Solidarni z Ukrainą

Kwartalnik Policyjny

Nr 2(69)/2024
Rok XVIII
ISSN 1898-1453

CZASOPISMO
CENTRUM SZKOLENIA POLICJI
W LEGIONOWIE
www.kwartalnik.csp.edu.pl

W numerze m.in.:

■ Działalność Centralnego Biura Zwalczania Cyberprzestępczości ■ Cyberstalking ■ Informatyka śledcza ■ Cyberbezpieczeństwo w instytucjach publicznych ■ Malware ■ Ochrona dzieci i młodzieży w sieci ■ Konfiskata pojazdu ■ Służba na wodzie ■ Kynologia policyjna ■ Sport w Policji

DOŚCIGNĄĆ CYBERPRZESTĘPCÓW

W niniejszym wydaniu „Kwartalnika Policyjnego" powracamy do problematyki bezpieczeństwa w sieci. Już dawno stało się oczywiste, że żyjemy w świecie połączonym cyfrowo, jednak w ostatnim czasie dotkliwie sobie uświadamiamy, z jak wielką dynamiką cyberprzestępczości mamy do czynienia i jak ogromne straty może ona powodować.

W latach 2018–2022 prowadzone przez FBI Centrum Zgłaszania Przestępstw Internetowych (IC3) otrzymało łącznie ponad 3,2 mln skarg, które przełożyły się na stratę ponad 27,6 mld dolarów.

Według *Raportu Interpolu podsumowującego trendy przestępczości na świecie w 2022 r. (2022 Interpol Global Crime Trend Summary Report)*, opartego na danych ze 195 państw, przestępstwa finansowe i cyberprzestępczość są powodem największych obaw i przewiduje się ich największy wzrost. Interpol zaznacza, że policja musi w związku z tym nadążać za rozwojem technologicznym i dysponować niezbędną wiedzą specjalistyczną i umiejętnościami, aby radzić sobie z szybko rozwijającą się przestępczością cyfrową na szczeblu krajowym, regionalnym i międzynarodowym. Podkreśla też rolę partnerstwa i współpracy, tak by korzystać z wiedzy dostępnej w sektorze publicznym, prywatnym i akademickim.

Ze *Sprawozdania Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2023 rok* wynika, że w zeszłym roku w Polsce wzrastała aktywność różnego rodzaju grup prowadzących nielegalne działania w świecie cyfrowym, w tym haktywistów, grup cyberprzestępczych o charakterze zarobkowym, grup powiązanych z innymi państwami lub wręcz bezpośrednio działających w ramach instytucji państw-adwersarzy. Pełnomocnik prognozuje ponadto, że w kolejnych latach skala cyberataków będzie się zwiększać.

W celu lepszego monitorowania zagrożeń w sieci powoływane są krajowe systemy cyberbezpieczeństwa oraz centra zgłaszania przestępstw internetowych. W Polsce CSIRT NASK przyjmuje, analizuje i podejmuje działania oraz koordynuje reakcje na incydenty dotyczące cywilnej cyberprzestrzeni RP zgłaszane przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny, i osoby prywatne, a także na incydenty związane z publikowanymi w Internecie nielegalnymi treściami oraz zagrażającymi bezpieczeństwu dzieci. Jak wynika z raportu CERT NASK za 2023 r., liczba incydentów ciągle wzrasta. W 2023 r. było ich 80 267, czyli o ponad 100% więcej niż w 2022 r.

Najwyższa Izba Kontroli w *Informacji o wynikach kontroli „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości"* z 2022 r. podkreśliła, iż mimo że Internet stał się nieodłączną częścią naszego życia prywatnego i zawodowego, to istnieje wiele barier, które utrudniają obywatelom uzyskanie skutecznego wsparcia w sytuacji pokrzywdzenia przestępstwem.

Wskazała też, że w jednostkach Policji nie wypracowano instrukcji dla obywateli zgłaszających tego rodzaju zdarzenia, a algorytmy przyjmowania zgłoszeń stanowiły tylko ograniczoną pomoc dla funkcjonariuszy. W zleconym przez NIK badaniu ankietowani wskazali m.in., że aż 85% cyberataków, które ich dotknęły, nie zostało wyjaśnionych, zakończyło się umorzeniem postępowania lub utratą środków finansowych i danych, a tylko w 2% spraw wykryto i skazano sprawcę lub odzyskano stracone środki.

NIK oceniła natomiast pozytywnie utworzenie w styczniu 2022 r. nowej jednostki organizacyjnej Policji, wyspecjalizowanej w zwalczaniu przestępczości internetowej – Centralnego Biura Zwalczania Cyberprzestępczości (CBZC).

Charakterystyka współczesnej cyberprzestępczości i opis jej najnowszych form, geneza utworzenia Centralnego Biura Zwalczania Cyberprzestępczości, a także jego działalność to zagadnienia, o których mowa w pierwszym artykule tego wydania. Autor, policjant CBZC, zaznacza, że Biuro zajmuje się głównie zwalczaniem najbardziej zaawansowanej i zorganizowanej cyberprzestępczości, natomiast w masowej skali z tymi przestępstwami walczą inne jednostki Policji.

Jednak aby stawić czoła błyskawicznie rosnącej lawinie cyberzagrożeń, policjanci w całym kraju potrzebują wsparcia w zakresie szkolenia i rozpowszechnienia dobrych praktyk. Niebagatelna rola w tym zakresie przypada szkolnictwu policyjnemu. Chcąc przybliżyć i zaktualizować nieco wiedzę z zakresu cyberbezpieczeństwa, zaproponowaliśmy w tym numerze artykuły dotyczące informatyki śledczej, cyberstalkingu i innych zagrożeń, a także profilaktyki w obszarze bezpieczeństwa dzieci i młodzieży w sieci.

Zapraszam również do lektury opracowań spoza tematu przewodniego tego numeru. Dotyczą one bezpieczeństwa ruchu drogowego, policji wodnej, kynologii policyjnej, a także tradycji sportu w Policji.

Redaktor naczelny
mł. insp. Agnieszka Gorzałczyńska-Mróz

Grafika na podstawie: www.pixabay.com.

Nr 2(69)/2024

Kwartalnik Policyjny

Do pobrania na stronie:
www.kwartalnik.csp.edu.pl

CZASOPISMO CENTRUM SZKOLENIA POLICJI W LEGIONOWIE

Wydawca: Centrum Szkolenia Policji w Legionowie

Adres redakcji: ul. Zegrzyńska 121, 05-119 Legionowo
sekretariat tel. 47 72 558 81, faks 47 72 535 80,
e-mail: kwartalnik@csp.edu.pl

ZESPÓŁ REDAKCYJNY

Druk: Wydział Wydawnictw i Poligrafii CSP w Legionowie

Nakład: 1000 egz.

Numer zamknięto 5.07.2024 r.

RADA NAUKOWA „KWARTALNIKA POLICYJNEGO”

RADA WYDAWNICZA pod przewodnictwem Zastępcy Komendanta CSP insp. Tomasza Rylskiego

Czekamy na listy, propozycje tematów i opinie na temat zamieszczonych tekstów. Prosimy je przesyłać na adres kwartalnik@csp.edu.pl.
Redakcja zastrzega sobie prawo skracania tekstów i dokonywania w nich zmian oraz możliwość nieodpłatnego wykorzystania publikowanych materiałów na stronie internetowej www.kwartalnik.csp.edu.pl.

W NUMERZE

WSTĘP

2 AGNIESZKA GORZAŁCZYŃSKA-MRÓZ
Dosięgnąć cyberprzestępców

ZWALCZANIE CYBERPRZESTĘPCZOŚCI

5 MARIUSZ TOMCZAK
Zwalczanie cyberprzestępczości przez polską Policję

11 ZBIGNIEW BOGUSZ
Cyberstalking jako narzędzie przemocowe

16 TOMASZ KŁYS
Wykorzystanie informatyki śledczej w procesie zabezpieczania dowodów cyfrowych

OCHRONA PRZED CYBERZAGROŻENIAMI

25 PAWEŁ TOMASZEWSKI
Cyberbezpieczeństwo w instytucjach publicznych. Zagrożenia i sposoby ochrony

29 SŁAWOMIR SOBOLEWSKI, KAMIL JURCZYK
Zagrożenia w Policji wynikające z uruchomienia niezidentyfikowanych plików malware

33 ANNA RYWCZYŃSKA
Co robimy źle, a moglibyśmy robić lepiej. W ochronie dzieci przed zagrożeniami w sieci

37 AGNIESZKA KORŻ
Działania profilaktyczne w obszarze cyberbezpieczeństwa dzieci i młodzieży

BEZPIECZEŃSTWO RUCHU DROGOWEGO

40 RAFAŁ BLOCH
Konfiskata pojazdu mechanicznego w świetle nowych przepisów

SŁUŻBA NA WODZIE

44 KINGA CZERWIŃSKA
Konferencja Ratownictwa Wodnego „On Duty 2024”Gdynia

49 KINGA CZERWIŃSKA
Wykorzystanie skutera wodnego w pracy policji wodnej

KYNOLOGIA POLICYJNA

55 PIOTR MROZOWSKI, DANIEL TATERA
Bezpieczeństwo osobiste przewodnika psa podczas tropienia śladów ludzkich

61 PIOTR MROZOWSKI
Nazewnictwo i ewidencja psów służbowych

TRADYCJA SPORTU W POLICJI

67 DOMINIK JĘDRYKA
Pierwsze Ogólnokrajowe Zawody Sportowe Policji Państwowej

ZWALCZANIE CYBERPRZESTĘPCZOŚCI

przez polską Policję

nadkom. Mariusz Tomczak

radca Wydziału Wywiadu Kryminalnego
Centralne Biuro Zwalczania Cyberprzestępczości

Cyberprzestępczość, w jej różnych formach, stanowi od wielu już lat rosnące zagrożenie dla bezpieczeństwa globalnego. By uświadomić sobie skalę tego fenomenu, wystarczy tylko przytoczyć dane statystyczne komórki Internet Crime Complaint Center Federalnego Biura Śledczego Stanów Zjednoczonych (FBI), które wskazują, że liczba zgłoszeń w tym obszarze osiągnęła wartość 800 944 w 2022 r., w porównaniu do 351 937 takich zdarzeń w 2018 r. Cechą charakterystyczną tego zjawiska, obok niespotykanej dynamiki wzrostu, jest szerokie spektrum zagrożeń (np. cyberataki, rozpowszechnianie on-line treści pornograficznych z udziałem dzieci, oszustwa online i wiele innych), a także bardzo często niezwykle złożona konstrukcja przestępstw.

Tworzenie struktur zwalczania cyberprzestępczości w Polsce i w Europie

W Polsce, w ujęciu historycznym, cyberprzestępczość długo nie była postrzegana jako oddzielny obszar zagrożeń, wymagający dedykowanego podejścia. Zagrożenia tego typu były klasyfikowane jako zdarzenia w obrębie przestępczości gospodarczej. W rezultacie były zwalczane przez komórki pionu przestępczości gospodarczej w Policji. Ponadto wszelkie incydenty związane z wykorzystaniem narzędzi cyfrowych były raczej traktowane jako pewien czynnik ułatwiający popełnianie przestępstw, a więc jako element szerszej perspektywy. Z czasem jednak świadomość organów ścigania dotycząca odrębności cyberprzestępczości i jej rosnącej skali zaczęła się zwiększać, prowokując tworzenie zalążków struktur zajmujących się tymi zagrożeniami. Pierwszym tego zwiastunem było wypracowanie, zaakceptowanej przez Komendanta Głównego Policji „Koncepcji technicznego wsparcia zwalczania cyberprzestępczości". Na podstawie tego dokumentu powołano w czerwcu 2007 r., w strukturze Biura Kryminalnego Komendy Głównej Policji, Sekcję Wsparcia Zwalczania Cyberprzestępczości. Do zadań tej komórki należało przede wszystkim monitorowanie cyberzagrożeń, wdrażanie zaawansowanych narzędzi, służących zwalczaniu cyberprzestępczości, a także wspieranie funkcjonariuszy w całym kraju, w przypadku skomplikowanych spraw związanych z wykorzystaniem technologii informatycznych. W następnych latach ranga tego zagadnienia nieustannie rosła, znajdując odzwierciedlenie w kolejnych zmianach organizacyjnych. Wymusiło to podjęcie strategicznej decyzji o utworzeniu zupełnie nowej struktury, która uzyskała scentralizowany i w dużym stopniu samodzielny wymiar w obszarze zwalczania cyberprzestępczości. W efekcie w dniu 12 stycznia 2022 r. zostało utworzone Centralne Biuro Zwalczania Cyberprzestępczości (CBZC).

Wspomniane procesy adaptacyjne do zagrożeń w cyberprzestrzeni zostały również podjęte, znacznie wcześniej, na poziomie europejskim. Wiodącą rolę w tym zakresie pełni Agencja Unii Europejskiej do spraw Współpracy Organów Ścigania (Europol). To właśnie w strukturze tej Agencji w styczniu 2013 r. utworzono Europejskie Centrum ds. Cyberprzestępczości (EC3, European Cy-

bercrime Center). Rolą Centrum jest wspieranie państw członkowskich UE oraz państw trzecich w zwalczaniu zaawansowanych form cyberprzestępczości o zasięgu globalnym. Podobna współpraca realizowana jest także na forum Międzynarodowej Organizacji Policji Kryminalnych (INTERPOL). W ramach tej organizacji również funkcjonuje Centrum ds. Cyberprzestępczości (**Cybercrime Directorate**). Polskie organy ścigania, w tym w szczególności CBZC, ściśle współpracują ze wspomnianymi organizacjami.

Katalog cyberprzestępstw

Jak zostało to zasygnalizowane we wstępie, cyberprzestępczość stanowi w istocie szeroki katalog zagrożeń, których wspólnym mianownikiem jest wykorzystanie technologii cyfrowych jako narzędzia popełnienia przestępstwa bądź też potraktowanie środowiska cyfrowego jako celu przestępstwa. Poniżej wymieniono najpoważniejsze obecnie zagrożenia w tym obszarze.

Ataki i oszustwa motywowane finansowo, bądź ukierunkowane na kradzież danych

- **Phishing** – metoda, w której cyberprzestępcy próbują uzyskać poufne informacje, takie jak nazwy użytkowników, hasła i dane kart kredytowych, imitując zaufane podmioty w komunikacji elektronicznej.
- **Ransomware** – złośliwe oprogramowanie, które szyfruje pliki ofiary; atakujący żąda następnie okupu od ofiary w zamian za przywrócenie dostępu do danych po dokonaniu płatności.
- **Hacking** – nieautoryzowany dostęp do systemów komputerowych lub sieci; hakerzy mogą wykorzystywać luki w systemie do kradzieży, modyfikacji lub niszczenia danych.
- **Kradzież tożsamości** – kradzież danych osobowych w celu popełnienia oszustwa, takiego jak dokonywanie nieautoryzowanych zakupów lub otwieranie nowych kont na nazwisko ofiary.
- **Oszustwa internetowe** – różnorodne schematy przestępcze realizowane w sieci Internet w celu oszukania osób, tak aby przekazały pieniądze, dane osobowe lub inne wartościowe aktywa. Tego rodzaju przestępstwami są oszustwa metodą „na pracownika banku", „na policjanta" i „na prokuratora", gdzie sprawcy, wykorzystując m.in. metody socjotechniczne, uzyskują od swoich ofiar dane dostępowe do kont bankowych bądź też prowokują je do transferów pieniężnych.
- **Oszustwa inwestycyjne** – oszustwa, które polegają na wyłudzaniu środków poprzez nakłonienie ofiary do udziału w inwestycjach kapitałowych.
- **Oszustwa metodą Business Email Compromise (BEC) CEO Fraud** – to metoda oszustwa, w której cyberprzestępcy przejmują kontrolę nad firmowymi kontami e-mail lub tworzą bardzo podobne adresy e-mail, aby oszukać pracowników firmy. Atakujący najczęściej podszywają się pod osoby o wysokim statusie w firmie, np. dyrektorów, menedżerów lub dostawców, aby nakłonić ofiary do wykonania nieautoryzowanych przelewów finansowych lub ujawnienia poufnych informacji.
- **Kradzież własności intelektualnej** – kradzież lub używanie cudzej własności intelektualnej (takiej jak oprogramowanie, muzyka, filmy i inne treści cyfrowe) bez zgody właściciela.

