprawy, że tak ich marzenia, jak i oni sami stali się Twoim

narzędziem. Jesteś UBO<sup>4</sup> undercover kontrolującym wszystko z cienia. Inni niech ryzykują, pracują i potencjalnie się tłumaczą przed kontrahentami, pracownikami lub właściwymi organami.

Jeżeli jednak jesteś po dobrej stronie i uważasz, że tak ma być, to przeczytaj ten tekst jeszcze raz i zastanów się, jakie i gdzie możesz znaleźć ślady wskazujące na działania quasi inwestora, jak je pozyskać i zabezpieczyć.

## **BIBLIOGRAFIA**

1. Janiak Sz., Ciemna strona start-upów, 2023
2. Kahneman D., Pułapki myślenia. O myśleniu szybkim i wolnym, Media Rodzina 2011

---

<sup>4</sup> Beneficjent rzeczywisty

# DOPUSZCZALNOŚĆ ZASTOSOWANIA ART. 40 USTAWY O SŁUŻBIE KONTRWYWIADU WOJSKOWEGO I SŁUŻBIE WYWIADU WOJSKOWEGO W RAMACH OSŁONY KONTRWYWIADOWCZEJ WŁASNYCH STRUKTUR

Łukasz WARCHAŁ

**Streszczenie:** Niniejsze wystąpienie ma celu zwrócić uwagę na problem dopuszczalności wykorzystania funkcjonariuszy Służby Kontrwywiadu Wojskowego w charakterze osób udzielających pomocy przy wykonywaniu ustawowych zadań Służby w ramach jej osłony kontrwywiadowczej. Podniesiony problem dotyczy nie tylko SKW, ale również pozostałych instytucji uprawnionych do wykonywania czynności operacyjno – rozpoznawczych mierzących się z potrzebą posiadania dobrze uplasowanej i wiarygodnej agentury niezbędnej do zapewnienia odpowiedniego poziomu bezpieczeństwa wewnętrzne własnej organizacji. Przedstawiam i oceniam występujące w doktrynie stanowiska i proponuję wnioski de lege ferenda. Artykuł jest częścią większej pracy dotyczącej osłony kontrwywiadowczej SKW, opartej również i na własnych doświadczeniach, ale z pominięciem faktów i ocen, których ujawnienie mogłoby narazić na dekonspirację podlegające ochronie przyjęte rozwiązania i przeprowadzone przedsięwzięcia.

**Słowa kluczowe:** osobowe źródła informacji, osoby udzielające pomocy niebędące funkcjonariuszami, czynności operacyjno – rozpoznawcze, Służba Kontrwywiadu Wojskowego, osłona kontrwywiadowcza, bezpieczeństwo wewnętrzne służby.

**Summary:** The contemporary world, with globalised access to information and high data transfer creates new opportunities for science, and also serves as a stage for possible numerous and serious military, economic, and political conflicts. In times of acute conflict for example experienced in 2024, the flow of information within the academic community can contribute not only to the advancement of knowledge but also pose significant risks. The article aims to present the environment and factors associated with the free circulation of scientific information in the context of contemporary conflicts. Information is a key resource in today's academic landscape, driving the development of science, technology, and the knowledge-based economy. However, unrestricted access to information, which underpins scientific progress, has simultaneously become a considerable challenge, especially during periods of intense military and political conflicts. Such circumstances carry the risk that scientific research – particularly that of strategic importance – may be intercepted or misused in ways that violate original ethical principles and threaten both the security and the integrity of scientific values and achievements.

**Keywords:** academy, information security, threat

## WSTĘP

Służba Kontrwywiadu Wojskowego jest jedną z dwóch, obok Agencji Bezpieczeństwa Wewnętrznego, służb kontrwywiadowczych RP. Każda ze służb, w ramach swoich ustawowych kompetencji samodzielnie organizuje osłonę kontrwywiadowczą. SKW organizuje osłonę podmiotów należących bądź działających na rzecz sfery militarnej, w tym również wobec samej siebie, natomiast ABW zapewnia osłonę kontrwywiadowczą podmiotów nie zaliczających się do domeny SKW. Na mocy art. 39 ust. 1 ustawy o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego<sup>1</sup>, SKW została uprawniona do prowadzenia działań mających za cel zapewnienie ochrony stosowanym przez nią środkom, formom i metodom realizacji swoich zadań, zgromadzonym informacjom oraz własnym obiektom i danym identyfikujących jej funkcjonariuszy. W zakresie wyznaczonym przez art 39 ust. 1 ustawy, SKW w ramach osłony kontrwywiadowczej swoich struktur realizuje, te zadania spośród wymienionych w art. 5 ustawy<sup>2</sup>, których przedmiot i zakres umożliwia osiągnięcie postawionych w tym zakresie celów. Ogół przedsięwzięć mających służyć zapewnieniu tej ochrony, o której mówi art 39 ust. 1 ustawy nosi nazwę osłony kontrwywiadowczej<sup>3</sup>, czyli skoordynowanego zespołu aktywnych i pasywnych przedsięwzięć służących zapewnieniu bezpieczeństwa wewnętrznego Służby rozumianego jako stan zapewniający jej możliwość niezakłóconego funkcjonowania w celu możliwie najbardziej optymalnego realizowania postawionych przed nią zadań. Osłona kontrwywiadowcza jest realizowana za pomocą czynności operacyjno-rozpoznawczych, ale przy wykorzystaniu informacji oraz możliwości jakie wynikają z pozaoperacyjnych kompetencji Służby. Aktualnie to zagadnienie leży w kompetencjach Biura I SKW<sup>4</sup>.

## OSOBY UDZIELAJĄCE POMOCY PRZY WYKONYWANIU CZYNNOŚCI OPERACYJNO-ROZPOZNAWCZYCH

---

<sup>1</sup> Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego Dz.U. 2006 Nr 104 poz. 709. W dalszej części będę posługiwał się terminem „ustawa”. Jednocześnie dla zapewnienia przejrzystości tekstu oraz w związku z tematem pracy, cytując lub odwołując się do przepisów niniejszej ustawy pomijam nazwy Służba Wywiadu Wojskowego oraz SSW.

<sup>2</sup> Art. 5 ustawy zawiera katalog zadań SKW

<sup>3</sup> Termin osłona kontrwywiadowcza nie posiada definicji legalnej. Obok niego funkcjonują synonimiczne określenia takie jak ochrona kontrwywiadowcza lub zabezpieczenie kontrwywiadowcze. Decyzja użycia w niniejszej pracy pojęcia „osłona kontrwywiadowcza” wynika stąd, że występuje ona w oficjalnym dokumencie jakim jest aktualnie obowiązujący Statut Służby Kontrwywiadu Wojskowego z dnia 21.04.2017 z późniejszymi zmianami. Jedną z jednostek organizacyjnych Służby nosi nazwę Centrum Kontrwywiadowczej Osłony Wojsk Sojusznicznych, co pozwala przyjąć, że termin „osłona kontrwywiadowcza” wszedł do nomenklatury SKW.

<sup>4</sup> Interpelacja nr 7143 posła Mariusza Błaszczaka do ministra obrony narodowej w sprawie kontrowersyjnych działań Służby Kontrwywiadu Wojskowego.