Ataki na infrastrukturę i cyberprzestrzeń

- **Cryptojacking** – nieautoryzowane użycie komputera innej osoby do wydobywania kryptowaluty. Zasoby systemu ofiary są wykorzystywane do generowania cyfrowych walut dla atakującego.
- **Ataki hybrydowe –** szczególnie groźne ataki wymierzone w bezpieczeństwo państwa i obejmujące infrastrukturę krytyczną, instytucje publiczne i gospodarcze, a także akty cyberszpiegostwa.
- **Ataki typu DoS (Denial of Service) i DDoS (Distributed Denial of Service)** – ataki przeciążające system, sieć lub stronę internetową poprzez generowanie dużego ruchu sieciowego, przez co czynią te systemy i usługi niedostępnymi dla użytkowników.

Działania szkodliwe dla osób i społeczności

- **Cyberstalking** – wykorzystywanie sieci Internet lub innych środków elektronicznych do nękania lub prześladowania osoby, grupy osób lub organizacji.
- **Wykorzystywanie dzieci** – wykorzystywanie sieci Internet do produkcji oraz dystrybucji treści pornograficznych z udziałem małoletnich.
- **Inżynieria społeczna (Social Engineering)** – manipulowanie ludźmi w środowisku cyfrowym poprzez wykorzystanie narzędzi socjotechnicznych w celu sprowokowania ich do określonych zachowań bądź przyjęcia fałszywych informacji lub ujawnienia informacji poufnych.

Charakterystyka współczesnej cyberprzestępczości

W rzeczywistości jednak cyberprzestępczość to bardzo skomplikowana struktura powiązań i zależności, która przyjmuje cechy dojrzałego rynku, oferującego potężny zakres usług przestępczych i generującego ogromne dochody finansowe. W praktyce cyberprzestępstwa stanowią wieloetapowe i niezwykle złożone przedsięwzięcia, które obejmują wiele kroków, np. od początkowego włamania do systemu po wykradanie danych, przy udziale różnych aktorów na różnych etapach tego procesu.

W rezultacie usługi cyberprzestępcze stanowią obecnie profesjonalny rynek, charakteryzujący się wysoką specjalizacją i strukturą współpracy. Dostępne są usługi, takie jak brokery dostępu początkowego (Initial Access Broker) i droppery (programy służące do dostarczenia złośliwego oprogramowania do urządzenia końcowego), które są kluczowe dla ataków ransomware i oszustw, i zapewniają monitorowanie i dostarczanie złośliwego oprogramowania. Ponadto dostępne są wyspecjalizowane metody ukrywania, takie jak cryptery i usługi przeciwko oprogramowaniu antywirusowemu (CAV), które pomagają ukryć złośliwe działania i unikać wykrycia przez programy antywirusowe. Przestępcy również używają sieci VPN (Virtual Private Networks) do maskowania swojej tożsamości i lokalizacji. Narzędzia te wymagają infrastruktury odpornej na zakłócenia i infiltrację ze strony organów ścigania. Niektórzy dostawcy usług internetowych (Internet Service Providers) i dostawcy hostingu, często używani przez przestępców, nie prowadzą szeroko zakrojonego monitoringu i nie przestrzegają prawnych

wniosków o informacje. Popularny jest w tym przypadku Bulletproof, czyli usługa hostingu internetowego, odporna na skargi dotyczące nielegalnych działań i służąca przestępcom jako podstawowy budulec do usprawnienia różnych cyberataków.
Obrona przed cyberprzestępczością jest tak silna, jak najsłabsze ogniwo, którym często jest czynnik ludzki. Wiadomości phishingowe, złośliwe pliki, techniki socjotechniczne i nieaktualizowane oprogramowanie stanowią najczęstsze punkty wejścia do systemu dla cyberprzestępców. Metody socjotechniczne, a w szczególności phishing, są szeroko stosowane do manipulowania ludźmi w celu ujawnienia poufnych informacji. Ponieważ regulacje UE utrudniły oszustwa z użyciem kart płatniczych, przestępcy coraz częściej skupiają się na użytkownikach. W rezultacie phishing pozostaje główną metodą oszustw online i ataków złośliwego oprogramowania.
Wykorzystanie fałszywych tożsamości jest również powszechne w kontekście seksualnego wykorzystywania małoletnich w sieci, gdzie przestępcy na szeroką skalę korzystają z mediów społecznościowych. Ponadto powszechne stały się oszustwa związane z działalnością charytatywną, wykorzystujące kryzysy, takie jak pandemia COVID-19, inwazja Rosji na Ukrainę czy klęski żywiołowe. Kolejne zagrożenie to spoofing, czyli technika stosowana do zdobycia zaufania ofiar poprzez fałszowanie identyfikatorów dzwoniących. Oszustwa online dotyczą również manipulowania systemami płatności. Złośliwe oprogramowanie może być instalowane w bankomatach, aby wypłacać pieniądze lub przejmować systemy płatności cyfrowych w celu kradzieży danych kart poprzez tzw. digital skimming.
Głównym towarem w kontekście cyberprzestępczości są skradzione dane. Dane te, uzyskane poprzez skompromitowane bazy danych i techniki socjotechniczne, są sprzedawane na nielegalnym rynku. Przestępcy seksualni wykorzystują natomiast informacje wrażliwe do szantażu. Ponadto skradzione dane wspierają liczne, pozostałe działania przestępcze, w tym np. szpiegostwo i wymuszenia.
Dobrym przykładem rozwoju rynku usług przestępczych jest jedno z największych forów hakerskich RaidForums, służące do handlu skradzionymi danymi, które zostało zamknięte w kwietniu 2022 r. Bez wątpienia, skradzione dane napędzają oszustwa przeciwko systemom płatności i kradzież tożsamości. Rozwój ekosystemu handlu danymi zwiększył zagrożenie przejęcia konta (ATO, Account Takeover Fraud), które polega na nielegalnym uzyskaniu przez przestępców dostępu do kont online w celu osiągnięcia korzyści finansowych lub dalszego handlu danymi. ATO stało się łatwiejsze dzięki dostępności dedykowanych narzędzi.
Ogromną rolę w ułatwianiu funkcjonowania rynku związanego z cyberprzestępczością odgrywa środowisko tzw. ciemnego Internetu (Darknet). Fora w tej sieci są intensywnie wykorzystywane przez cyberprzestępców do komunikacji, wymiany wiedzy i doświadczeń, handlu cyfrowymi aktywami, a także rekrutowania specjalistów. W szczególności grupy hakerskie korzystają z tychże forów do rekrutowania wszelkiego rodzaju specjalistów, których można zaangażować na poszczególnych etapach schematu przestępczego. Przestępcy seksualni używają natomiast forów do nawiązywania kontaktów, dzielenia się wiedzą i wymiany materiałów przedstawiających wykorzystywanie seksualne dzieci (CSAM – *Child Sexual Abuse Material*).
Na tych platformach sprzedawane są różne usługi przestępcze, w tym skradzione dane i usługi typu „crime-as-a-service". Fora dostarczają informacji na temat bezpieczeństwa operacyjnego (OpSec), metod oszustw, wykorzystywania dzieci, prania pieniędzy, phishingu i złośliwego oprogramowania. Informacje i wskazówki dotyczące operacji na rynkach dark web są powszechnie dostępne. Niemniej jednak działania organów ścigania i ataki DDoS spowodowały niestabilność na tych rynkach, co doprowadziło do zamknięcia kilku znanych platform w ostatnich latach.

Struktura i zadania CBZC

CBZC stanowi obecnie wiodącą jednostkę Policji w zakresie zapobiegania i zwalczania cyberprzestępczości. Biuro ma charakter scentralizowany. Oznacza to że na poziomie centralnym funkcjonuje kierownictwo oraz wydziały i zarządy centralne. Ponadto w każdym województwie funkcjonują zarządy i wydziały terenowe.
Podstawę działalności Biura określają przepisy prawne, takie jak ustawa z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz. U. poz. 2447, z późn. zm.) oraz Regulamin Centralnego Biura Zwalczania Cyberprzestępczości z dnia 14 maja 2024 r. CBZC wypełnia swoje zadania statutowe poprzez podejmowanie działań na rzecz zapewnienia bezpieczeństwa publicznego, będąc tym samym jednostką organizacyjną Policji służącą zwalczaniu cyberprzestępczości. CBZC odpowiedzialne jest za realizację na obszarze całego kraju zadań w zakresie:

- rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw;
- wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu tych przestępstw.

Biuro koncentruje się przede wszystkim na zwalczaniu najbardziej zaawansowanych i zorganizowanych form cyberprzestępczości, natomiast w ujęciu globalnym przestępstwa tego rodzaju, w szczególności o mniejszej skali i stopniu skomplikowania, są również zwalczane przez pozostałe jednostki Policji. Ponadto ważną rolą CBZC jest wyznaczanie właściwych standardów i dobrych praktyk w zakresie prowadzenia spraw w obszarze cyberprzestępczości, a także identyfikowanie i wypracowanie odpowiedniej strategii wobec zupełnie nowych zagrożeń, najczęściej związanych z pojawieniem się nowych, przełomowych technologii (np. ChatGPT – technologia przetwarzania języka naturalnego oparta na wykorzystaniu sztucznej inteligencji, mająca na celu naśladowanie ludzkiej konwersacji).
Przedmiotem działania CBZC jest w szczególności zwalczanie dwóch grup przestępstw. Pierwsza grupa to przestępstwa, które można popełnić tylko z wykorzystaniem technologii informatycznych, tj. hacking, ransomware,

ataki DDoS, malware, bulletproof hosting. Druga grupa obejmuje przestępstwa, które można popełnić także z wykorzystaniem technologii cyfrowych, np. oszustwa internetowe, prowadzenie sklepów internetowych z nielegalnym towarem, oszustwa phishingowe i oszustwa inwestycyjne. Obok wspomnianych powyżej grup ważnym obszarem jest również zwalczanie produkcji i dystrybucji treści pornograficznych z udziałem małoletnich.

W ujęciu merytorycznym metodyka działania CBZC w obszarze zapobiegania i zwalczania cyberprzestępczości opiera się na kilku podstawowych filarach. Zaliczamy do nich:

- prowadzenie spraw operacyjnych i postępowań przygotowawczych;
- monitorowanie i analiza cyberprzestępczości w ujęciu statystycznym oraz w zakresie identyfikowanych trendów, w tym analiza transakcji z wykorzystaniem kryptowalut;
- informatyka śledcza;
- realizacja programów zapobiegania przestępczości i kampanii profilaktycznych;
- reagowanie na nagłe incydenty w sieci, w szczególności związane z zagrożeniem życia i zdrowia ludzkiego;
- współpraca międzynarodowa organów ścigania.

Działalność CBZC w 2023 r. w liczbach

W celu zobrazowania skali działania CBZC warto zapoznać się z podstawowymi danymi statystycznymi, które wskazują, że tylko w 2023 r. Biuro prowadziło 617 postępowań przygotowawczych. Ponadto zatrzymano 501 osób oraz zabezpieczono mienie w wysokości ponad 441 000 000 PLN. W obszarze informatyki śledczej dokonano zabezpieczenia danych z 2500 telefonów komórkowych, sporządzono 808 analiz danych z telefonów komórkowych i 1331 analiz dysków, wykonano 1000 kopii binarnych oraz zabezpieczono 2000 TB materiału dowodowego. Ponadto udzielono wsparcia (w szczególności technicznego) w ramach 440 spraw prowadzonych przez pozostałe jednostki Policji. Przy czym wsparcie obejmowało także analizy w zakresie transakcji kryptowalutowych, jak również działalność szkoleniową w zakresie wybranych aspektów zwalczania cyberprzestępczości. W obszarze reagowania na nagłe incydenty zrealizowano 2380 spraw związanych z zagrożeniem życia i zdrowia ludzkiego, w ramach których ustalono 2303 osoby, z czego 1887 osób wymagało hospitalizacji bądź przekazano je pod opiekę najbliższych.

Współpraca międzynarodowa

Istotnym elementem, bez którego nie byłoby możliwe skuteczne zwalczanie cyberprzestępczości, jest międzynarodowa współpraca organów ścigania. Obecnie najbardziej kluczowe znaczenie ma współpraca ze wspomnianymi wcześniej instytucjami, tj, Europolem i Interpolem.

W ramach współpracy z Europolem realizowany jest szereg poważnych spraw operacyjnych o charakterze międzynarodowym, w które zaangażowane są także inne państwa członkowskie UE. W celu zoptymalizowania tej współpracy CBZC jest także członkiem specjalnej grupy zadaniowej państw członkowskich przy Europolu J-CAT, która skupia oficerów łącznikowych na co dzień zajmujących się koordynacją współpracy w ramach wspólnych spraw w obszarze cyberprzestępczości.

CBZC jest ponadto uczestnikiem operacji realizowanych pod egidą Interpolu. Organizacja ta oferuje wiele zaawansowanych narzędzi i form współpracy ułatwiających zwalczanie cyberprzestępczości. Współpraca z Interpolem jest szczególnie cenna z uwagi na zasięg geograficzny, obejmujący wszystkie kontynenty. Ponadto Interpol zapewnia ogromne wsparcie i wiedzę w zakresie wykorzystania najnowszych technologii do celów przestępczych. CBZC było m.in. uczestnikiem Grupy ds. Metaverse[1], która na przełomie lat 2023 i 2024 opracowała raport dotyczący przestępczości w światach wirtualnych metaverse i metodyki działania organów ścigania w metaverse.

Współpraca międzynarodowa to jednak nie tylko wspomniane powyżej organizacje i agencje, ale także wiele innych narzędzi i regulacji ułatwiających współpracę organów ścigania. Najlepszym tego przykładem jest Konwencja Budapesztańska, która stanowi potoczną nazwę Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23 listopada 2001 r., obowiązującej w Polsce od 1 czerwca 2015 r. (Dz. U. z 2015 r. poz. 728). Jej celem jest poprawa współpracy międzynarodowej związanej ze zwalczaniem cyberprzestępczości m.in. poprzez przyjęcie wspólnej terminologii, określenia czynów, które uznawane będą za przestępstwa (art. 2–11 konwencji), określenie zasad współpracy pomiędzy państwami ratyfikującymi konwencję i ujednolicenie ich systemów prawnych, np. w zakresie zabezpieczania przed utraceniem danych teleinformatycznych (tzw. mrożenie danych, art. 16 i 29 konwencji) oraz przekazywanie informacji z własnej inicjatywy (art. 26 konwencji).

Konwencja budapesztańska daje podstawy do zabezpieczania danych informatycznych w firmach działających na terenie innych państw, które ratyfikowały konwencję. Zgodnie z jej zapisami **mrożenie następuje na okres dziewięćdziesięciu dni (90 dni)**, od daty, kiedy „nakaz mrożenia danych" za pośrednictwem partnera zagranicznego otrzyma firma, od której chcemy uzyskać dane. W przepisach konwencji znajduje się zapis o możliwości przedłużenia przedmiotowego nakazu o kolejne dziewięćdziesiąt dni (90 dni). Wnioski o mrożenie danych przesyłamy tylko do spraw procesowych.