<https://sejm.gov.pl/Sejm10.nsf/InterpelacjaTresc.xsp?key=DCFBHE> dostęp 5.02.2025

Jedną z podstawowych metod pracy operacyjnej jest współpraca uprawnionego organu z osobami fizycznymi niejawnie udzielającymi mu pomocy. W literaturze przedmiotu, jak i w publicystyce takie osoby określa się zwykle mianem „osobowych źródeł informacji”<sup>5</sup>, co w moim przekonaniu nie do końca jest właściwe. Współpraca z organem uprawnionym do prowadzenia czynności operacyjno – rozpoznawczych, rzeczywiście najczęściej polega na udzielaniu pomocy poprzez dostarczanie informacji, niemniej pojęcie współpracy jest szersze niż samo tylko informowanie organu. Współpraca obejmuje również wykonywanie innych zadań, takich jak np. udostępnianie ruchomości bądź nieruchomości, dzielenie się wiedzą ekspercką, legendowanie działań operacyjnych, udział w działaniach dezinformacyjnych, dezintegracyjnych czy też realizowanie innych zadań niepolegających wyłącznie na dostarczaniu informacji. W związku z powyższym w dalszej części pracy, w odniesieniu do SKW będę posługiwał się terminem „osoba udzielająca pomocy”, gdyż jest to określenie nie tylko merytorycznie poprawne, ale również zgodne z terminologią zastosowaną przez ustawodawcę w ustawie o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego.

Przepisy regulujące zasady współpracy SKW z osobami udzielającymi jej pomocy zostały ujęte w artykułach 40, 41 ust. 1 i ust. 3 ustawy, oraz w art. 39 ust. 3 w zw. z art. 39 ust. 2 i ust. 2a oraz w art. 27a ustawy. Z uwagi na zakres przedmiotowy niniejszej pracy wyżej wymienione przepisy zostaną omówione przede wszystkim pod kątem ich zastosowania w działaniach operacyjnych tworzących osłonę kontrwywiadowczą Służby Kontrwywiadu Wojskowego. Takie ujęcie nie wyczerpuje oczywiście całej problematyki współpracy SKW z osobami udzielającymi jej pomocy, ale odmienne podejście wiązałoby się z istotnym wykroczeniem poza ramy wyznaczone przez temat pracy. Należy zauważyć, że przepis art. 40 ustawy, który wprowadził możliwość korzystania przez SKW z pomocy osób niebędących jej funkcjonariuszami jest odpowiednikiem przepisów zawartych w art. 22 ust. 1 ustawy o Policji<sup>6</sup>, art. 36 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu<sup>7</sup>, art. 36 ust. 1 ustawy o Żandarmerii Wojskowej<sup>8</sup>, art. 25 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym<sup>9</sup>, art. 9 b ust. 1 ustawy o Straży Granicznej<sup>10</sup>, art. 23 zc ustawy o Służbie Więziennej<sup>11</sup>, art. 11z ustawy o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych, dotyczącej m.in. prowadzenia czynności operacyjno – rozpoznawczych

---

<sup>5</sup> *Patrz preambula do ustawy z dnia 18 października 2006 r. o ujawnianiu informacji o dokumentach organów bezpieczeństwa państwa z lat 1944-1990 oraz treści tych dokumentów Dz. U. 2006 Nr 218 poz. 1592.*

<sup>6</sup> Ustawa z dnia 6 kwietnia 1990 r. o Policji Dz. U. 1990 Nr 30 poz. 179

<sup>7</sup> Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu Dz. U. 2002 Nr 74 poz. 676

<sup>8</sup> Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych Dz. U. 2001 Nr 123 poz. 1353

<sup>9</sup> Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym Dz. U. 2006 Nr 104 poz. 708 dalej ustawa o CBA

<sup>10</sup> Ustawa z dnia 12 października 1990 o Straży Granicznej Dz. U. 1990 Nr 78 poz. 462

<sup>11</sup> Ustawa z dnia 9 kwietnia 2010 r. o Służbie Więziennej Dz. U. 2010 Nr 79 poz. 523

przez Biuro Nadzoru Wewnętrznego<sup>12</sup> oraz art. 128. 1 ustawy o Krajowej Administracji Skarbowej<sup>13</sup>. Wymienione przepisy regulują zagadnienie korzystania w ramach czynności operacyjno – rozpoznawczych z pomocy osób udzielających jej uprawnionym organom. W związku z tym literatura przedmiotu jaka powstała na kanwie analizy tych przepisów, może, przy zachowaniu zasady odpowiedniości mieć znaczenie przy ocenie przepisów ustawy o SKW i SWW regulujących omawiane tu zagadnienie.

W przepisach art. 40 ustawy oraz 41 ust. 1 i 3 ustawy, ustawodawca określił kto może, a właściwie kto nie może zostać osobą udzielającą Służbie pomocy. Przepis art. 40. 1. ustawy stanowi, że SKW przy wykonywaniu swoich zadań może korzystać, z zastrzeżeniem art. 41, z pomocy osób niebędących jej funkcjonariuszami. W art. 41 ust. 1 ustawy umieszczony został katalog wyłączeń podmiotowych, czyli wykaz stanowisk oraz zawodów zaufania publicznego, których piastowanie lub wykonywanie wyłącza możliwość niejawną współpracę ze służbą. Te wyłączenia mogą mieć charakter względny lub bezwzględny. Względny charakter wyłączenia podmiotowego polega na możliwości anulowania w konkretnym przypadku ustawowego zakazu tajnej współpracy pod warunkiem uprzedniego uzyskania stosownej zgody (art. 41 ust. 3 ustawy). Bezwzględne wyłączenie podmiotowe oznacza, że Służba nigdy, w żadnych warunkach nie może przy wykonywaniu swoich zadań korzystać z tajnej współpracy osób piastujących wymienione stanowiska lub wykonujących zawody zaufania publicznego.

## **UDZIELENIE POMOCY PRZY CZYNNOŚCIACH INNYCH NIŻ OPERACYJNO–ROZPOZNAWCZE**

W tym miejscu należy udzielić odpowiedzi na pytanie, czy współpraca z osobami, o których mowa w art. 40 ustawy ma zawsze charakter niejawną oraz czy jest ona zarezerwowana wyłącznie dla działań operacyjno–rozpoznawczych, czy też przeciwnie, dotyczy wszystkich rodzajów czynności prowadzonych przez SKW. Zgodnie z art. 25 ustawy, w granicach zadań, o których mowa w art. 5 ustawy, funkcjonariusze<sup>14</sup> SKW wykonują czynności: operacyjno-rozpoznawcze, analityczno-informacyjne oraz wynikające z przepisów ustawy o ochronie informacji niejawnych<sup>15</sup>.

Konstrukcja przepisu art. 40 ust. 1 ustawy daje podstawę, aby zakładać, że współpraca nie musi mieć charakteru tajnego. Przemawia za tym treść pierwszego zdania art. 40. ust 1. ustawy, z którego wynika, że korzystanie z pomocy osób niebędących funkcjonariuszami nie musi mieć charakteru tajnego i nie jest ograniczone wyłącznie do

---

<sup>12</sup> Ustawa z dnia 21 czerwca 1996 r. o o szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych Dz. U. 1996 Nr 106 poz. 491

<sup>13</sup> Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej Dz. U. 2016 poz. 1947 dalej ustawa o KAS

<sup>14</sup> W art. 24 ustawy, prawa i obowiązki żołnierzy zawodowych wyznaczonych na stanowiska służbowe w SKW zostały, przy zachowaniu zasady odpowiedniości zrównane prawami i obowiązkami funkcjonariuszy SKW. W związku z powyższym w każdym przypadku gdy mowa jest o funkcjonariuszu SKW, należy to odnosić również do żołnierza zawodowego wyznaczonego na stanowisko służbowe w SKW.

<sup>15</sup> Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych Dz. U. 2010 Nr 182 poz. 1228 dalej ustawa o o.i.n.

czynności operacyjno – rozpoznawczych. Niejawność współpracy oraz przypisanie jej wyłącznie do działań operacyjnych wynika dopiero z treści drugiego zdania interpretowanego przepisu. W przeciwieństwie np. do ustawy o Policji, nie jest jednak możliwe przyjęcie stanowiska zakładającego, że świadczona Służbie pomoc może mieć również charakter jawny<sup>16</sup>. Jawność współpracy wyklucza bowiem art. 40 ust. 6 ustawy, który nakłada na osobę, o której mowa w ust. 1 obowiązek zachowania w tajemnicy faktu oraz okoliczności związanych z udzieleniem przez nią pomocy. Dotyczy to każdej osoby, która w tym trybie udzieliła pomocy, a nie tylko osoby udzielającej pomocy w związku z wykonywaniem przez SKW czynności operacyjno – rozpoznawczych. Kolejna sprawa to czy, i jeżeli tak, to w jakim zakresie jest możliwe korzystanie z pomocy osób, o których mowa w art. 40 ustawy. O ile wykorzystanie tej pomocy w toku czynności operacyjno – rozpoznawczych nie budzi żadnej wątpliwości, o tyle w przypadku dwóch pozostałych rodzajów czynności realizowanych przez SKW sprawa nie jest już tak jednoznaczna. Zgodnie z art. 25 pkt. 2 ustawy, funkcjonariusze SKW wykonują m.in. czynności analityczno – informacyjne. Pojęcie czynności analityczno – informacyjnych w polskim systemie prawnym nie posiada definicji legalnej<sup>17</sup>. Poza art. 25 ustawy, żaden powszechnie obowiązujący akt prawny, nie zawiera regulacji precyzujących sposób wykonywania tych czynności przez SKW. Wobec tego, z uwagi na przepis zawarty w pierwszym zdaniu art. 40 ust. 1 ustawy oraz art. 25 ustawy, Służba może korzystać z pomocy osób, o których mówi art 40 ustawy przy wykonywaniu czynności analityczno – informacyjnych. Trzecim obszarem aktywności ustawowej SKW jest ochrona informacji niejawnych w granicach jakie wyznacza ustawa o ochronie informacji niejawnych. Zgodnie z przedstawionym wyżej wywodem dopuszczalne jest korzystanie z możliwości jakie daje art. 40 ustawy do realizacji zadań innych niż operacyjno – rozpoznawcze. O ile w przypadku czynności analityczno – informacyjnych nie budzi to wątpliwości, o tyle w przypadku czynności realizowanych na podstawie ustawy o ochronie informacji niejawnych sprawa wygląda diametralnie inaczej. Ustawa o ochronie informacji niejawnych przewiduje możliwość powoływania oraz korzystania z pomocy biegłych i specjalistów (art. 12 ust. 1 pkt 7 ustawy o o.i.n.). Należy jednak mieć na względzie, że powołanie tych osób odbywa się na podstawie przepisów ustawy o ochronie informacji niejawnych oraz w przypadku biegłych na podstawie art. 84 § 1 kodeksu postępowania administracyjnego, a nie art. 40 ustawy. Zatem w zakresie czynności realizowanych na podstawie ustawy o ochronie informacji niejawnych należy przyjąć niedopuszczalność zastosowania art. 40 ustawy. Wyłączenie możliwości zastosowania art. 40 ustawy wynika z tego, że współpraca z osobą, o której w nim mowa musi mieć charakter niejawni, podczas gdy czynności realizowane na podstawie ustawy o ochronie informacji

---

<sup>16</sup> Art. 22 ustawy o Policji. Dalej ustawa oP

<sup>17</sup> Piotr Chlebowicz, Czynności analityczno-informacyjne w polskim porządku prawnym. Prawo w działaniu. Sprawy Karne 51/2022 [https://pzd.iks.gov.pl/wp-content/uploads/2022/09/02\\_Pzd51.pdf](https://pzd.iks.gov.pl/wp-content/uploads/2022/09/02_Pzd51.pdf) Dostęp 2.01.2024

niejawnych, a w szczególności art. 12 ustawy o o.i.n., mają zawsze charakter jawny, w tym znaczeniu, że są dostępne dla kontrolowanego podmiotu.

## **POJĘCIE OSOBY NIEBĘDĄCEJ FUNKCJONARIUSZEM**

Kwestią wzbudzającą najwięcej kontrowersji jest ustalenie występującego w art. 40 ustawy, właściwego znaczenia, pojęcia „osób niebędących funkcjonariuszami SKW”. Rozstrzygnięcie tej sprawy jest szczególnie ważne w kontekście osłony kontrwywiadowczej struktur samej Służby. Przyjęcie takiego bądź innego stanowiska w znaczący sposób wpływa na możliwości operacyjne, gdyż poszerza lub zawęża bazę werbunkową. W literaturze przedmiotu ukształtowały się dwa przeciwstawne stanowiska. Zwolennicy pierwszego z nich kategorycznie wykluczają możliwość wykorzystania funkcjonariuszy danej służby w charakterze osób niejawnie udzielających pomocy swojej macierzystej służbie. Można zatem powiedzieć, że na gruncie ustawy o SKW i SWW ich stanowisko wpływa na powiększenie katalogu wyłączeń podmiotowych (art 41 ust. 1 ustawy) o funkcjonariuszy SKW oraz żołnierzy zawodowych żołnierzy zawodowych wyznaczonych na stanowiska służbowe w SKW. W opozycji do tego poglądu stoją ci, którzy uważają, że służba ma pełne prawo korzystać z niejawnej pomocy swoich funkcjonariuszy w szczególności w celu zwalczania przestępczości wewnątrzorganizacyjnej.

Na gruncie przepisów ustawy o Policji swoją opinię przedstawił Krzysztof Horosiewicz, którego zdaniem, Policja wykonując czynności operacyjno-rozpoznawcze, nie może korzystać z niejawnej pomocy funkcjonariuszy Policji. Wynika to jego zdaniem wprost z art. 22 ust. 1 ustawy o Policji, który zezwala Policji na korzystanie przy wykonywaniu swych zadań tylko z pomocy osób niebędących policjantami. Swoje stanowisko podparł on odwołaniem się do opinii Biura Prawnego nr KGP PL-549/08/pf-15/08/AP z 29.01.2008 r., której jednak nie zacytował z uwagi na to, że jest to dokument niejawny<sup>18</sup>. Analogiczny pogląd wyraził Piotr Herbowski, który analizując ustawę o Policji, ustawę o Straży Granicznej oraz ustawę o Żandarmerii Wojskowej zauważył, że jedynym ograniczeniem podmiotowym dotyczącym Policji, SG i ŻW jest zakaz korzystania z pomocy, odpowiednio policjantów, funkcjonariuszy SG i żołnierzy ŻW<sup>19</sup>. Możliwość werbunku funkcjonariuszy Policji oraz SG, autor widzi jedynie na gruncie ustawy z dnia 9 listopada 2017 r. o zmianie ustawy o niektórych uprawnieniach pracowników urzędu obsługującego ministra właściwego do spraw wewnętrznych oraz funkcjonariuszy i pracowników urzędów nadzorowanych przez tego ministra oraz niektórych innych ustaw<sup>20</sup>. Przedmiotowa ustawa zezwala, aby wyspecjalizowana

---

<sup>18</sup> Krzysztof Horosiewicz, *Współpraca policjantów z osobowymi źródłami informacji*. Warszawa 2015, s. 97.