Bardzo ważnym aspektem w kontekście skutecznego zwalczania cyberprzestępczości jest współpraca w zakresie wymiany informacji z dostawcami usług internetowych (Internet Service Providers), a w szczególności z globalnymi graczami (np. Google, Meta, X itp.). Uzyskiwanie informacji na potrzeby prowadzonych postępowań i spraw operacyjnych może odbywać się w różnoraki sposób. Najszybciej uzyskiwane są informacje poprzez zapytania bezpośrednie (za pomocą interaktywnych formularzy dostawców usług) oraz z wykorzystaniem międzynarodowych policyjnych kanałów wymiany informacji (np. aplikacja wymiany informacji SIENA, udostępniana przez Europol). Przy czym tą drogą uzyskujemy tylko podstawowe informacje (tzw. Basic Subscriber Information, czyli np. dane rejestracyjne i „wykazy logowań"). Nie uzyskamy natomiast treści wiadomości (tzw. content). W takim przypadku konieczne jest wystąpienie z międzynarodową pomocą prawną.

Kierunki rozwoju CBZC

Z uwagi na fakt, że środowisko cyfrowe i technologie informatyczne podlegają gwałtownemu rozwojowi, ta sama prawidłowość ma również zastosowanie do cyberprzestępczości. Wymusza to ciągły rozwój i adaptację instytucji zwalczających to zjawisko. W rezultacie priorytetem CBZC na najbliższe lata jest ewoluowanie Biura w kierunku jednostki zaawansowanej technologicznie i organizacyjnie, która skutecznie zapobiega i zwalcza najbardziej zaawansowane formy cyberprzestępczości.
Najważniejsze priorytety obejmują:

- rozpoznawanie cyberprzestępczości przez budowanie przestrzeni cyberbezpieczeństwa oraz właściwej komunikacji wraz z zaangażowaniem społeczeństwa w zakresie przeciwdziałania cyberprzestępczości – działalność prewencyjna i komunikacyjna za pośrednictwem dostępnych kanałów, a także współpraca międzyinstytucjonalna,
- zoptymalizowanie pracy operacyjnej i procesowej w ramach CBZC – wypracowanie jednolitych, wystandaryzowanych w skali całego Biura wzorców realizacji spraw, w wymiarze operacyjnym i procesowym,
- zacieśnienie współpracy z krajowymi podmiotami publicznymi i prywatnymi oraz instytucjami międzynarodowymi,
- gromadzenie informacji w zakresie danych dotyczących cyberprzestępczości – pełnienie roli hubu informacyjnego w zakresie cyberprzestępczości w celu budowania pełnego obrazu zjawiska, w kontekście jego charakterystyk, a w efekcie traktowania tego jako fundamentu przyszłych, ukierunkowanych działań,
- wdrażanie i rozwijanie nowoczesnych technologii i innowacji – rozwijanie bądź pozyskiwanie najnowszych technologii wspierających zwalczanie cyberprzestępczości i przetwarzanie dużych zbiorów danych,
- stałe podnoszenie kompetencji funkcjonariuszy i pracowników CBZC w zakresie zwalczania cyberprzestępczości oraz w zakresie cyberprofilaktyki, **a także realizowanie podobnych szkoleń dla pozostałych funkcjonariuszy i pracowników w Policji.**

Przykłady operacji CBZC

Likwidacja i zajęcie infrastruktury przestępczej „EXCLU CHAT"

Policjanci CBZC w ramach międzynarodowej operacji z udziałem organów ścigania z Niemiec i Holandii, a także przy wsparciu Eurojustu i Europolu zlikwidowali infrastrukturę służącą do działalności przestępczej, poprzez wyłączenie szyfrowanego komunikatora Crypto-Messenger Exclu. Funkcjonariusze CBZC wraz z niemieckimi kolegami oraz przy pomocy pracowników Państwowego Instytutu Badawczego NASK dokonali 6 przeszukań na terenie RP. Równocześnie realizowane były przeszukania na terenie Niemiec, Holandii i Belgii. W realizacji na terenie Niemiec brał udział funkcjonariusz CBZC odpowiedzialny za koordynację działań. Policja holenderska przeprowadziła 79 przeszukań, zatrzymano 42 osoby, ujawniono dwa laboratoria narkotykowe oraz palarnię kokainy, zabezpieczono znaczne ilości narkotyków i ponad 4 mln euro w gotówce. Przejęta aplikacja używana była do wymiany informacji w zakresie handlu narkotykami i bronią palną w znacznych ilościach. Funkcjonariusze CBZC w wyniku przeprowadzonych czynności zabezpieczyli 6 serwerów o pojemności 30 TB, 32 sztuk pamięci masowej o pojemności 30 TB oraz inny sprzęt wykorzystywany do popełniania przestępstw. W wyniku operacji Policji serwis nie jest już dostępny[2].

Operacja „POWER OFF”

Policjanci CBZC we współpracy z Prokuraturą Okręgową w Bydgoszczy zatrzymali 2 osoby zajmujące się wytwarzaniem i udostępnianiem płatnej usługi do przeprowadzania ataków DDoS. Korzystanie z usługi możliwe było po dokonaniu opłaty w kryptowalucie. Przeprowadzane cyberataki w istotny sposób zakłócały pracę systemów informatycznych ulokowanych na terenie całego świata. Usługa ta funkcjonowała od 2013 r. i została skutecznie zablokowana w ramach międzynarodowej operacji „Power Off”.
Operacja prowadzona była przy ścisłej współpracy z Europolem, FBI, policją Holandii, Niemiec i Belgii oraz koordynowana przez Grupę Zadaniową ds. Cyberprzestępczości J-CAT. W postępowaniu uzyskano dane z serwera sprawców zlokalizowanego w Szwajcarii. Ustalono ponad 35 tys. kont użytkowników, 76 tys. zapisów logowań do platformy i ponad 320 tys. unikalnych adresów IP zaatakowanych serwerów. Ustalono również 11 tys. zapisów dotyczących wykupionych „planów ataku” wraz z adresem e-mail kupującego usługę (na łączną sumę około 400 tys. USD) oraz ponad tysiąc zapisów dotyczących wykupionych „planów ataków” (na łączną sumę około 44 tys. USD).
W ramach przeprowadzonej przez policjantów CBZC realizacji zatrzymano 2 osoby i przeprowadzono 10 przeszukań. Na komputerze jednego z podejrzanych ujawniono i zabezpieczono dowody prowadzenia i administrowania przestępczej domeny. Zabezpieczono sprzęt elektroniczny w postaci 15 twardych dysków, 5 komputerów stacjonarnych i 6 przenośnych, 10 telefonów, 5 pamięci USB, 3 karty SIM oraz wydruk portfela kryptowalutowego z kluczem prywatnym[3].

Podsumowanie

Reasumując, należy podkreślić, że zapobieganie i zwalczanie cyberprzestępczości jest zadaniem niezwykle złożonym, którego nie da się mierzyć miarą właściwą dla zwalczania tradycyjnej przestępczości. Mierzenie się z tym zagrożeniem wymaga bowiem nie tylko ogromnej wiedzy technicznej, ale wiedzy interdyscyplinarnej obejmującej, obok aspektów technologicznych, także zagadnienia społeczne, ekonomiczne, a nawet geopolityczne. Cyberprzestępczość stanowi bowiem pewien horyzontalny system, który przenika wszystkie obszary ludzkiej aktywności. Tak wymagające wyzwanie wymaga podejścia opartego na ciągłym doskonaleniu, uczeniu się i inwestowaniu w odpowiednie narzędzia i metodyki.

[1] Metaverse – wirtualne środowisko on-line, które łączy w sobie rzeczywistość rozszerzoną (świat rzeczywisty łączony z generowanym komputerowo, np. grafika 3D nakładana na obraz z kamery), rzeczywistość wirtualną, rzeczywistość mediów społecznościowych, gier on-line, a także kryptowalut [przyp. red.].
[2] Centralne Biuro Zwalczania Cyberprzestępczości, Aktualności, https://cbzc.policja.gov.pl/bzc/aktualnosci/ [dostęp: 2.07.2024 r.].
[3] Tamże.

Summary

Combating cybercrime by the Polish Police

This article defines the concept of cybercrime, and presents a catalog of the most serious threats in this area. It characterizes contemporary cybercrime and emphasizes that it is a complex phenomenon and already has the character of a “mature market”, which requires law enforcement agencies to have an interdisciplinary approach and makes it difficult to combat. Furthermore, the genesis of the creation of a specialized Polish unit — the Central Cybercrime Bureau — is explained, as well as its tasks, structure, and international cooperation, in particular within the framework of Europol and INTERPOL. An interesting and important addition to the article is data on the evidence secured by the CCB, as well as descriptions of exemplary operations carried out by the Bureau in cooperation with the police of other countries.

Tłumaczenie: Katarzyna Olbryś

CYBERSTALKING

jako narzędzie przemocowe

podinsp. Zbigniew Bogusz

Zakład Prawa i Kryminalistyki
Szkoła Policji w Pile

Rozwój informacyjno-komunikacyjny, a także pośpiech w realizacji planów prywatnych oraz zawodowych doprowadziły do tego, że życie codzienne dzieci, młodzieży, a nawet dorosłych stało się mało atrakcyjne, a w ekstremalnych przypadkach – dało nawet poczucie odtrącenia. Znaczna część społeczeństwa zaczęła więc poszukiwać w Internecie pracy, spokoju, poczucia bezpieczeństwa, relaksu, nowych znajomości, przyjaźni, a nawet miłości. Można więc postawić sobie pytanie: Dlaczego tak się dzieje? Odpowiedź wydaje się stosunkowo prosta. Internet to „ktoś" lub „coś", co zawsze na nas czeka, daje nadzieję i władzę, rozładowuje wszelkie emocje.

WPROWADZENIE

Należy podkreślić, że Internet może stanowić źródło wielu dobrych, wartościowych oraz rozwijających wiadomości. Trzeba jednak pamiętać, że może on również dostarczać informacji sprzyjających niewłaściwemu rozładowywaniu negatywnych emocji, co bez wątpienia może stanowić podłoże dopuszczania się szeregu przestępstw i zachowań niepożądanych różnego rodzaju. Jednym z nich jest właśnie cyberstalking.

Zjawisko cyberstalkingu określane jest również jako cyberprzemoc, której w wielu przypadkach dopuszcza się względnie anonimowa osoba, zwana cyberstalkerem. „Cyberstalking jest to więc wykorzystywanie technik informacyjnych i komunikacyjnych do świadomego, wielokrotnego i wrogiego zachowania się osoby lub grupy osób, mającego na celu krzywdzenie innych"[1]. Cyberstalker wykorzystuje technologię informacyjną, w szczególności Internet, jako narzędzie, dzięki któremu może dręczyć osobę lub grupę osób.

Działania cyberstalkera najczęściej polegają na: śledzeniu, obserwowaniu, nagrywaniu wizerunku osoby, przesyłaniu niechcianych wiadomości, publikowaniu negatywnych komentarzy czy też zdjęć, szykanowaniu danej osoby, grupy lub organizacji, prześladowaniu, prowokowaniu pokrzywdzonego do nieracjonalnego zachowania i/lub reakcji, zachęcaniu innych użytkowników do znieważania i/lub pomawiania.

Można więc stwierdzić, że mianem cyberstalkingu możemy określić wszystkie te zachowania cyberstalkera, które w jakiś sposób wypływają na to, że osoba pokrzywdzona poczuje, że jej bezpieczeństwo lub bezpieczeństwo jej osoby bliskiej jest zagrożone, że jest poniżona, udręczona lub zachowania te w sposób istotny naruszają jej prywatność.

Należy zauważyć, że określenie cyberstalking ma swój początek od słowa „stalking", pochodzącego z języka angielskiego – „to stalk" (prześladować, śledzić, podchodzić)[2]. Zamiennie stosowane jest również określenie – „cybernękanie" czy też „przemoc emocjonalna". Psychologowie, prawnicy i kryminolodzy, badając zjawisko stalkingu, posługują się wieloma definicjami. Jak się wydaje, najbardziej trafną z nich przedstawiła Dagmara Woźniakowska-Fejst, która po analizie licznych badań naukowych, słusznie stwierdziła, że możliwe jest zdefiniowanie *stalkingu* jako uporczywe, powtarzalne zachowanie (lub różnego rodzaju zachowania), skierowane przeciwko konkretnej jednostce, które w nieuzasadniony sposób rażąco narusza granice prywatności tej osoby lub w inny sposób zagraża jej dobrom osobistym. Skutkiem działania prześladowcy jest najczęściej wywołanie u nękanej osoby, osób jej najbliższych lub odpowiedzialnych za jej bezpieczeństwo uzasadnionego niepokoju i lęku[3].

Do najczęstszych zachowań występujących w ramach zjawiska „tradycyjnego" stalkingu zalicza się: uporczywe kontakty osobiste lub za pośrednictwem środków teleinformatycznych lub osób trzecich, obecność w pobliżu domu czy miejsca pracy, a także wysyłanie korespondencji w każdej dostępnej formie – od tradycyjnej po elektroniczną, śledzenie pokrzywdzonego, w tym z zastosowaniem kamer, rozsyłanie fałszywych informacji lub plotek, nękanie osób najbliższych, jak również napaści na pokrzywdzonego lub osoby mu bliskie.

W Polsce słowo stalking pojawiło się w latach 90. XX w., kiedy zaobserwowano w życiu społecznym przejawy tego zjawiska. Zanim jednak wprowadzono art. 190a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny[4] (dalej: „k.k."), Ministerstwo Sprawiedliwości zainicjowało badania analityczne mające na celu rozpoznanie skali zjawiska stalkingu w Polsce. Badanie zostało przeprowadzone na reprezentatywnej, losowo wybranej grupie 10 200 respondentów, z których niemal co dziesiąty (9,9%) odpowiedział twierdząco na pytanie, czy był ofiarą uporczywego nękania.

Sposób szykanowania ofiar podejmowany przez sprawców był zróżnicowany. Najczęściej polegał na: rozpowszechnianiu oszczerstw, nawiązywaniu kontaktu za pomocą osób trzecich, groźbach lub szantażu, głuchych, obscenicznych telefonach, groźbach pod adresem najbliższych, niechcianych listach, e-mailach lub SMS-ach, niechcianym robieniu zdjęć, niszczeniu rzeczy, niechcianym dotyku, upublicznianiu wizerunku ofiary i innych.

Ponad połowa pokrzywdzonych miała w związku z takim zdarzeniem problemy natury emocjonalnej lub inne – natury psychicznej. Co szósta ofiara zadeklarowała, że w wyniku uporczywego nękania utraciła lub zmieniła pracę, zaś co dziewiąta była zmuszona do zmiany miejsca zamieszkania. Połowa pokrzywdzonych stwierdziła, że konsekwencją było unikanie pewnych miejsc, ludzi lub sytuacji, a ponad 40% wskazało na pogorszenie się funkcjonowania w życiu zawodowym lub rodzinnym. Za penalizacją uporczywego nękania opowiedziało się w efekcie aż 87% badanych, przeciw – zaledwie 5%, a 8% nie miało w tej sprawie opinii[5]. Wystąpienie zjawiska stalkingu w Polsce stało się więc faktem, a jego rozmiar i zakres działania sprawców okazał się dalece niepokojący. Wobec tego ustawodawca, po wcześniejszej analizie wydarzeń w obszarze życia społecznego, gospodarczego, politycznego, a także w wyniku zwiększonej brutalizacji nowych form przestępczości, które ulegały wielu przemianom, postanowił dodać art. 190a do Kodeksu karnego, czyniąc to w drodze art. 1 pkt 2 ustawy z dnia 25 lutego 2011 r. o zmianie ustawy – Kodeks karny, która weszła w życie z dniem 6 czerwca 2011 r. Następnie zaś dokonał nowelizacji przedmiotowego przepisu na mocy art. 13 pkt 2 ustawy z dnia 31 marca 2020 r. o zmianie ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw.