<sup>19</sup> Piotr Herbowski, *Poufne osobowe źródła informacji. Aspekty kryminalistyczne i prawnodowodowe*. Str. 161. Warszawa 2018

<sup>20</sup> Ustawa z dnia 9 listopada 2017 r. o zmianie ustawy o niektórych uprawnieniach pracowników urzędu obsługującego ministra właściwego do spraw wewnętrznych oraz funkcjonariuszy i pracowników urzędów nadzorowanych przez tego ministra oraz niektórych innych ustaw Dz.U. 2018 Nr 106 poz. 138 dalej ustawa o sz.f.s.n.

jednostka organizacyjna MSWiA, jaką jest Biuro Nadzoru Wewnętrznego mogła korzystać z tajnej pomocy m.in. funkcjonariuszy oraz pracowników służb podległych Ministrowi Spraw Wewnętrznych i Administracji<sup>21</sup>. Biuro Nadzoru Wewnętrznego w stosunku do służb podległych MSWiA pełni funkcję organu, przy pomocy którego minister właściwy do spraw wewnętrznych sprawuje nadzór nad podległymi mu lub przez niego nadzorowanymi służbami, jakimi są Policja, Straż Graniczna, Służba Ochrony Państwa oraz Państwowa Straż Pożarna. Nadzór realizowany jest m.in. poprzez prowadzone przez BNW czynności operacyjno – rozpoznawcze, obejmujące również pozyskiwanie agentury spośród funkcjonariuszy Policji, SG, SOP i strażaków PSP. Herbowski wyklucza jednak możliwość pozyskiwania przez BNW do niejawnej współpracy inspektorów oraz ekspertów tego Biura. W jego opinii, w świetle prawa dopuszczalne jest natomiast pozyskiwanie do niejawnej współpracy żołnierzy ŻW przez służby specjalne lub służby policyjne<sup>22</sup>. Jak można wnioskować dopuszcza on możliwość pozyskiwania w charakterze osób niejawnie udzielających pomocy będących funkcjonariuszami czy żołnierzami organów uprawnionych do prowadzenia działań operacyjnych przez inne organy prowadzące analogiczną działalność, ale odmawia on tego prawa jednostkom organizacyjnym odpowiedzialnym za bezpieczeństwo wewnętrzne ich macierzystych organów. Autor dostrzega ryzyko jakie wiąże się z przyjęciem takiego rozwiązania, ale uważa, że można je zniwelować poprzez zapewnienie przez przełożonych właściwego nadzoru nad swoimi funkcjonariuszami (żołnierzami) wykonującymi czynności operacyjne, w ramach, których niejawnie korzystają z pomocy funkcjonariuszy (żołnierzy) innych organów prowadzących czynności operacyjno -rozpoznawcze<sup>23</sup>. Ryzyko jakie identyfikuje, posługując się przykładem działań funkcjonariuszy BNW, to: narażenie osób przekazujących informacje na zarzut ujawnienia informacji niejawnych osobom do tego nieuprawnionym oraz zarzut podżegania przez funkcjonariuszy BNW do ujawnienia im tych informacji. Jak twierdzi, w konkretnej sytuacji faktycznej obie strony tej relacji mogą być również narażone na odpowiedzialność karną z art. 231 kk<sup>24</sup>. Herbowski słusznie dostrzega ryzyko korzystania w ramach pracy operacyjnej z możliwości jakie uprawnionemu organowi daje niejawną współpracę z osobami funkcjonującymi w szeregach innej służby, niemniej wybrany przez niego przypadek, który miałby to ilustrować nie do końca jest trafny. Ustawa, powołująca instytucję Inspektora Nadzoru Wewnętrznego oraz kierowane przez niego Biuro Nadzoru Wewnętrznego, wyposażała BNW w kompetencje do prowadzenia działań operacyjno – rozpoznawczych wobec funkcjonariuszy Policji, SG, SOP, strażaków PSP oraz pracowników cywilnych tych służb (art.11j ustawy o sz.f.s.n.). Prowadzenie pracy operacyjnej zawsze wiąże się z korzystaniem z pomocy osób udzielających jej w sposób niejawni. Przywołana ustawa, podobnie jak i inne ustawy

---

<sup>21</sup> Ibidem str. 161

<sup>22</sup> Ibidem str. 162

<sup>23</sup> Ibidem str. 162

<sup>24</sup> Ibidem str. 162

regulujące czynności operacyjno – rozpoznawcze milczy na temat pozyskiwania tą metodą również i informacji niejawnych. Należy jednak pamiętać, że jedną z cech pracy operacyjnej jest jej odformalizowanie na poziomie wykonawczym, wobec czego przepisy ustawy o ochronie informacji niejawnych nie mogą tu mieć żadnego zastosowania. Nie zmienia to oczywiście faktu, że w sensie formalnym przekazanie informacji niejawnej w ramach dialogu operacyjnego wywołuje po stronie odpowiedzialnej za ich ochronę co najmniej odpowiedzialność dyscyplinarną oraz z uwagi na niewłaściwe postępowanie z informacjami niejawnymi może być przesłanką do wszczęcia kontrolnego postępowania sprawdzającego<sup>25</sup>. Problem „obrotu” informacjami niejawnymi, a nawet szerzej informacjami podlegającymi ochronie, w toku działań operacyjnych jest nadal istotnym wyzwaniem dla wszystkich uczestników tych działań. Dogłębne omówienie tej kwestii wykracza jednak poza ramy niniejszej pracy. Można jedynie skonstatować, że w obecnym stanie prawnym nie ma możliwości unormowania obiegu informacji niejawnych w innym trybie niż wynika to z przepisów ustawy o ochronie informacji niejawnych, a więc nie jest możliwe zharmonizowanie trybu właściwego dla czynności operacyjno – rozpoznawczych z przepisami ustawy o ochronie informacji niejawnych.

W komentarzu do ustawy o Centralnym Biurze Antykorupcyjnym, Stanisław Hoc i Przemysław Szustakiewicz zwrócili uwagę na funkcjonujące w strukturze tej służby Biuro Kontroli i Spraw Wewnętrznych, odpowiedzialne m.in. za bezpieczeństwo wewnętrzne. Autorzy uważają, że obecnie nie jest możliwe, aby ta jednostka organizacyjna pozyskiwanie do współpracy z CBA funkcjonariuszy tej służby (art. 25 ust. 1 ustawy o CBA). Tym niemniej, realistycznie oceniając sytuację, zakładają, że BKiSW „niewątpliwie korzysta z pomocy funkcjonariuszy” (CBA), ale ich zdaniem nie powinno to być tajna współpraca<sup>26</sup>. Zaprezentowana opinia jest wewnętrznie sprzeczna. Autorzy przyjmują za niedopuszczalne pozyskanie do współpracy przez BKiSW funkcjonariuszy CBA, a jednocześnie uznają, że BKiSW może korzystać z takiej współpracy o ile nie jest ona tajna. Zdanie pierwsze art. 25 ust. 1 ustawy o CBA mówi o korzystaniu z pomocy osób niebędących funkcjonariuszami tej służby, nie przesądza jednak, że ta współpraca ma być tajna i mieścić się wyłącznie w obrębie czynności operacyjno – rozpoznawczych. Przyjmując, że pojęcie „nie będących funkcjonariuszami”, wyklucza funkcjonariuszy CBA jako udzielających pomocy tej służbie, należy stwierdzić, że bez względu na to czy współpraca ma charakter jawny czy tajny żaden funkcjonariusz CBA nie może zostać uznany za osobę udzielającą pomocy w rozumieniu art. 25 ust. 1 ustawy o CBA. Niezależnie od tego absolutnie nie można się zgodzić z poglądem, że współpraca z BKiSW, czy jednostką organizacyjną innej służby odpowiedzialnej za bezpieczeństwo wewnętrzne może mieć jawny charakter. Ochrona bezpieczeństwa osób udzielających pomocy uprawnionym organom należy do podstawowych obowiązków instytucji

---

<sup>25</sup> Art. 33 ust. 1 w związku z art. 24 ust.2 pkt 6 ustawy o ochronie informacji niejawnych.

<sup>26</sup> Stanisław Hoc i Przemysław Szustakiewicz, Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz, wyd. II <https://sip.lex.pl/komentarze-i-publicacje/komentarze/ustawa-o-centralnym-biurze-antykorupcyjnym-komentarz-wyd-ii-587334427> Dostęp 30.12.2024.

korzystających z ich pomocy. Osoba współpracująca z jednostką tzw. pionu wewnętrznego jest narażona na szereg niebezpieczeństw, z których ostracyzm własnego środowiska jest najmniejszym problemem. Jeżeli ta współpraca jest częścią działań operacyjnych, a tak jest zawsze, gdy przedmiotem współpracy jest przekazywanie informacji, to te działania muszą być niejawne. Informacje o tych działaniach oraz informacje uzyskane w ich wyniku są informacjami niejawnymi, oznaczonymi odpowiednio klauzulą ściśle tajne lub tajne (art. 5 ust. 1 pkt 5 i 6 ustawy o o.i.n.).

Dostępne w języku polskim informacje na temat przepisów regulujących współpracę służb policyjnych wybranych państw : Wielkiej Brytanii, ustawa w sprawie uregulowania środków śledczych<sup>27</sup>, Holandii, kodeks postępowania karnego<sup>28</sup> i USA, wytyczne Prokuratora Generalnego w sprawie określenia zasad użycia tajnych informatorów<sup>29</sup>, z osobami udzielającymi im niejawnej pomocy wskazują, że niezależnie od dzielących je różnic, ich wspólną cechą jest podkreślenie, że osoba udzielająca pomocy nie jest funkcjonariuszem.

Diametralnie przeciwne stanowisko co możliwości korzystania przez Policję z pomocy swoich funkcjonariuszy zajęli Tomasz Cichoń i Rafał Kręgulec. Ich zdaniem zastosowana przez K.Horosiewicza wykładnia literalna art. 22 ust. 1 ustawy oP. nie wystarcza, aby ustalić właściwe znaczenie tego przepisu. Autorzy, odwołując się do reguł wnioskowania prawniczego, interpretując ten przepis posługując się regułą *argumentum a maiori ad minus*, co należy tutaj tłumaczyć, komu wolno więcej, temu tym bardziej wolno mniej. Jak piszą, „Jeżeli z treści przepisu wynika, że można więcej, to wnioskujemy, że wolno i mniej. Jeżeli ktoś jest zobowiązany do czegoś więcej to jest zobowiązany do czegoś mniej. System prawny powinien być nie tylko spójny, ale także zupełny. Jeżeli jakaś sytuacja powinna być rozstrzygnięta przez prawo a ono tej sytuacji nie reguluje albo nie reguluje wprost, to należy ją uzupełnić w drodze analogii, albo przez analogię z prawa lub w drodze wykładni prawa innej niż językowa”<sup>30</sup>. Zdaniem cytowanych autorów przepis art. 22 ust. 1 ustawy oP. nie jest normą prawną o charakterze zakazującym, ale normą uprawniającą, wobec czego uważają, że zastosowanie tutaj reguły *a maiori ad minus* jest w pełni zasadne. Ich zdaniem, art. 22 ust. 1 ustawy oP. nadając tej formacji uprawnienie do korzystania z pomocy osób niebędących jej funkcjonariuszami, w ogóle nie odnosi się do możliwości korzystania z niejawnej pomocy funkcjonariuszy policji, a tym bardziej niczego on w tym przedmiocie nie zakazuje. W ich opinii: „Kuriozalny byłby zresztą zapis ustawowy, że Policja przy wykonywaniu swoich zadań może korzystać z pomocy osób będących

---

<sup>27</sup> Robert Netczuk, Tajny współpracownik policji na tle porównawczym, str. 146. Katowice 2006

<sup>28</sup> Ibidem str. 224

<sup>29</sup> Ibidem str. 229

<sup>30</sup> Tomasz Cichoń, Rafał Kręgulec, Możliwości niejawnej współpracy w ramach czynności operacyjno – rozpoznawczych funkcjonariuszy Biura Spraw Wewnętrznych Policji z innymi funkcjonariuszami Policji, str. 56 w „Oblicza bezpieczeństwa a współczesne zagrożenia”. Kraków 2016

funkcjonariuszami. Do wykonywania ustawowych zadań zobligowany jest przecież ustawą każdy policjant<sup>31</sup>.

Obok argumentacji prawnej, swoje stanowisko podpierają również argumentami natury czysto użytecznej. Zdaniem tych autorów, Policja, aby właściwie realizować swoje zadania musi mieć prawo pozyskiwania osobowych źródeł informacji wśród policjantów, gdyż w przeciwnym razie wykrywanie przestępstw i ściganiu ich sprawców ze środowiska policyjnego byłoby prawie niemożliwe, a to: „prowadziłyby do absurdalnych rozwiązań prawnych, a w szczególności zaś stawiałyby pod znakiem zapytania konstytucyjną zasadę demokratycznego państwa prawa”<sup>32</sup>.

## **ARTYKUŁ 128 UST. 1 USTAWY O KAS**

W odmienny sposób, unikając interpretacyjnej dychotomii skonstruowany został art. 128 ust. 1 ustawy o KAS. Przepis tego artykułu stwierdza: „Funkcjonariusz wykonujący czynności operacyjno-rozpoznawcze przy wykonywaniu tych czynności może korzystać z pomocy innych osób”. Jak zatem widać, po pierwsze zakres udzielanej pomocy został ograniczony wyłącznie do czynności operacyjno – rozpoznawczych. Po drugie, w związku z tym, że adresatem dyspozycji tego przepisu jest funkcjonariusz a nie służba, to pod pojęciem inne osoby należy rozumieć każdego kto nie jest tym konkretnym funkcjonariuszem wykonującym czynności operacyjno – rozpoznawcze. Tym samym osobą udzielającą pomocy może być również inny funkcjonariusz KAS. Przyjęte rozwiązanie jest niewątpliwie bardziej przejrzyste i zrozumiałe. Jest to przesłanka za przyjęciem tezy, świadczącej, że ustawodawca dopuszcza możliwość korzystania przez służbę uprawnioną do prowadzenia działań operacyjnych, z niejawną pomocą świadczoną przez jej funkcjonariuszy. Przedstawiona teza może mieć oczywiście znaczenie przy interpretacji art. 40 ust. 1 ustawy i jego odpowiedników, niemniej nie ma ona charakteru rozstrzygającego, a jedynie pomocniczy. Jest oczywiste, że poszczególne służby mają różne uprawnienia. Powody, dla których ustawodawca zdecydował się je różnicować nie zawsze są jasne i merytorycznie uzasadnione<sup>33</sup>.