Art. 190a k.k.

§ 1. Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

§ 2. Tej samej karze podlega, kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej.

§ 3. Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od lat 2 do 15.

§ 4. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Trafnie zauważa M. Mozgawa, że przed wejściem w życie przepisu art. 190a k.k., na gruncie polskiego prawa karnego, w zależności od charakteru danego zdarzenia, do walki z nękaniem można było stosować niektóre z przepisów Kodeksu karnego bądź ustawy z dnia 20 maja 1971 r. – Kodeks wykroczeń[6] (dalej: „k.w."), np.: złośliwe niepokojenie (art. 107 k.w.), znęcanie się (art. 207 k.k.), groźba karalna (art. 190 k.k.), zmuszanie (art. 109 k.k.), naruszenie miru domowego (art. 193 k.k.), zniesławienie (art. 212 k.k.), znieważenie (art. 216 k.k.), naruszenie tajemnicy korespondencji (art. 267 k.k.).

Zasadniczy problem, jaki pojawił się w walce z nękaniem, był taki, że zachowania sprawcy (niekiedy niezwykle dolegliwe dla ofiary) często w ogóle nie były przestępstwami ani wykroczeniami (wystawanie pod domem czy miejscem pracy, pisanie listów, SMS-ów itp.)[7]. Dlatego też zasadna była decyzja o kryminalizacji uporczywego nękania w Kodeksie karnym, w którym spenalizowano zachowania godzące w wolność człowieka, chronioną ustawą z dnia 2 kwietnia 1997 r. – Konstytucja Rzeczypospolitej Polskiej[8] (np.: art. 30, 31 ust. 1 i 2, art. 40, art. 41 ust. 1 i art. 47, art. 50).

Art. 47 Konstytucji RP

Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Art. 50 Konstytucji RP

Zapewnia się nienaruszalność mieszkania. Przeszukanie mieszkania, pomieszczenia lub pojazdu może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony.

Oczywiście można się zastanowić, czy stalking i cyberstalking to dwa jakościowo różne rodzaje działań, czy też w obu przypadkach jest to po prostu uporczywe nękanie, wykonywane jednak za pomocą różnych środków[9]. Słusznie zauważa D. Woźniakowska-Fajst, że trudno potraktować stalking i cyberstalking rozdzielnie, tym bardziej, że polski ustawodawca definiuje uporczywe nękanie w taki sposób, że dla uznania danego zachowania za prześladowanie nie ma znaczenia, z jakich środków korzysta stalker. Nie ulega więc wątpliwości, że zasadne jest omówienie zjawiska cyberstalkingu na gruncie art. 190a k.k.

USTAWOWE ZNAMIONA PRZESTĘPSTW Z ART. 190A K.K.

Przedmiot ochrony przestępstw z art. 190a k.k.

Przestępstwo stalkingu (cyberstalkingu) godzi w szereg dóbr prawnych, co powoduje złożoność przedmiotu ochrony.

Art. 190a k.k. opisuje dwa podstawowe typy czynów zabronionych, tj.:

a) uporczywe nękanie (art. 190a § 1 k.k.)
Kto przez uporczywe nękanie innej osoby lub osoby dla niej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
b) przywłaszczenie tożsamości (art. 190a § 2 k.k.)
Tej samej karze podlega, kto podszywając się pod inną osobę, wykorzystuje jej wizerunek, inne jej dane osobowe lub inne dane, za pomocą których jest ona publicznie identyfikowana, przez co wyrządza jej szkodę majątkową lub osobistą.

Przedmiotem ochrony na gruncie art. 190a § 1 k.k. jest przede wszystkim wolność człowieka, a także prawo do życia w poczuciu szeroko rozumianego bezpieczeństwa, wolnego od przejawów nękania, dręczenia, poniżania, a nawet poczucia zagrożenia, nie tylko w realnym życiu, ale również w Internecie. Ochronie podlega zatem wolność psychiczna człowieka, ale także jego prawo do ochrony życia prywatnego i rodzinnego, gdyż sprawca może być karany również za istotne naruszenie prywatności ofiary[10].

W przypadku art. 190a § 2 k.k. należy wskazać, że posiada on wspólną część przedmiotu ochrony z art. 190a § 1 k.k., tj. wolność od bezprawnej ingerencji w sferę życia prywatnego. Ponadto, w przypadku art. 190a § 2 k.k. przedmiotem ochrony jest także wolność w zakresie swobodnego dysponowania swoim wizerunkiem i innymi danymi osobowymi, a więc wolność w zakresie samodecydowania o wykorzystaniu informacji o swoim życiu osobistym[11]. Co za tym idzie, to właściciel ww. dóbr prawnie chronionych podejmuje decyzję, gdzie, kiedy i w jaki sposób je udostępni zarówno w sieci, jak i bezpośrednio.

Art. 190a § 3 k.k. dodatkowo wprowadza typ kwalifikowany, tj. sytuację, w której w wyniku czynu zabronionego następuje targnięcie się pokrzywdzonego na własne życie – *Jeżeli następstwem czynu określonego w § 1 lub 2 jest targnięcie się pokrzywdzonego na własne życie, sprawca podlega karze pozbawienia wolności od lat 2 do 15.* Tym przepisem ochroną zostało więc dodatkowo objęte najistotniejsze dobro prawne, jakim jest życie człowieka.

Strona przedmiotowa przestępstwa z art. 190a § 1 k.k.

W przypadku czynu zabronionego opisanego w art. 190a § 1 k.k. zachowanie sprawcy cechuje uporczywe nękanie danej osoby lub jej osoby najbliższej, co w konsekwencji wzbudza w niej uzasadnione poczucie zagrożenia, poniżenia, udręczenia lub powoduje istotne naruszenie jej prywatności. Stalker, którym może być każda osoba fizyczna, zarówno dobrze znana pokrzywdzonemu (np. były partner, partnerka), jak i obca (np. niepokojenie telefonami w nocy przez nieznaną osobę, wysyłanie wiadomości) lub grupa osób (np. mieszkańcy osiedla, osoby z miejsca pracy), może podejmować różne formy działania, m.in.: głuche telefony, rozmowy telefoniczne, niechciane SMS-y, publikowanie nieprawdziwych informacji, kontakty e-mailowe, obserwowanie, śledzenie, składanie niechcianych (niemoralnych) propozycji, zamawianie i obdarowywanie niechcianymi prezentami, często nieprzyzwoitymi, nagrywanie. Przy czym zachowanie sprawcy musi być nacechowane wielokrotnością działania, nie może to być czynność wykonana tylko raz. Według T. Bojarskiego „uporczywe nękanie" to zachowanie, które polega na ustawicznym dręczeniu, dokuczaniu komuś, tropieniu, a także niepokojeniu innej osoby, niedanie jej spokoju. Ponadto zachowanie takie jest nacechowane wyraźną intencją, powtarzające się, nieustanne oraz długotrwałe. Musi być ono wysoce nieprzyjemne, a także wzbudzające obawę bądź też naruszające w istotnym stopniu prywatność osoby.

O uporczywości można mówić wówczas, gdy dochodzi do sytuacji powtarzającego się nękania, zabarwionego ujemnie z uwagi na złą wolę sprawcy. Uporczywość jest więc połączeniem dwóch elementów. Jeden z nich charakteryzuje postępowanie sprawcy od strony podmiotowej. Polega zaś na szczególnym nastawieniu psychicznym ujawniającym się chęcią postawienia na swoim, nieustępliwością, obojętnie z jakich pobudek. Natomiast drugi element polega na trwaniu takiego stanu przez pewien dłuższy, bliżej nieokreślony czas[12] (wyrok Sądu Rejonowego w Tarnowskich Górach z 4 kwietnia 2023 r. – sygn. akt II K 894/22).

Elementy obiektywno-subiektywne dotyczące uporczywego nękania zostały trafnie przedstawione m.in. w wyroku Sądu Najwyższego z 29 marca 2017 r. (sygn. akt IV KK 413/16): „Wprawdzie w przepisie mowa jest o poczuciu zagrożenia, które oznacza wewnętrzny odbiór, odczucie lęku i osaczenia osoby doświadczanej nękaniem, jednak przepis odwołuje się także do kryterium obiektywnego, wskazując na to, że poczucie zagrożenia musi być uzasadnione okolicznościami. Oznacza to, że subiektywne odczuwanie zagrożenia przez daną osobę należy konfrontować z wiedzą, doświadczeniem i psychologią reakcji ogółu społeczeństwa, obiektywizować poprzez poczucie zagrożenia w danych okolicznościach, jakie towarzyszyłoby przeciętnemu człowiekowi, o ile oczywiście działania sprawcy nie zmaterializowały się w konkretnym skutku. Wówczas jednak w grę wchodzić może inny czyn karalny. Kwestie te są więc czysto ocenne, na co wskazuje orzecznictwo sądowe i doktryna prawa".

Ponadto Sąd Najwyższy zauważył, że warunkiem uznania zachowania sprawcy za stalking, nękanie przez sprawcę musi być uporczywe, a zatem polegać na nieustannym oraz istotnym naruszeniu prywatności innej osoby oraz wzbudzeniu w pokrzywdzonym uzasadnionego okolicznościami poczucia zagrożenia. Ustawodawca nie wymaga, aby zachowanie stalkera posiadało cechy agresji, gdyż zachowanie sprawcy może być kierowane takimi pobudkami, jak: miłość, nienawiść, chęć dokuczenia, złośliwość czy też chęć zemsty. Sąd orzekł ponadto, iż dla bytu tego przestępstwa nie ma znaczenia, czy sprawca ma zamiar wykonać swoje groźby, a decydujące jest tu subiektywne odczucie zagrożenia, które musi być oceniane w sposób zobiektywizowany[13].

Odnosząc się natomiast do „istotnego naruszenia prywatności", Sąd Najwyższy w wyroku z 12 stycznia 2016 r. (sygn. akt IV KK 196/15) orzekł, że o istotności naruszenia prawa do prywatności nie decyduje sama treść materiałów powstała w wyniku nieuprawnionego wkroczenia w sferę prywatności pokrzywdzonego, ale przede wszystkim to, w jaki sposób do naruszenia doszło i ewentualnie jak często dochodziło do tych naruszeń[14]. Zagadnienie to wyraża się również w sferze wolności człowieka od ingerencji w życie prywatne, rodzin-

ne i domowe, niezależnie czy dotyczy to okoliczności obojętnych czy kłopotliwych dla pokrzywdzonego. W tej sytuacji działanie sprawcy może polegać np. na daleko idącym wkroczeniu w życie prywatne pokrzywdzonego poprzez fotografowanie lub nagrywanie, a następnie publikowaniu takich materiałów w Internecie bez zgody pokrzywdzonego. Sąd Najwyższy, dostrzegając trudności w zdefiniowaniu pojęcia „prawo do prywatności", postanowił więc odwołać się do powołanej w piśmiennictwie rezolucji Zgromadzenia Parlamentarnego Rady Europy nr 42 z 1970 r., gdzie uznano, że: „prawo do prywatności wyraża się przede wszystkim w prawie do prowadzenia własnego życia z minimum ingerencji. Obejmuje prywatne, rodzinne i domowe życie, fizyczną i psychiczną integralność, honor i reputację, prawo do tego, aby nie być przedstawianym w fałszywym świetle, do nieujawniania zarówno faktów obojętnych (podkr. – SN), jak i kłopotliwych, do zakazu publikacji bez zgody własnej wypowiedzi i wizerunku, ochronę przed ujawnianiem informacji przekazanych lub otrzymanych w warunkach poufności" (cyt. za: N. Kłączyńska, w: *Komentarz do art. 190a Kodeksu karnego*, w: *Kodeks karny. Część szczególna. Komentarz*, red. J. Giezek, Lex 2014, teza 9)[15].

Odnosząc się natomiast do kwestii „poczucia poniżenia lub udręczenia", należy wskazać, że poniżenie oznacza zachowanie polegające na obrażaniu godności innej osoby, umniejszeniu jej wartości, przedstawieniu w złym świetle wobec innych, upokorzeniu jej lub w inny sposób okazaniu jej lekceważenia albo braku szacunku. Udręczenie natomiast obejmuje zachowanie polegające na dokuczaniu, przysparzaniu cierpień, w szczególności psychicznych. Wytworzone poczucia poniżenia lub udręczenia również muszą być uzasadnione, a zatem poparte obiektywnym przekonaniem, że każdy przeciętny człowiek o porównywalnych do ofiary cechach osobowości, psychiki, intelektu i umysłowości, w porównywalnych warunkach, także odczuwałby takie poniżenie lub udręczenie[16].

Skutkiem działania sprawcy jest bowiem nie tylko wzbudzenie u pokrzywdzonego zagrożenia, ale także innych stanów, jak poniżenie lub udręczenie, przy czym z redakcji przepisu wynika, że wystarczające jest zaistnienie któregokolwiek z nich.

Strona przedmiotowa przestępstwa z art. 190a § 2 k.k.

Art. 190a § 2 k.k. odnosi się do zachowania sprawcy polegającego na podszywaniu się pod inną osobę, wykorzystywaniu jej wizerunku lub innych danych osobowych, bądź też jeszcze innych danych, za pomocą których osoba ta jest publicznie identyfikowana. Również i w tym przypadku sprawcą może być każda osoba fizyczna, oczywiście znana lub nie. Może być nim np. osoba, której wcześniej zaufaliśmy (np. przyjaciel) i która weszła w posiadanie informacji, zdjęć, a nawet oryginalnych dokumentów w sposób legalny. Sprawcą może natomiast być również osoba, która podszywa się pod pokrzywdzonego. Co jednak istotne, sprawca musi podszywać się pod osobę autentycznie istniejącą (nie fikcyjną) i nie pod osobę zmarłą.

Zachowaniem określonym w art. 190a § 2 k.k. będzie np. przedstawienie się w rozmowie telefonicznej nazwiskiem innej osoby lub wysłanie do gazety albo umieszczenie na stronie internetowej oferty z podpisem drugiej osoby. Zachowanie takie musi być podjęte bez wiedzy i zgody osoby, za którą sprawca się podaje. Ten typ wymaga, aby osoba podszywająca się pod drugą osobę wykorzystała jej wizerunek lub jej inne dane osobowe. Czynność sprawcza polega więc na wprowadzeniu w błąd odbiorcy informacji przez stworzenie wrażenia za pomocą wizerunku lub innych danych osobowych, że informacja ta pochodzi od osoby, do której odnosi się wizerunek lub odnoszą się inne dane osobowe, gdy w rzeczywistości informacja ta pochodzi od sprawcy. Przekazana informacja nie ma być dla osoby, której wizerunkiem lub innymi danymi osobowymi sprawca się posłużył, obojętna, lecz jej przekazanie ma wyrządzić tej osobie szkodę majątkową lub osobistą[17].

Podszywanie się pod inną osobę może być wyrażone słowem, dźwiękiem lub obrazem (np. ogłoszenie o świadczeniu przez daną osobę usług seksualnych), w tym także wraz z wykorzystaniem tradycyjnych środków masowego przekazu, jak i szeroko rozumianej cyberprzestrzeni. Ponadto informacje przekazywane w ten sposób mogą być zrozumiałe dla nieograniczonej grupy odbiorców, jak i stanowić materiał, którego sens odczytają tylko konkretne osoby. Co ważne, zachowanie sprawcy nie musi być wielokrotne.

Strona przedmiotowa przestępstwa z art. 190a § 3 k.k.

Czynność sprawcza typu określonego w art. 190a § 3 k.k. będzie odpowiadała czynności realizującej znamiona typu z § 1 albo 2. W związku z tym kwalifikacja prawna powinna być złożona (art. 190a § 3 k.k. w zw. z § 1 albo art. 190a § 3 k.k. w zw. z § 2). Oczywiście nie zachodzi w takim wypadku kumulatywny zbieg przepisów i nie należy powoływać art. 11 § 2 k.k.[18]

Podmiot przestępstwa

(Cyber)stalker nie musi charakteryzować się żadnymi szczególnymi kwalifikacjami. Dlatego też przestępstwa określone w art. 190a § 1–3 k.k. mają charakter powszechny, co oznacza, że może popełnić je każda osoba, która jest zdolna do ponoszenia odpowiedzialności karnej.

Strona podmiotowa przestępstw z art. 190a § 1–3 k.k.

Znamię uporczywości wskazuje na nastawienie sprawcy w kierunku kontynuowania nękania innej osoby lub osoby jej najbliższej pomimo świadomości braku zgody osoby pokrzywdzonej na tego typu zachowanie. Sprawca musi mieć świadomość możliwości wzbudzania u drugiej osoby poczucia zagrożenia lub istotnego naruszenia prywatności. Nie są istotne motywy działania sprawcy. W grę wchodzi działanie w celu dokuczenia innej osobie, ale motywem zachowania może być także miłość do drugiej osoby i chęć jej adorowania. Te cechy znamienia strony podmiotowej przemawiają za uznaniem, że może być brany pod uwagę tylko zamiar bezpośredni. Strona podmiotowa czynu zabronionego opisanego w art. 190a § 2 k.k. charakteryzuje się umyślnością w sensie zamiaru bezpośredniego. Czynność sprawcza musi być podjęta w celu wyrządzenia osobie pokrzywdzonej szkody majątkowej lub szkody osobistej. Jest to więc działanie, którego celem ma być nie tylko osiągnięcie korzyści majątkowej, lecz także naruszenie dóbr tej oso-

by, pod której tożsamość sprawca się podszywa. Typ czynu zabronionego określony w art. 190a § 3 k.k. jest przykładem typu kwalifikowanego przez wystąpienie opisanego w ustawie następstwa. Stronę podmiotową tego typu określa więc art. 9 § 3 k.k. Sprawca realizuje znamiona typu z § 1 albo 2 umyślnie. Skutek natomiast w postaci targnięcia się osoby pokrzywdzonej na własne życie nie jest objęty zamiarem sprawcy, lecz jest obiektywnie przewidywalny[19].

TRYB ŚCIGANIA PRZESTĘPSTW Z ART. 190A K.K.

Należy nadmienić, że ściganie przestępstw, o których mowa w art. 190a § 1 i 2 k.k., następuje na wniosek pokrzywdzonego. W przypadku typu kwalifikowanego, opisanego w art. 190a § 3 k.k., ściganie podejmowane jest z urzędu.

ZBIEG PRZEPISÓW

M. Mozgawa zasadnie podnosi, że przestępstwo z art. 190a § 1 k.k. może pozostawać w rzeczywistym właściwym zbiegu z czynami zabronionymi ujętymi w następujących przepisach: art. 189 k.k. (pozbawienie wolności), art. 156, 157 k.k. (spowodowanie uszczerbku na zdrowiu), art. 211 k.k. (uprowadzenie małoletniego), art. 218 k.k. (złośliwe lub uporczywe naruszanie praw pracownika); a także z przepisami typizującymi przestępstwa przeciwko mieniu – np. z art. 278 k.k. (kradzież), art. 279 k.k. (kradzież z włamaniem), art. 288 k.k. (niszczenie lub uszkodzenie cudzej rzeczy) itd.

Rzeczywisty niewłaściwy zbieg zachodzi natomiast pomiędzy przepisami art. 190a § 1 k.k. oraz art. 191 § 1 k.k. (zmuszanie), art. 193 k.k. (naruszenie miru domowego), art. 212 k.k. (zniesławienie), art. 216 k.k. (zniewaga), art. 217 § 1 k.k. (naruszenie nietykalności cielesnej), które to przypadki rozwiązywane są przy zastosowaniu zasady *lex consumens derogat legi consumptae* (gdzie przepisem pochłaniającym jest art. 190a k.k.)[20].

Problematyczna może być natomiast wzajemna relacja zachodząca pomiędzy przepisami art. 190a § 1 k.k. i art. 207 k.k. (znęcanie się), gdzie w zależności od konkretnego stanu faktycznego możliwy jest zarówno zbieg pomijalny (przy zastosowaniu zasady konsumpcji, gdzie przepisem pochłaniającym będzie art. 207 k.k.), jak i kumulatywna kwalifikacja.

Natomiast art. 190a § 2 k.k. może pozostawać w rzeczywistym niewłaściwym zbiegu z przepisami typizującymi przestępstwa przeciwko ochronie informacji (art. 265–268a, 269a k.k.), przeciwko wiarygodności dokumentów (art. 270, 272, 273 i 275 k.k.). Należy również zauważyć, że w praktyce może pojawić się kumulatywna kwalifikacja przepisu art. 190a § 2 k.k. z przepisami z zakresu ochrony danych osobowych i prawa autorskiego.

W przypadku art. 190a § 2 k.k. zachowanie sprawcy może wyczerpywać równocześnie znamiona innych przestępstw. Możliwy jest w szczególności zbieg realny z przestępstwami przeciwko dokumentom (np. art. 270 § 1 k.k. czy art. 275 § 1 k.k.). Może również zajść zbieg z art. 65 § 1 k.k. W przypadku przestępstwa zniesławienia uznać należy, że dojdzie do pomijalnego zbiegu przepisów i czyn należy kwalifikować, bazując na art. 190a § 2 k.k. jako *lex specialis*. Nie zachodzi natomiast zbieg z art. 286 § 1 k.k. (oszustwo) ze względu na inny cel działania (osiągnięcie korzyści majątkowej). Z tego samego względu nie zachodzi również zbieg z art. 297 § 1 k.k. (wyłudzenie kredytu)[21].

[1] M. Konieczny, *Cyberprzestępczość – krótka historia, współczesne oblicza i trudna do przewidzenia przyszłość*, Roczniki Administracji i Prawa 2023, XXIII, z. 1, s. 29–50.
[2] *Wielki słownik polsko-angielski*, Wydawnictwo Naukowe PWN, Oxford University Press, Warszawa 2002, s. 1138.
[3] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej, Studium kryminologiczne*, Wydawnictwo Uniwersytetu Warszawskiego, Warszawa 2019, s. 39–40.
[4] Ustawa z dnia 20 maja 1971 r. – Kodeks karny (Dz. U. z 2023 r. poz. 2119).
[5] B. Guszczyńska, M. Marczewski, P. Ostaszewski, A. Siemaszko, D. Woźniakowska-Fajst, *Stalking w Polsce. Rozmiary – formy – skutki. Raport z badania nt. uporczywego nękania*, pod red. Andrzeja Siemaszki, w: A. Siemaszko (red.), *Księga jubileuszowa z okazji XX-lecia Instytutu Wymiaru Sprawiedliwości*, Warszawa 2011, s. 832–867; zob. również sejm VI kadencji, druk sejmowy Nr 3553.
[6] Ustawa z dnia 6 czerwca 1997 r. – Kodeks wykroczeń (Dz. U. z 2024 r. poz. 17).
[7] M. Mozgawa, *Kodeks karny. Część szczególna. Art. 148–251. Komentarz*, 2020, wyd. 1 (art. 190a – uporczywe nękanie).
[8] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483, z późn. zm.).
[9] D. Woźniakowska-Fajst, *Stalking i inne formy przemocy emocjonalnej, Studium kryminologiczne*, s. 52.
[10] A. Grześkowiak, K. Wiak, S. Hyps, *Kodeks karny. Komentarz*, 2024, wyd. 8, Legalis (art. 190a – uporczywe nękanie).
[11] R. Stefański, *Kodeks karny. Komentarz,* 2020, wyd. 25 (art. 190a – uporczywe nękanie).
[12] A. Łyżwa, w: *Kodeks karny. Część szczególna. Art. 148–251. Komentarz,* red. M. Banaś-Grabek, wyd. 1, Warszawa 2020, art. 190a.
[13] Wyrok SN z dnia 12.12.2013 r., III KK 417/13.
[14] A. Łyżwa, w: *Kodeks karny. Część szczególna. Art. 148–251. Komentarz*, red. M. Banaś-Grabek, wyd. 1, Warszawa 2020, art. 190a.
[15] Wyrok SN z dnia 12.01.2016 r., IV KK 196/15.
[16] A. Grześkowiak, K. Wiak, S. Hyps, *Kodeks karny. Komentarz*, 2024, wyd. 8, Legalis (art. 190a – uporczywe nękanie).
[17] *Kodeks karny. Część szczególna. Tom II. Część I. Komentarz do art. 117–211a*, red. W. Wróbel, A. Zoll, opublikowano: WKP 2017.
[18] Tamże.
[19] Tamże.
[20] M. Mozgawa, w: *System Prawa Karnego*, t. 10, s. 475; tenże w*: Kodeks karny*, red. M. Mozgawa, s. 574–575. w: A. Łyżwa, w: *Kodeks karny. Część szczególna. Art. 148–251. Komentarz,* wyd. 1, red. M. Banaś-Grabek, Warszawa 2020, art. 190a.
[21] A. Łyżwa, w: *Kodeks karny. Część szczególna. Art. 148–251. Komentarz*, wyd. 1, red. M. Banaś-Grabek, Warszawa 2020, art. 190a.

Summary

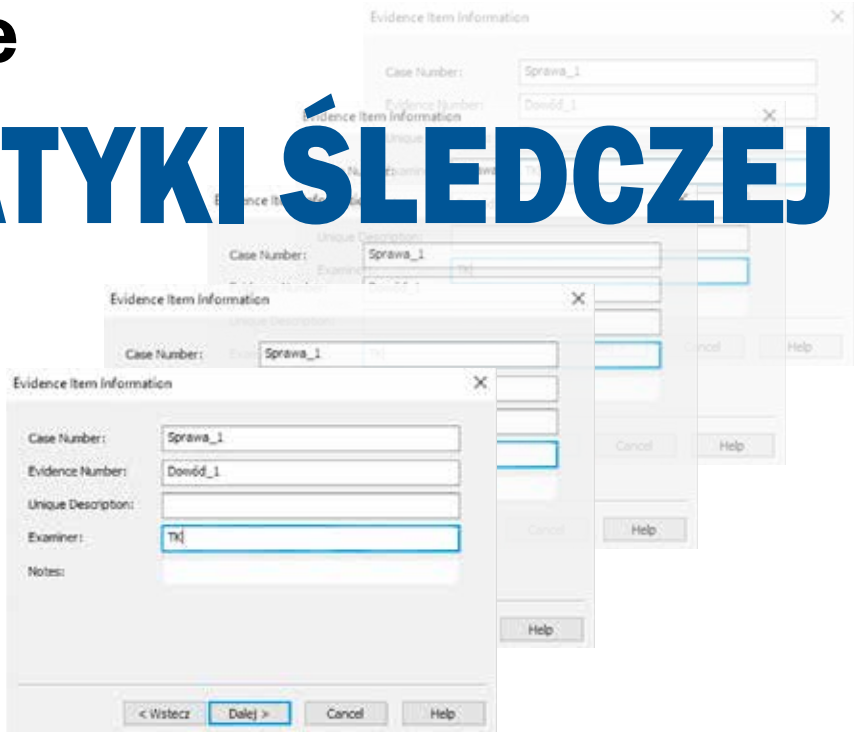
Cyberstalking as a violent tool

The article presents the legal aspects of the crime of "cyberstalking," also discussed in other publications as "cyberbullying" or persistent harassment via the Internet. Cyberstalking is the use of information and communication techniques for deliberate, repeated and hostile behavior by a person or group of persons, aimed at harming others.

The publication describes the statutory elements of the crimes of Article 190a § 1–3 of the Penal Code by subject and object, including in the context of Internet activities. Attention was also paid to the possible concurrence of crimes and the mode of prosecution. The characterization of individual elements has been based on court case law and the recognized position of representatives of the legal doctrine.

Tłumaczenie: Katarzyna Olbryś

Wykorzystanie INFORMATYKI ŚLEDCZEJ w procesie zabezpieczania dowodów cyfrowych



podkom. Tomasz Kłys

Zakład Kryminalny
Szkoła Policji w Pile

Niniejszy artykuł jest kompleksowym ujęciem zagadnienia dotyczącego wykorzystania informatyki śledczej oraz oprogramowania *live forensic*[1] do zabezpieczania danych zgromadzonych na nośnikach cyfrowych. Przedstawiono w nim definicję i podział dowodów cyfrowych, a także omówiono rolę i znaczenie prawidłowego zabezpieczania danych do celów dowodowych. Ponadto zaprezentowano metodologię wykonywania kopii binarnej dysku z wykorzystaniem oprogramowania kryminalistycznego FTK Imager, wskazując na istotę właściwego zabezpieczenia dowodu cyfrowego za pomocą jednokierunkowej funkcji skrótu, gwarantującej zachowanie integralności danych.

Wprowadzenie

Rozwój branży informatycznej doprowadził do wzrostu wydajności komputerów oraz zwiększenia pojemności elektronicznych nośników pamięci. Pojawiające się zmiany w istotny sposób wymusiły konieczność wprowadzenia modyfikacji w metodach i technikach pozwalających na ujawnianie, zabezpieczanie, analizę i skuteczne wykorzystanie w procesie karnym informacji, których nośnikiem jest sprzęt komputerowy[2].

Współczesne prawo dowodowe nieustannie napotyka na coraz to nowsze metody dochodzenia prawdy. Dowody cyfrowe stanowią kolejną propozycję, choć ich gromadzenie, zabezpieczanie, a następnie zastosowanie bardzo często bywa procesem charakteryzującym się wysokim poziomem skomplikowania. Warto zatem zaznaczyć, jak ważna jest standaryzacja metodyki postępowania z dowodami cyfrowymi i szkolenie w tej dziedzinie funkcjonariuszy organów ścigania i wymiaru sprawiedliwości oraz biegłych.

Czym są dowody cyfrowe?