## **USTALENIE RATIO LEGIS ART. 40 USTAWY**

Ustalenie właściwego znaczenia przepisu art. 40 ust.1 ustawy, a w szczególności terminu „niebędących jej funkcjonariuszami” zależy od prawidłowego odczytania motywów ustawodawcy, który zdecydował, że ten przepis znalazł się w ustawie właściwie w takim a nie innym kształcie. Aby to zrobić należy na art. 40 ust. 1 ustawy spojrzeć przez pryzmat art. 27a ustawy oraz Zarządzenia Ministra Spraw Wewnętrznych

---

<sup>31</sup> Ibidem str.56

<sup>32</sup> Ibidem str. 56

<sup>33</sup> Przykładem jest Inspektorat Wewnętrzny Służby Więziennej, który jako jedyny organ uprawniony do prowadzenia czynności operacyjno – rozpoznawczych ma prawo wykorzystywać w tych działaniach informacje uzyskane w toku postępowania sprawdzającego art. 72 ust. 1 pkt 7 ustawy o ochronie informacji niejawnych.

Nr 0073/84 z dnia 27 grudnia 1984 r., regulującego m.in. pozyskiwanie osobowych źródeł informacji przez Zarząd Ochrony Funkcjonariuszy MSW.

Wprowadzenie art. 27a ustawy<sup>34</sup> poszerzyło zakres oportunistycznego procesu poprzez możliwość odstąpienia od wynikającego z art. 27 ust. 3 ustawy, obowiązku złożenia przez Szefa SKW zawiadomienia o uzasadnionym podejrzeniu popełnienia przestępstwa oraz osobie, która według uzyskanych przez SKW informacji lub materiałów może być jego sprawcą, w zamian za podjęcie tajnej współpracy przez osobę, której dotyczyłoby to zawiadomienie<sup>35</sup>. Przysługujące Szefowi SKW uprawnienie zostało obwarowane szeregiem warunków, od których spełnienia uzależnione jest uruchomienie procedury opisanej w art. 27a ustawy. Przepis niniejszego artykułu ma zastosowanie jedynie w przypadku, gdy informacje lub materiały uzyskane przez SKW podczas realizacji zadań, o których mowa w art. 5 ust. 1 ustawy wskazują na popełnienie przestępstwa szpiegostwa albo uprawdopodobniają działalność zmierzającą do popełnienia przestępstwa o charakterze terrorystycznym. Sprawca przestępstwa szpiegostwa albo podejrzewany o przestępstwa o charakterze terrorystycznym musi świadomie i dobrowolnie ujawnić wszelkie okoliczności popełnionego czynu lub prowadzonej działalności oraz jednocześnie zobowiązać się do podjęcia tajnej współpracy z SKW (art. 27a ust. 2 ustawy). Wówczas Szef SKW po uznaniu, że za odstąpieniem od obowiązku wynikającego z art. 27 ust. 3 ustawy przemawiają względy bezpieczeństwa państwa, może skorzystać ze swego uprawnienia. Zarówno doświadczenie zawodowe jak i historia służb specjalnych wskazują, że nie można wykluczyć przypadku, gdy sprawcą przestępstwa szpiegostwa lub podejrzewanym o popełnienie przestępstwa o charakterze terrorystycznym będzie funkcjonariusz SKW. Ponieważ ustawa milczy na temat statusu osoby, o której mowa w art. 27a, wobec czego obowiązek nawiązania tajnej współpracy z SKW odnosi się również do jej funkcjonariusza, o ile oczywiście będzie on zainteresowany takim rozwiązaniem. Użycie przez ustawodawcę określenia „tajna współpraca” oraz odesłanie do art. 39 ust. 3, a w szczególności do art. 40 ustawy nie pozostawia wątpliwości, że funkcjonariusz SKW, który zdecydował się spełnić warunki, o których mowa w art. 27a ustawy, musi być traktowany jako osoba udzielająca pomocy przy realizacji czynności operacyjno - rozpoznawczych w rozumieniu art. 40 ustawy. W tej sytuacji należy przyjąć, że art. 27a ustawy, stanowi *lex specialis* w stosunku do art. 40 ustawy, a więc wyjątkowo, dopuszcza możliwość skorzystania przez SKW z niejawniej pomocy udzielanej jej przez funkcjonariusza tej Służby. Należy zwrócić uwagę, że funkcjonariusz, który znalazłby się w sytuacji, o której mówi art. 27a ustawy, byłby formalnie narażony na ryzyko wszczęcia

---

<sup>34</sup> Analogiczny przepis, tj. art. 22b został wprowadzony do ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu.

<sup>35</sup> Dariusz Pożaroszczak, Artykuł 22b ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu jako nowy wyjątek od zasady legalizmu procesowego – analiza wybranych problemów. Prokuratura i Prawo 6/2019

kontrolnego postępowania sprawdzającego<sup>36</sup>. Problemy jakie wynikają z tego tytułu mogą nawet doprowadzić do dekonspiracji współpracy i zaprzepaszczenia szansy zinfiltrowania wrogiego środowiska. Aby tego uniknąć, zasadnym byłoby takie zinterpretowanie sytuacji tego funkcjonariusza, aby uznać, że nawiązanie tajnej współpracy jest wystarczającym powodem odstąpienia od wszczęcia kontrolnego postępowania sprawdzającego. Na marginesie warto zwrócić uwagę na uwypuklony w art. 27a ustawy ofensywny aspekt pracy kontrwywiadowczej, określanej w literaturze przedmiotu mianem kontrszpiegostwa<sup>37</sup>. Jest to o tyle ważne, ponieważ wprowadzenie tego przepisu wskazuje, że SKW wpisuje się w trend, obowiązujący już od pewnego czasu w świecie służb kontrwywiadowczych polegający na wyjściu z roli typowo defensywnej na rzecz służby kreującej sytuację operacyjną w obszarze powierzonej jej odpowiedzialności<sup>38</sup>.

W latach 1984 do 1990 w strukturze Ministerstwa Spraw Wewnętrznych funkcjonowała jednostka organizacyjna o nazwie Zarząd Ochrony Funkcjonariuszy MSW<sup>39</sup>. Była to struktura, wchodząca w skład Służby Bezpieczeństwa odpowiedzialna za bezpieczeństwo wewnętrzne resortu spraw wewnętrznych, uprawniona m.in. do prowadzenia czynności operacyjno – rozpoznawczych. W latach 1983 -1990, a więc w okresie obejmującym istnienie ZOF czynności operacyjno – rozpoznawcze regulowała ustawa z dnia 14 lipca 1983 r. o urzędzie Ministra Spraw Wewnętrznych i zakresie działania podległych mu organów<sup>40</sup>. W art. 6 przywołanej ustawy, uprawnienia do prowadzenia czynności operacyjno–rozpoznawczych zostały nadane funkcjonariuszom Służby Bezpieczeństwa i Milicji Obywatelskiej. Z kolei art. 15 tej ustawy wyposażył SB i MO przy wykonywaniu swych zadań z dziedziny bezpieczeństwa Państwa i porządku publicznego w możliwość korzystania z pomocy obywateli. Użycie pojęcia „obywatele”, oznacza, że ustawodawca dopuszczał możliwość pozyskania o tajnej współpracy każdego obywatela PRL, a więc i funkcjonariuszy służb podległych MSW. Praca operacyjna ZOF została uregulowana Zarządzeniem Ministra Spraw Wewnętrznych nr 0073/84 z dnia 27 grudnia 1984 r. w sprawie uprawnień oraz metod i środków pracy pionu ochrony funkcjonariuszy i pracowników cywilnych. Na podstawie tego aktu prawnego ZOF miał prawo pozyskiwać osobowe źródła informacji także spośród personelu MSW. O ile co do pracowników cywilnych, zarządzenie nie wprowadzało żadnych ograniczeń, o tyle pozyskiwanie funkcjonariuszy zostało wykluczone, poza dwoma wyjątkami (§ 4 Zarządzenia) . Pierwszy dotyczył możliwości werbowania funkcjonariuszy

---

<sup>36</sup> Art.33 ustawy o ochronie informacji niejawnych.