W procedurze karnej brak jest osobnej definicji dowodów cyfrowych lub elektronicznych. Są to więc dowody rzeczowe, które jednak ze względu na swoją formę posiadają charakterystyczne cechy. Za taki dowód można uznać informację występującą pod postacią danych w formie cyfrowej, która ma znaczenie dla postępowania karnego.
Do specyficznych cech danych w formie cyfrowej należy zaliczyć przede wszystkim:
– łatwość dokonania zmiany danych (przypadkowo lub celowo); dane cyfrowe są łatwe do zmodyfikowania, niekiedy można tego dokonać w sposób niemożliwy do wykrycia; wymagają więc szczególnej ostrożności przy ich zabezpieczaniu i analizie;
– brak rzeczywistych różnic pomiędzy „kopią" a „oryginałem" danych; ponieważ dane cyfrowe zapisywane są za pomocą wartości binarnych (0 lub 1), to nie mają one indywidualnych cech identyfikacyjnych; możliwe jest więc wykonanie wiernej i wiarygodnej kopii danych, która będzie identyczna z oryginałem[3].
Dowody elektroniczne mogą składać się z materiałów różniących się od siebie pod względem prezentowanych treści. Zaliczają się do nich:
– dowody zawierające tekst – dokumenty elektroniczne sporządzone w formie pisemnej, które najczęściej zapisane zostały w plikach z rozszerzeniem .doc, .pdf lub .txt;
– dowody zawierające obrazy – mogą one składać się z zapisów zdjęć, filmów lub nagrań z kamer; do najczęściej wykorzystywanych formatów zaliczyć można rozszerzenie .jpg, .gif, .avi, .mpg;
– dowody zawierające zapis dźwięku – nagrania audialne, które mogą być zapisane jako dane cyfrowe lub analogowe; w szczególności mogą być to pliki o rozszerzeniu .wav lub .mp3;
– dowody zawierające dane o pracy systemu – są to logi lub zapisy audytowe, które umożliwiają odtworzenie historii pracy systemu; w rezultacie pozwala to na odtworzenie *modus operandi* sprawcy ataku; wielu informacji na temat aktywności użytkownika w ramach korzystania z różnych usług sieciowych dostarczają również pliki cookies;
– dowody zawierające dane tworzące kod maszynowy oprogramowania – to skomplikowane pliki programów, które są całkowicie nieczytelne dla człowieka; wykonywane są one wyłącznie przez przystosowane do tego urządzenia, czyli na przykład komputer z odpowiednim systemem operacyjnym[4].
Biorąc pod uwagę kryterium powstania zapisu, dowody elektroniczne można podzielić na:
– dowody elektroniczne pierwotne,
– dowody zdigitalizowane[5].
Ostatni podział dowodów elektronicznych uwzględnia kryterium źródła, z którego materiał dowodowy został pozyskany. Wyodrębnione zostały:
– dowody elektroniczne przechwycone w czasie transmisji, zebrane w ramach kontroli operacyjnej lub podsłuchu procesowego,
– dowody elektroniczne tworzone przez dane zapisane lokalnie na informatycznych nośnikach danych[6].

Materiał dowodowy w postaci elektronicznej można spotkać właściwie w każdym miejscu, w którym odbywa się ludzka aktywność[7]. Wszystko za sprawą nieustannie postępującego procesu cyfryzacji. Coraz trudniej wykonywać codzienne zadania bez wykorzystania urządzeń elektronicznych, zestawiania połączeń głosowych, obsługi poczty elektronicznej, dokonywania transakcji z wykorzystaniem kart płatniczych lub korzystania z najróżniejszych aplikacji. Charakteryzując dowody elektroniczne, nie można zatem ograniczać się wyłącznie do materiałów, które zapisane zostały na nośnikach danych lub komputerach.
Dane komputerowe mogą być przetwarzane lokalnie lub w szeroko rozumianej cyberprzestrzeni o potencjalnie globalnym zasięgu. Źródła odseparowane od cyberprzestrzeni wiążą się bezpośrednio z wszelkiego rodzaju pamięcią przenośną, która nie została podłączona do sieci lub też do urządzenia posiadającego czynne połączenie sieciowe. Z kolei szeroko rozumiane zasoby cyberprzestrzeni oznaczają materiały, które mogą być zlokalizowane w dowolnym typie pamięci systemów teleinformatycznych, funkcjonujących w sieci urządzeń cyfrowych, a przede wszystkim w Internecie. W tej kategorii źródeł dowodowych mieszczą się również urządzenia wykorzystywane do budowy infrastruktury sieciowej, takie jak routery, przełączniki lub centrale[8].
Istotą dowodu elektronicznego jest jego szczególna forma, która wyraża się w elektronicznym zapisie, przez co odczyt treści materiału nie jest możliwy bez zastosowania odpowiedniego urządzenia do przetwarzania informacji. Mogą one przybierać rozmaite formy w postaci zapisu plików tekstowych, multimedialnych, wiadomości pocztowych, historii ruchu sieciowego lub wpisów na forach i portalach społecznościowych. W celu ich pozyskania istnieje możliwość fizycznego zabezpieczenia danego nośnika wykorzystanego w systemie pracującym lokalnie lub w sieci, albo też w ramach zabezpieczenia materiałów przetwarzanych online[9].

Wykorzystanie informatyki śledczej

Informatyka śledcza służy poszukiwaniu, zabezpieczaniu oraz analizie danych elektronicznych, czyli innymi słowy – dowodów elektronicznych. Jest ona wykorzystywana przez organy ścigania w walce z przestępczością, w szczególności zaś z przestępstwami popełnianymi w Internecie oraz za pomocą komputera.
Podczas wykonywania czynności związanych z zabezpieczaniem danych cyfrowych pojawia się pytanie o konieczność zabezpieczania sprzętu komputerowego oraz nośników. Zasada proporcjonalności wymusza na organach procesowych potrzebę kierowania się w swoich decyzjach faktyczną koniecznością, a nie wygodą prowadzącego czynność[10].

Wykonanie kopii binarnej dysku

W sprawach, w których nie zachodzi konieczność zabezpieczenia danych wraz z nośnikiem, regułą będzie sporządzenie pełnego duplikatu zawartości danego nośnika w postaci jego kopii binarnej, mogącej mieć postać klona bądź obrazu. Klonowanie danych, jak sama nazwa wska-

zuje, prowadzi do utworzenia lustrzanej kopii zawartości dysku dowodowego na odrębnym dysku twardym, z uwzględnieniem danych niewidocznych/usuniętych oraz niezalokowanych obszarów oryginalnego nośnika, w którym również mogą znajdować się dane istotne dla sprawy[11].

Z praktycznego punktu widzenia klon dysku bez przeszkód można zamontować w komputerze, z którego pochodzi dysk dowodowy, uruchomić system operacyjny i korzystać z zainstalowanych w nim aplikacji. Klonowanie dysku ma też niestety istotną wadę. Mianowicie, przy każdym starcie systemu operacyjnego zmianie ulegają wpisy w dziennikach zdarzeń (logach) oraz daty dostępu i zawartość niektórych plików używanych przez system operacyjny. Analogiczne zmiany zachodzą też w plikach otwieranych przez użytkownika. Tym samym dochodzi do naniesienia zmian w materiale dowodowym, co na etapie postępowania sądowego może być przyczyną jego zakwestionowania. Dlatego też nie można ograniczyć się do sporządzenia tylko jednego egzemplarza klona dysku dowodowego, muszą zostać sporządzone przynajmniej dwie kopie – jedna dla celów dowodowych, a druga do wykorzystania w badaniach kryminalistycznych. Trzeba też mieć świadomość, że nawet w przypadku dołączenia sklonowanego dysku do komputera (jako kolejnego, np. za pomocą zewnętrznej kieszeni USB) również nastąpią zmiany w jego zawartości, przez co jego wiarygodność jako materiału dowodowego może zostać podważona. Z tego też względu generalną zasadą jest operowanie na dysku dowodowym wyłącznie z użyciem urządzenia blokującego zapis, popularnie zwanego blokerem[12].

Fot. 1. Forensic Blocker UltraDock FUDv6.

Źródło: Paraben. Sklep dla specjalistów kryminalistyki laboratoryjnej, https://paraben.pl/paraben-pl-3/forensic-ultradock-write-blocker/ [dostęp: 20 czerwca 2024 r.].

Sprzętowa blokada zapisu wykorzystuje interfejs, przez który dysk twardy jest podłączany do badawczej stacji roboczej. Urządzenie blokujące włączane jest między kontrolerem interfejsu zainstalowanym w stacji roboczej a badanym dyskiem twardym. Gdy system operacyjny wysyła polecenie zapisu (lub kasowania) dysku do kontrolera interfejsu, kontroler dokonuje translacji tych żądań na rozkazy specyficzne dla konkretnego interfejsu i wysyła te rozkazy do kontrolera wbudowanego w dysk twardy. Sprzętowa blokada zapisu przechwytuje te rozkazy, chroniąc dysk przed modyfikacją zawartości. Z kolei rozkazy, które nie ingerują w zawartość dysku dowodowego, są przekazywane dalej w sposób transparentny dla użytkownika[13].

Blokery mogą mieć postać modułu montowanego w zatoce na przednim panelu komputera (tak jak napędy optyczne), karty typu riser (montowanej na płycie głównej), urządzenia kieszonkowych rozmiarów w formie „kostki" z wyprowadzonymi interfejsami bądź też przenośnej lub stacjonarnej obudowy z kieszeniami na dyski twarde[14].

Alternatywą dla klonowania dysku jest utworzenie tzw. obrazu jego zawartości. Obraz dysku zwykle dzielony jest na segmenty o ustalonym rozmiarze i ma postać zbioru plików. Podobnie jak klon dysku, obraz zawiera wszelkie zapisane na nim dane, łącznie z danymi usuniętymi oraz pustymi przestrzeniami. Przewaga obrazu nad klonem polega na tym, że jego zawartości nie da się w żaden sposób zmodyfikować, w związku z czym można przeprowadzać wszelkie badania w sposób całkowicie bezpieczny. W przeciwieństwie do klona, obrazu dysku nie można zamontować w komputerze i uruchomić z niego systemu operacyjnego, jednakże wszystkie aplikacje służące do badań kryminalistycznych (tzw. *forensic software*) umożliwiają w razie potrzeby odtworzenie danych zapisanych w obrazie do postaci klona. Podobnie jak podczas tworzenia klona, należy bezwzględnie korzystać z blokera, natomiast na etapie dalszych badań konieczność taka już nie występuje. Oprogramowanie typu forensic umożliwia sporządzanie obrazów w standardowych formatach (Linux – DD, EnCase – E01), przez co możliwe jest zabezpieczenie danych jednym programem, a przeprowadzanie ich analizy innym, dowolnie wybranym przez osobę wykonującą badania kryminalistyczne[15].

Zastosowanie jednokierunkowej funkcji skrótu

Kryptograficzna funkcja haszująca to specjalna klasa funkcji haszujących, które mapują dane o dowolnym rozmiarze na probabilistycznie unikalny ciąg bitów o ustalonym rozmiarze – hash. Cechą wyróżniającą kryptograficzną funkcję skrótu jest to, że została zaprojektowana jako funkcja jednokierunkowa. Oznacza to, że praktycznie nie można jej odwrócić – tj. użyć skrótu i odtworzyć danych wejściowych użytych do jego utworzenia. Funkcje skrótu kryptograficznego mają wiele zastosowań, w tym podpisy cyfrowe, kody uwierzytelniania wiadomości (MAC) i inne formy uwierzytelniania. Mogą być również używane jako zwykłe funkcje mieszające, do indeksowania danych w tabelach haszujących. Mogą być użyte też do odcisków palców, do wykrywania duplikatów danych lub jednoznacznej identyfikacji plików oraz jako sumy kontrolne do wykrywania przypadkowego uszkodzenia danych[16].

Stosowanie urządzeń blokujących zapis, odpowiednich narzędzi programistycznych oraz właściwe dokumentowanie wykonywanych czynności jest warunkiem koniecznym do zapewnienia wiarygodności w procesie zabezpieczania danych cyfrowych, jednakże nie jest warunkiem wystarczającym[17].

Zabezpieczenie danych rozpoczyna jedynie łańcuch dowodowy, a jego niezbędnym elementem jest wyliczona za pomocą odpowiedniego algorytmu suma kontrolna zabezpieczonych danych, dzięki której możliwe będzie udowodnienie, że na żadnym etapie postępowania dane nie zostały zmienione. Suma kontrolna jest swoistym „odciskiem palca" zawartości danego nośnika i jest respektowanym przez sądy dowodem integralności danych stanowiących dowód cyfrowy[18].

Do najbardziej znanych należą: MD2, MD4, MD5, HAVAL, RIPE-MD 160, Snefru, GOST, N-Hash, SHA-1, SHA-2, zaś zdecydowanie najszersze zastosowanie praktyczne zdobyły algorytmy: MD5 i SHA-1, które są standardowo używane w programach informatyki śledczej (np. EnCase, X-Ways, FTK, PRTK), operujących na cyfrowym materiale dowodowym[19]. Algorytmy MD5 i SHA-1 generują wartości *hash* o długości odpowiednio 128 i 160 bitów, czyli liczba możliwych kombinacji wynosi 2^{128} i 2^{160}. Liczby te są praktycznie nieskończone[20].

Jakakolwiek zmiana zawartości pliku skutkuje jednocześnie wygenerowaniem zupełnie nowych sum kontrolnych. Dzięki temu w prosty sposób można dokonać sprawdzenia integralności danych. Przebieg tego procesu z użyciem oprogramowania Hasher, wykorzystywanego do obliczania funkcji skrótu, został zaprezentowany na fotografiach nr 2–7.

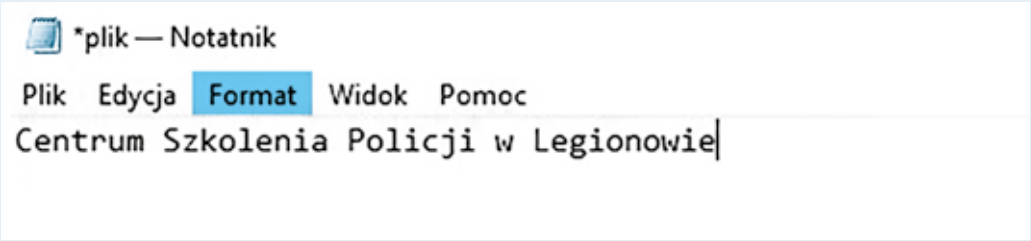
Live forensic z wykorzystaniem oprogramowania FTK Imager

FTK Imager to narzędzie do podglądu danych i tworzenia obrazów zabezpieczonego materiału dowodowego. Umożliwia szybką ocenę dowodów elektronicznych w celu ustalenia, czy dalsza analiza za pomocą narzędzi kryminalistycznych (np. takich jak Forensic Toolkit) jest uzasadniona.

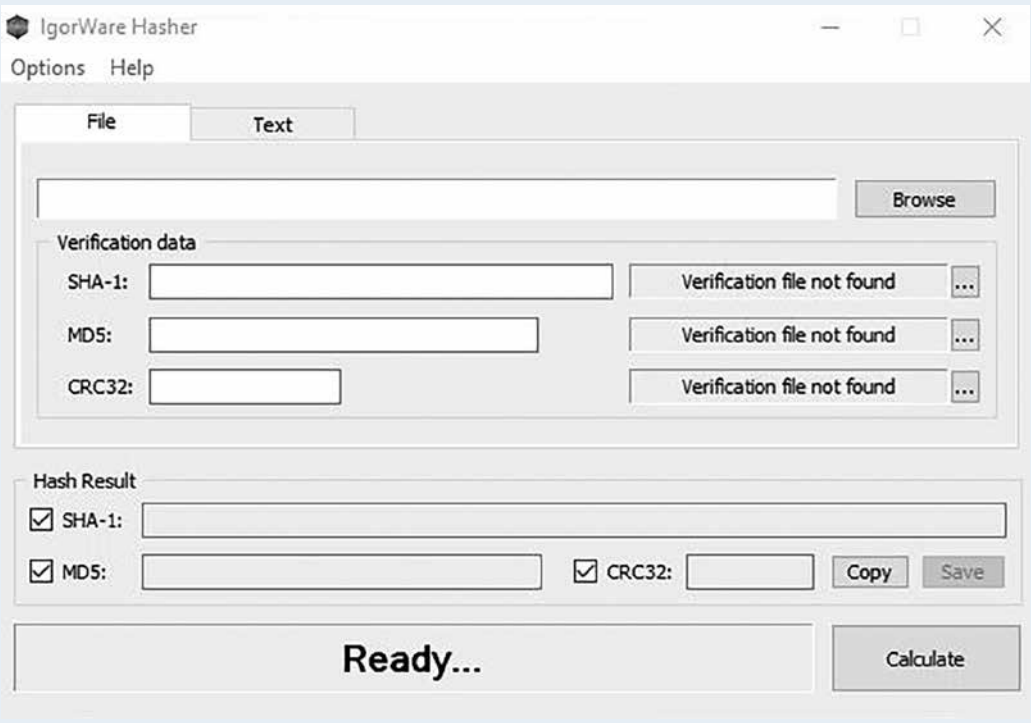
Oprogramowanie może także tworzyć kopie danych bez wprowadzania zmian w oryginalnych materiałach dowodowych. Umożliwia akwizycję fizycznych obrazów dysków, tworzenie wielokrotnych obrazów jednego źródła oraz pozwala na łatwy dostęp do systemów plików w formatach CDFS i DVD. Dedykowane jest służbom rządowym i profesjonalistom zajmującym się bezpieczeństwem informacji, którzy są zainteresowani szybkim kopiowaniem danych z systemów plików FAT, NTFS EXT 2 i 3, HFS i HPFS.

Za pomocą oprogramowania FTK Imager można stworzyć obrazy w formatach DD, SMART, EnCase rozpoznawane przez oprogramowanie do zaawansowanej analizy danych (Magnet AXIOM, EnCase Forensic, Forensic Toolkit, X-Ways Forensic)[21] (fot. 8).

Do stworzenia kopii binarnej nośnika należy skorzystać z opcji Create Disk Image (fot. 9).

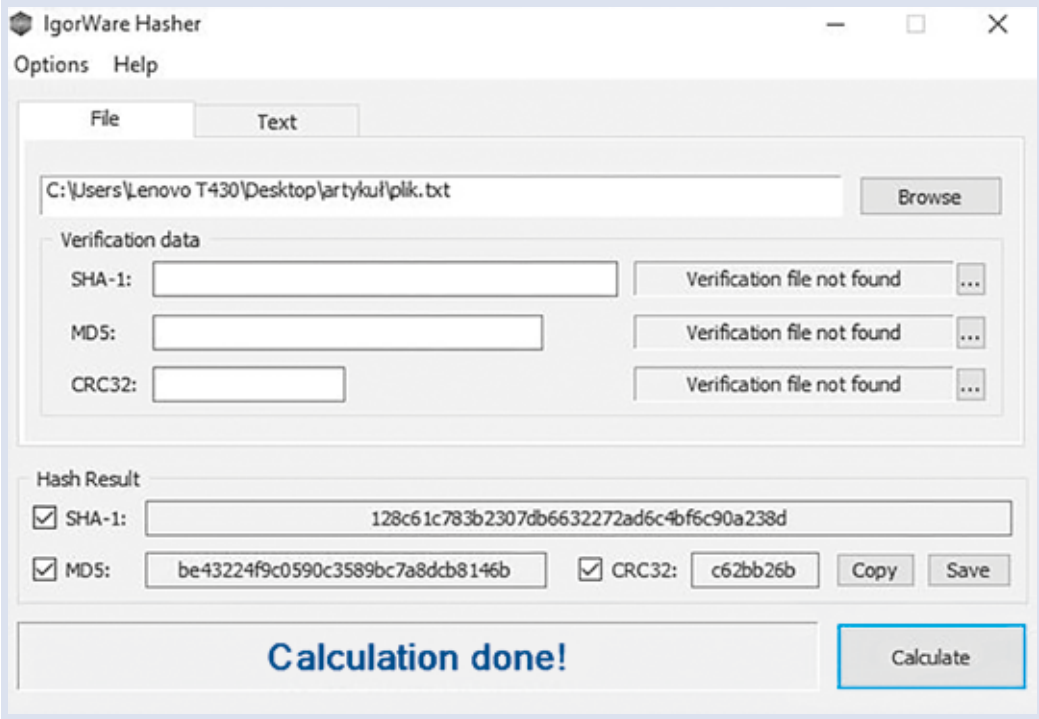


Fot. 2. Wykorzystany plik testowy.
Źródło: opracowanie autora.

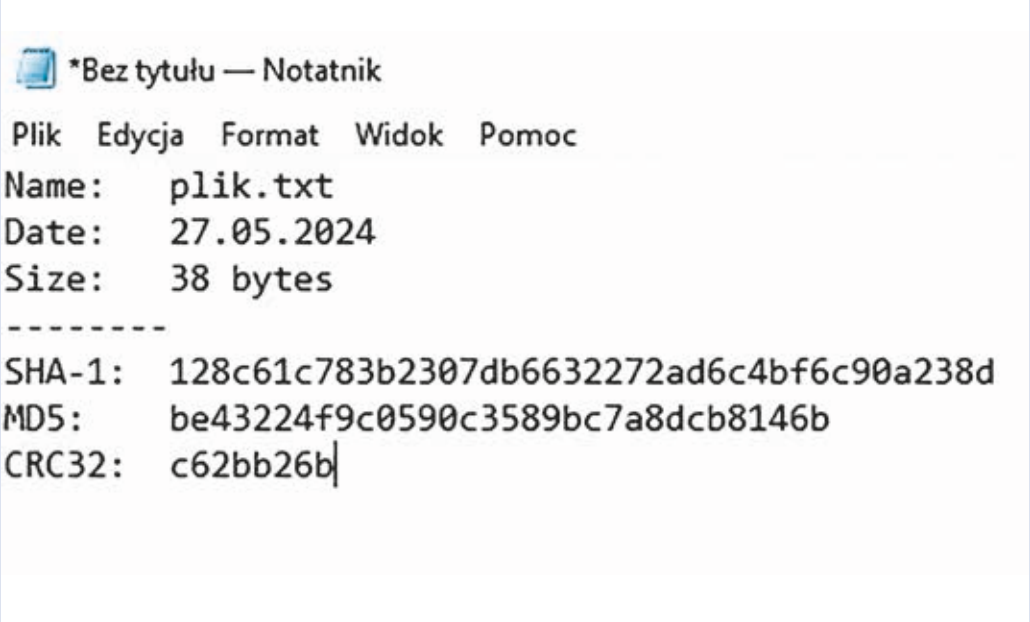


Fot. 3. Program Hasher.
Źródło: opracowanie autora.

Nośniki w postaci dysków twardych lub innych zewnętrznych nośników pamięci mogą zostać sklonowane lub zabezpieczone pod postacią wykonania obrazu dysku, poprzez wybranie opcji Physical Driver. Możliwe jest również zabezpieczenie logicznej partycji, pliku, folderu lub nośników optycznych (fot. 10).
Następnie należy wskazać interesujący nas nośnik (fot. 11). Oprogramowanie umożliwia wykonanie kopii binarnej w jednym z wybranych przez użytkownika formatów. Najczęściej wykorzystywany jest format Raw (dd) lub E01, który daje możliwość zastosowania dodatkowej kompresji. W rezultacie wielkość pliku jest mniejsza, jednak sam proces kompresji wiąże się z wydłużeniem czasu potrzebnego do wykonania kopii binarnej (fot. 12–15).
Po jego zakończeniu w sposób zautomatyzowany dochodzi do wygenerowania sum kontrolnych z wykorzystaniem algorytmów MD5 i SHA-1. Jednocześnie pojawiają się informacje o zgodności danych zawartych na pierwotnym nośniku z jego kopią (fot. 16).

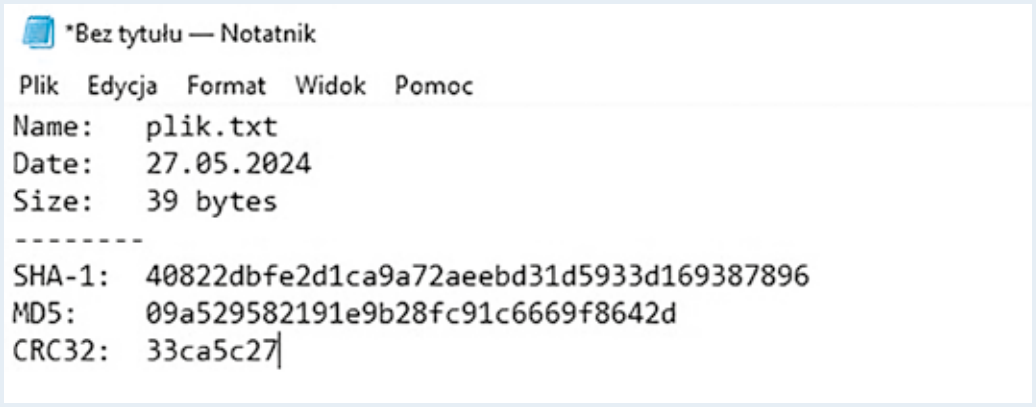


Fot. 4. Wyliczone funkcje skrótu w formatach SHA-1, MD5 oraz CRC32.
Źródło: opracowanie autora.

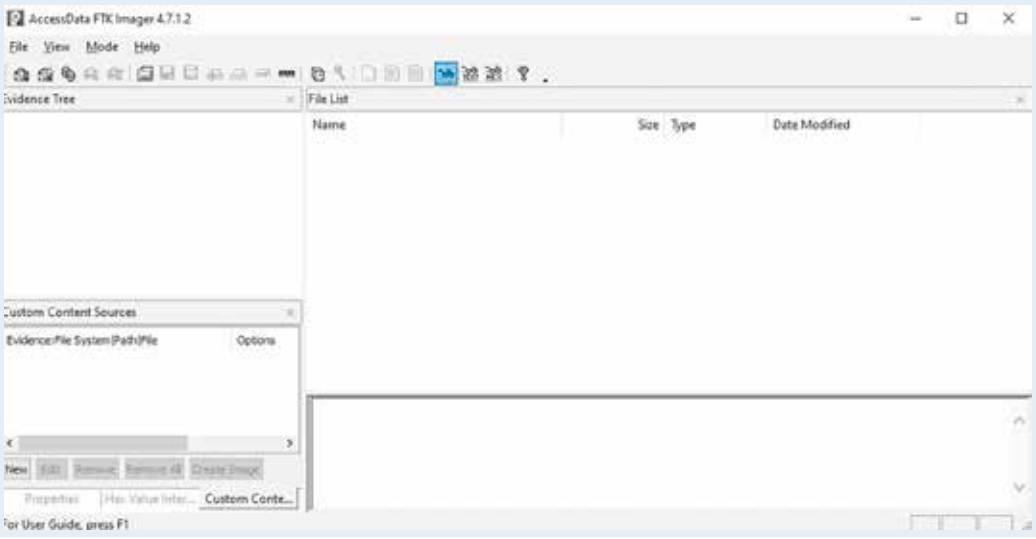


Fot. 5. Raport z obliczeń
Źródło: opracowanie autora.

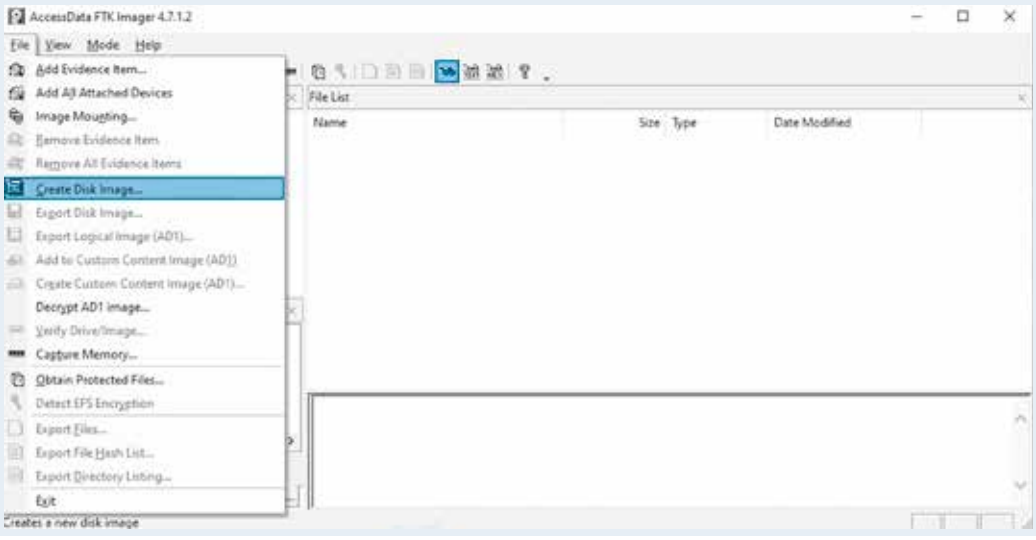
Fot. 6. W pliku testowym dokonano zmiany, wprowadzając na końcu wpisu pusty znak w postaci spacji.
Źródło: opracowanie autora.



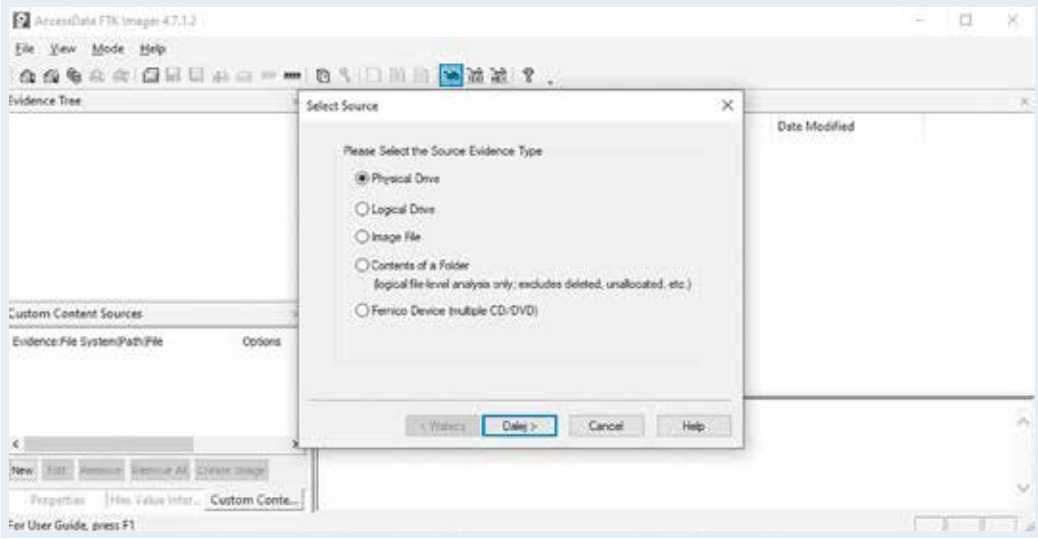
Fot. 7. Ponowne wygenerowanie funkcji haszujących wskazuje na zmianę zapisów w każdym z wykorzystanych algorytmów, co jednoznacznie świadczy o ingerencji w pierwotnym pliku.
Źródło: opracowanie autora.