<sup>37</sup> Damian Przybylski, Działalność kontrwywiadowcza FBI. Łomianki 2024 str. 37 i n.

<sup>38</sup> Ibidem str. 37

<sup>39</sup> W strukturach Wojewódzkich Urzędów Spraw Wewnętrznych istniały Inspektoraty Ochrony Funkcjonariuszy, czyli terenowe struktury ZOF. Daniel Wicenty – „Kiszczakowska „policja w policji”. O Zarządzie Ochrony Funkcjonariuszy”. Str. 142 [https://dn-ihpan.edu.pl/images/DN2016-48-1/WA303\\_78595\\_A507-DN-R-48-1\\_Wicenty.pdf](https://dn-ihpan.edu.pl/images/DN2016-48-1/WA303_78595_A507-DN-R-48-1_Wicenty.pdf) Dostęp. 3.02.2025 r.

<sup>40</sup> Ustawa z dnia 14 lipca 1983 r.o urzędzie Ministra Spraw Wewnętrznych i zakresie działania podległych mu organów Dz.U.1983. Nr.38 poz.172 dalej ustawa o MSW

odbywających służbę wojskową w Batalionach Centralnego Podporządkowania ZOMO. Status takiego funkcjonariusza był zbliżony do statusu żołnierza zasadniczej służby wojskowej. W świetle ówczesnie obowiązującego prawa był to funkcjonariusz w służbie kandydackiej<sup>41</sup>. Podstawą nawiązania stosunku służbowego była w tym przypadku ustawa z dnia 12 listopada 1967 r. o powszechnym obowiązku obrony Polskiej Rzeczypospolitej Ludowej, podczas gdy stosunek służbowy pozostałych funkcjonariuszy MO i SB powstawał w drodze mianowania, co pociągało za sobą zróżnicowanie wewnątrz nominalnie tej samej formacji mundurowej<sup>42</sup>. Drugi wyjątek, przywidywał możliwość dokonania werbunku funkcjonariusza każdej ze służb podległych MSW, ale tylko w przypadku łącznego zaistnienia dwóch przesłanek. Sprawa, w której miało dojść do pozyskania musiała zostać zakwalifikowana do kategorii tych, które określono mianem szczególnie uzasadnionych przypadków. Sam werbunek musiał się odbyć w oparciu o materiały obciążające funkcjonariusza. Pozyskany funkcjonariusz, po zakończeniu procedury operacyjnej do której go zwerbowano podlegał zwolnieniu ze służby, ale z zachowaniem uprawnień emerytalnych<sup>43</sup>. O ile przepis pozwalający na korzystanie z niejawnej pomocy funkcjonariuszy w służbie kandydackiej nie budzi zdziwienia, bo faktycznie osoby wchodzące w skład tej grupy nie były traktowane jako pełnoprawni funkcjonariusze resortu spraw wewnętrznych o tyle sposób postępowania w stosunku do drugiej z grup tworzących bazę werbunkową ZOF daje dużo do myślenia. Po pierwsze werbunek odbywał się wyłącznie w oparciu o materiały obciążające i jak można wnioskować ich ciężar gatunkowy musiał być znaczny, skoro przekreślał dalszą karierę w MSW. Zwerbowany funkcjonariusz po ustaniu jego przydatności operacyjnej, czyli zakończeniu konkretnej procedury był ze służby zwalniany. Jest to o tyle istotne, że ZOF przedkładał ograniczenie swoich możliwości operacyjnych wynikających z prowadzenia źródła uplasowanego w strukturze MSW nad dalsze jego prowadzenie, ale przy jednoczesnym zachowaniu jego statusu funkcjonariusza MO lub SB<sup>44</sup>. Co więcej przepisy obowiązującej wówczas ustawy o urzędzie Ministra Spraw Wewnętrznych pozwalały MO i SB korzystać z niejawnej pomocy obywateli. Pojęcie „obywatel” zawiera w sobie pojęcia „funkcjonariusz MO” i „funkcjonariusz SB”. Nie byłoby zatem proceduralnych przeszkód, aby ZOF mógł prowadzić agenturę wśród funkcjonariuszy, inną niż ta pozyskana na podstawie § 4 wymienionego zarządzenia. Mimo oczywistych korzyści operacyjnych jakie by z tego wynikały, nie zdecydowano się jednak na to

---

<sup>41</sup> Art. 122 ustawy z dnia 31 lipca 1985 r. o służbie funkcjonariuszy Służby Bezpieczeństwa i Milicji Obywatelskiej, Dz.U. 1985 Nr 38 poz.181. Upřednio tę kwestię regulowały przepisy wewnętrzne Ministerstwa Spraw Wewnętrznych wydane na podstawie art 102a ustawy z dnia 31 stycznia 1959 r. o służbie funkcjonariuszy Milicji Obywatelskiej, Dz.U.1973 Nr 23 poz.136.

<sup>42</sup> Art. 5 ustawy z dnia 31 lipca 1985 r. o służbie funkcjonariuszy Służby Bezpieczeństwa i Milicji Obywatelskiej.

<sup>43</sup> Op. cit 39 str 147

<sup>44</sup> Oczywiście możliwe było kontynuowanie tajnej współpracy z tą osobą po jej odejściu ze służby, ale opuszczenie struktur MSW w naturalny sposób zmniejszało jej możliwości operacyjne w zakresie spraw pozostających w zainteresowaniu ZOF.

rozwiązanie. Uwarunkowania współpracy agenturalnej z funkcjonariuszem wskazują, że traktowano ją jako coś wyjątkowego, jako absolutne odstępstwo od normy.

Podobną prawidłowość można dostrzec w przypadku relacji zachodzącej pomiędzy art. 27a, a art. 40 ustawy. Funkcjonariusz SKW, popełniając przestępstwo szpiegostwa, uwiarygadnia się przed obcą służbą specjalną i poszerza możliwość jej infiltracji poprzez rozpoznanie metod pracy, kierunków zainteresowań czy identyfikacji jej pracowników. Podobnie wygląda to w przypadku, gdy funkcjonariusz SKW działa wewnątrz grupy terrorystycznej, zdobywając unikatową, insiderską wiedzę o jej działalności. W obu przypadkach, pierwszeństwo przed innymi okolicznościami, ustawodawca przyznał korzyściom operacyjnym, uzasadnionym względami bezpieczeństwa państwa.

Szczątkowe informacje na temat rozwiązań przyjętych w służbach policyjnych Wielkiej Brytanii, Holandii oraz USA wskazują, że obowiązujące w nich przepisy co do zasady wyłączają możliwość korzystania przez policję z niejawnej pomocy osób będących ich funkcjonariuszami.

Analiza przepisów dotyczących współpracy służb z osobami niejawnie udzielającymi pomocy, które zawarto w ustawie o MSW, Zarządzeniu nr 0073/84 Ministra Spraw Wewnętrznych, ustawie o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego, pozostałych aktualnie obowiązujących ustawach powołujących organy uprawnione do prowadzenia czynności operacyjno – rozpoznawczych, projekcie Kodeksu Pracy Operacyjnej<sup>45</sup> oraz uwzględniając informacje na temat rozwiązań przyjętych w innych państwach, pozwala ustalić co najmniej jedną, łączącą je zasadę. Zasadę polegającą na konieczności *wyodrębnienia podmiotu i przedmiotu pracy operacyjnej, a zarazem ich wyraźnego rozdzielenia. Jest to klasyczna, uniwersalna i ponadczasowa zasada oparta na doświadczeniach kolejnych pokoleń pracowników operacyjnych*. Podmiotem pracy operacyjnej są osoby, realizujące w imieniu organu jego ustawowe zadania, posługujące się środkami pracy operacyjnej. Do środków pracy operacyjnej, trzymając się systematyki przyjętej w KPO, należą m.in. „środki osobowe” (art.10 pkt.2 ppkt a) czyli osoby niejawnie udzielające pomocy. Zaliczenie „środków osobowych” do kategorii „środków pracy operacyjnej” (art. 10 projektu KPO) przesądza ich przedmiotowy charakter. Relatywizacja tej zasady, czyli odejście od jej stosowania w określonej sytuacji jest dopuszczalna, ale tylko przy zaistnieniu stypizowanych przesłanek, takich jak § 4 Zarządzenia Ministra Spraw Wewnętrznych Nr 0073/84 czy art 27a ustawy. Mając to na uwadze należy uznać, że norma prawna art. 40 ust. 1 ma charakter zakazujący, a nie uprawniający, gdyż *ratio legis* tego przepisu ma służyć właśnie oddzieleniu od siebie podmiotu i przedmiotu pracy operacyjnej<sup>46</sup>.

---

<sup>45</sup> <https://civitas.edu.pl/wp-content/uploads/2023/05/kodeks-pracy-operacyjnej-projekt-17042023.pdf> Dostęp 3.02.2025

<sup>46</sup> W świetle przedstawionej argumentacji rozwiązanie wprowadzone przez art. 128 ust. 1 ustawy o KAS należy uznać za ewenement.

## PODSUMOWANIE

Wnioski jakie wypływają z analizy przepisów skłaniają do odrzucenia możliwości uznania art. 40 ustawy za podstawę prawną korzystania przez SKW z tajnej pomocy udzielanej przez jej funkcjonariuszy, w ramach prowadzenia osłony kontrwywiadowczej własnych struktur. Z drugiej strony jest niezaprzeczalnym faktem, że Biuro I aby móc prowadzić skuteczną osłonę kontrwywiadowczą musi posiadać zdolność pozyskiwania informacji od funkcjonariuszy SKW, którzy realizując merytoryczne zadania naocznie stykają się z incydentami lub wręcz procederami godzącymi w bezpieczeństwo wewnętrzne Służby. Co więcej, ci funkcjonariusze z racji swojego doświadczenia zawodowego niejednokrotnie są w stanie fachowo ocenić rodzaj i skalę zagrożenia, przyczyniając się do ograniczenia szumu informacyjnego, groźnego zjawiska, które może doprowadzić do przeciążenia możliwości operacyjnych Biura I.

## WNIOSKI DE LEGE FERENDA

W tej sytuacji, aby pogodzić stanowisko wykluczające możliwość wykorzystania art. 40 ustawy do werbunku funkcjonariusza SKW, z koniecznością zapewnienia odpowiedniego wysokiego poziomu uzyskiwanych informacji, należy rozważyć możliwość wprowadzenia do przepisów wewnętrznych SKW instytucji „funkcjonariusza udzielającego pomocy”, jako jednej z metod pracy operacyjnej w rozumieniu projektu Kodeksu Postępowania Operacyjnego<sup>47</sup>. „Funkcjonariusz udzielający pomocy” nie byłby klasyfikowany jako osoba, o której mówi art. 40 ustawy, gdyż podstawa prawna jego działalności wynikałaby z właściwej interpretacji roty przysięgi jaką składa każdy funkcjonariusz oraz odpowiedniej interpretacji jego zakresu obowiązków służbowych.

Na koniec należy dodać, że przedstawiona propozycja rozwiązania problemu „funkcjonariusza udzielającego pomocy” jednostce organizacyjnej odpowiedzialnej na osłonę kontrwywiadowczą SKW, może zostać również zastosowana w przypadku, gdy pomoc tego funkcjonariusza będzie niezbędna dla innego pionu Służby, a okoliczności, a w szczególności uwarunkowania sytuacji operacyjnej nie będą temu stały na przeszkodzie.

## BIBLIOGRAFIA

1. Chlebowicz P., Czynności analityczno-informacyjne w polskim porządku prawnym. Prawo w działaniu, Sprawy Karne 51/2022, [https://pwd.iws.gov.pl/wp-content/uploads/2022/09/02\\_PwD51.pdf](https://pwd.iws.gov.pl/wp-content/uploads/2022/09/02_PwD51.pdf)
2. Cichoń T., Kręgulec R., Możliwości niejawnnej współpracy w ramach czynności operacyjno – rozpoznawczych funkcjonariuszy Biura Spraw Wewnętrznych Policji z innymi funkcjonariuszami Policji [w] „Oblicza bezpieczeństwa a współczesne zagrożenia”, Kraków 2016

---

<sup>47</sup> <https://civitas.edu.pl/wp-content/uploads/2023/05/kodeks-pracy-operacyjnej-projekt-17042023.pdf> Dostęp 3.02.2025

3. Herbowski P., Poufne osobowe źródła informacji. Aspekty kryminalistyczne i prawnodowodowe, Warszawa 2018
4. Hoc S., Szustakiewicz P., Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz, wyd. II, <https://sip.lex.pl/komentarze-i-publicacje/komentarze/ustawa-o-centralnym-biurze-antykorupcyjnym-komentarz-wyd-ii-587334427>
5. Horosiewicz K., Współpraca policjantów z osobowymi źródłami informacji, Warszawa 2015
6. <https://civitas.edu.pl/wp-content/uploads/2023/05/kodeks-pracy-operacyjnej-projekt-17042023.pdf>
7. Interpelacja nr 7143 posła Mariusza Błaszczaka do ministra obrony narodowej w sprawie kontrowersyjnych działań Służby Kontrwywiadu Wojskowego. <https://sejm.gov.pl/Sejm10.nsf/InterpelacjaTresc.xsp?key=DCFBHE>
8. Netczuk R., Tajny współpracownik policji na tle porównawczym, Katowice 2006
9. Pożaroszczuk D., Artykuł 22b ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu jako nowy wyjątek od zasady legalizmu procesowego – analiza wybranych problemów. Prokuratura i Prawo 6/2019
10. Przybylski D., Działalność kontrwywiadowcza FBI. Łomianki 2024
11. Ustawa z dnia 12 października 1990 o Straży Granicznej Dz. U. 1990 Nr 78 poz. 462
12. Ustawa z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej Dz. U. 2016 poz. 1947
13. Ustawa z dnia 21 czerwca 1996 r. o z szczególnych formach sprawowania nadzoru przez ministra właściwego do spraw wewnętrznych Dz. U. 1996 Nr 106 poz. 491
14. Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu Dz. U. 2002 Nr 74 poz. 676
15. Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych Dz. U. 2001 Nr 123 poz. 1353
16. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych Dz. U. 2010 Nr 182 poz. 1228
17. Ustawa z dnia 6 kwietnia 1990 r o Policji Dz. U. 1990 Nr 30 poz. 179
18. Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym Dz. U. 2006 Nr 104 poz. 708
19. Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego Dz.U. 2006 Nr 104 poz. 709
20. Ustawa z dnia 9 kwietnia 2010 r. o Służbie Więziennej Dz. U. 2010 Nr 79 poz. 523
21. Ustawa z dnia 9 listopada 2017 r. o zmianie ustawy o niektórych uprawnieniach pracowników urzędu obsługującego ministra właściwego do spraw wewnętrznych oraz funkcjonariuszy i pracowników urzędów nadzorowanych przez tego ministra oraz niektórych innych ustaw Dz.U. 2018 Nr 106 poz. 138