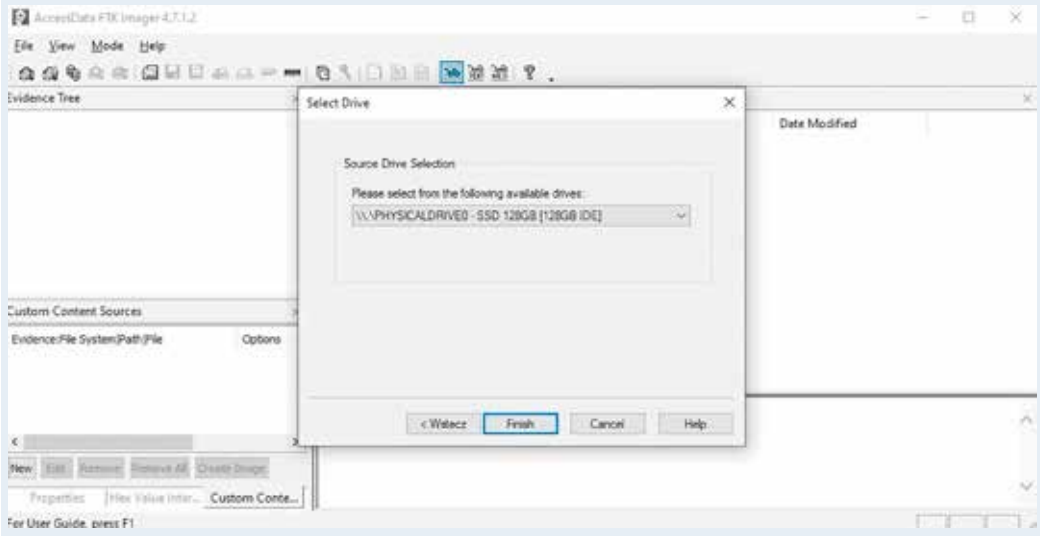
Fot. 8. Program FTK Imager.
Źródło: opracowanie autora.



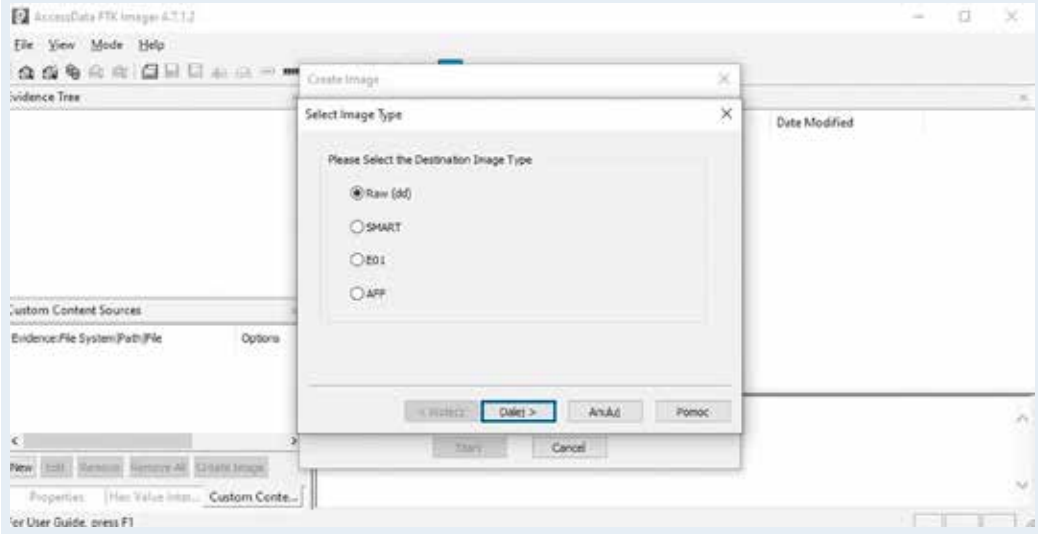
Fot. 9. Program FTK Imager.
Źródło: opracowanie autora.



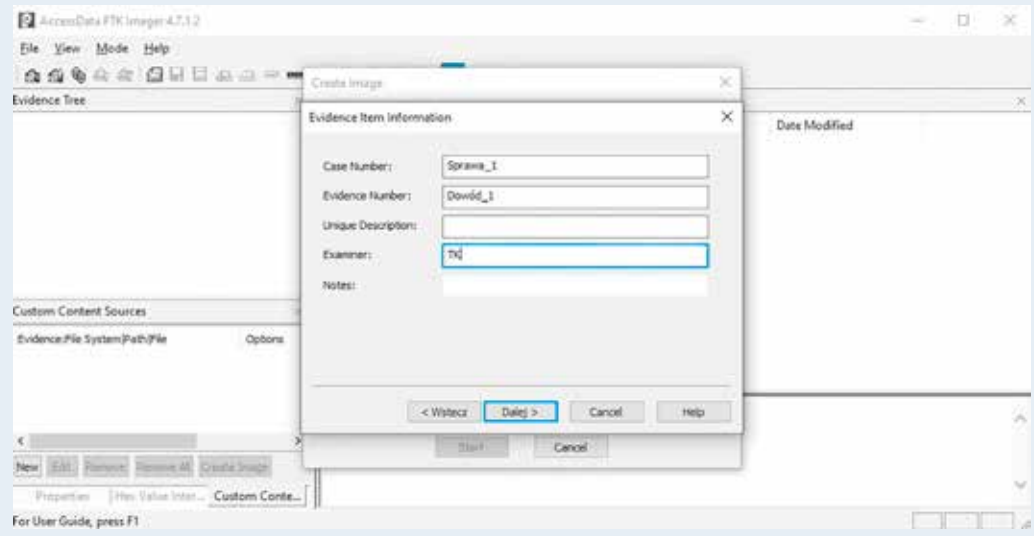
Fot. 10. Program FTK Imager.
Źródło: opracowanie autora.



Fot. 11. Program FTK Imager.
Źródło: opracowanie autora.

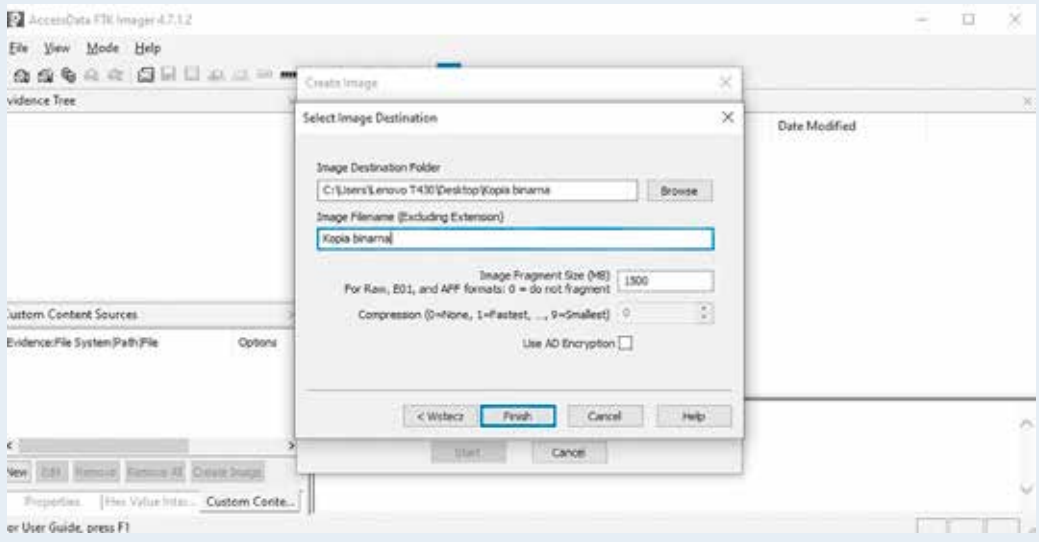


Fot. 12. Program FTK Imager.
Źródło: opracowanie autora.



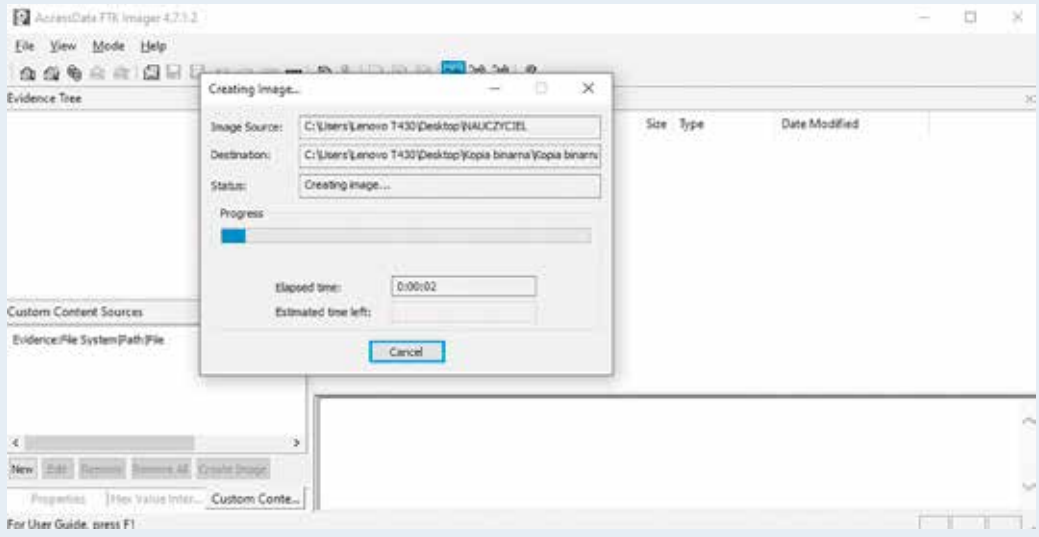
Fot. 13. Przed zapisem warto dodać szczegółowe informacje dotyczące pliku.

Źródło: opracowanie autora.



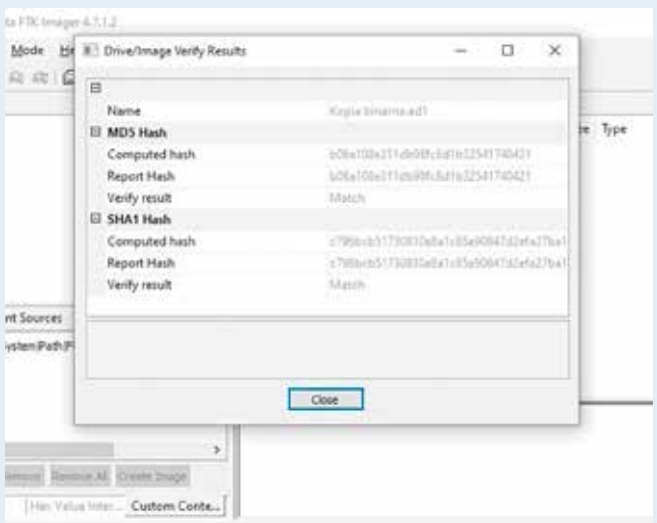
Fot. 14. Następnym krokiem jest wskazanie miejsca zapisu pliku oraz nadanie nazwy.

Źródło: opracowanie autora.



Fot. 15. Proces wykonywania kopii binarnej.

Źródło: opracowanie autora.



Fot. 16. Program FTK Imager.
Źródło: opracowanie autora.

Zabezpieczenie sprzętu w całości

Zabezpieczanie danych cyfrowych wraz z nośnikiem, na którym są one zapisane, jest zasadne w sytuacji, gdy:
– nośnik ten będzie zaliczony w poczet materiału dowodowego;
– sytuacja na miejscu przeszukania nie pozwala na poprawne, tj. zgodne z wypracowanymi zasadami kryminalistyki, skopiowanie danych;
– sposób zabezpieczenia danych przez ich dysponenta uniemożliwia ich skopiowanie;
– na nośniku zawarto dane objęte tajemnicą prawnie chronioną, a organ uprawniony do uchylenia tajemnicy nie jest organem dokonującym przeszukania;
– czas trwania zabezpieczenia danych przekraczałby rozsądne granice, np. trwałby ponad 10 godzin[22].

W pozostałych przypadkach organy procesowe mogą poprzestać na skopiowaniu danych z wykorzystaniem funkcji haszujących. Należy jednak pamiętać o tym, że prawidłowe zabezpieczanie dużej ilości danych, których skopiowanie wiąże się z ponaddziesięciogodzinnym czasem trwania czynności procesowej, w przypadku lokali zamieszkałych może zostać uznane za nieproporcjonalną dolegliwość[23].

Podsumowanie

W postępowaniu karnym wszelkie nieprawidłowości w sposobie zabezpieczenia dowodów elektronicznych mogą skutkować uznaniem tych dowodów za wadliwe i wykluczeniem ich z materiału dowodowego. Stwierdzenie wadliwości dowodu elektronicznego może wywołać uchylenie opartych na tych dowodach decyzji procesowych, a nawet doprowadzić do umorzenia postępowania bądź uniewinnienia oskarżonego. W szczególności dotyczy to sytuacji, gdy powstała wątpliwość co do wiarygodności dowodu elektronicznego zaciąży istotnie na stopniu uprawdopodobnienia zarzutu[24]. Wszystkie czynności powinny być wykonywane z należytą starannością oraz oparte o aktualną wiedzę specjalistyczną. Należy zatem zauważyć, jak dużą rolę odgrywa proces nieustannego poszerzania przez policjantów własnych kompetencji w tej materii.

[1] Metoda polegająca na zabezpieczaniu dowodów elektronicznych z uruchomionych systemów komputerowych.
[2] M. Chrabkowski, K. Gwizdała, *Zabezpieczenie dowodów elektronicznych*, „Prokuratura i Prawo" 2015, nr 12, s. 164.
[3] Kryminalistyka, *Dowody cyfrowe*, http://dowody.karne.pl/cyfrowe.html [dostęp: 2.05.2024 r.].
[4] J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne,* Białystok 2017, s. 311–312.
[5] A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 37.
[6] J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne,* s. 318.
[7] K.J. Pawelec, *Proces dowodzenia w postępowaniu karnym*, Warszawa 2010, s. 24.
[8] J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, s. 326.
[9] Tamże, s. 331.
[10] A. Lach, *Dowody elektroniczne w procesie karnym*, s. 110.
[11] M. Chrabkowski, K. Gwizdała, *Zabezpieczenie dowodów elektronicznych,* s. 167.
[12] Tamże, s. 167–168.
[13] T. Nieradko, *Sprzętowe zabezpieczenia dysków twardych przed zapisem*, w: Materiały poseminaryjne VII Seminarium Naukowego pt. „Przestępczość teleinformatyczna", red. J. Kosiński, Szczytno 2004, s. 270.
[14] M. Chrabkowski, K. Gwizdała, *Zabezpieczenie dowodów elektronicznych,* s. 168.
[15] Tamże, s. 169.
[16] Tamże.
[17] Tamże.
[18] P. Krejza, *Informatyka śledcza – zabezpieczanie danych w krytycznych zasobach on-line oraz w systemach z ryzykiem wyłączenia*, w: Materiały poseminaryjne X Seminarium Naukowego pt. „Przestępczość teleinformatyczna", red. J. Kosiński, Szczytno 2007, s. 102.
[19] J. Chmura, *Wybrane zagadnienia kryptologii w pracy ekspertów Pracowni Badań Sprzętu Komputerowego i Cyfrowych Nośników Danych*, Lublin 2009, s. 19.
[20] M. Chrabkowski, K. Gwizdała, *Zabezpieczenie dowodów elektronicznych,* s. 171.
[21] Mediarecovery, *FTK Imager*, https://mediarecovery.pl/product/ftk-imager/ [dostęp: 10.06.2024 r.]
[22] M. Chrabkowski, K. Gwizdała, *Zabezpieczenie dowodów elektronicznych,* s. 177.
[23] Tamże.
[24] Tamże, s. 178.

Summary

The use of computer forensics in the process of securing digital evidence

The publication is a comprehensive treatment of the issue of using computer forensics and live forensic software to secure data stored on digital media. It provides a definition and breakdown of digital evidence and discusses the role and importance of properly securing data for evidentiary purposes. The publication uses FTK Imager forensic software to demonstrate the methodology for making a binary copy of a disk, pointing out the importance of properly securing digital evidence using a one-way hash function to guarantee data integrity.

Tłumaczenie: autor

CYBERBEZPIECZEŃSTWO

W INSTYTUCJACH PUBLICZNYCH

Zagrożenia i sposoby ochrony

mł. asp. Paweł Tomaszewski

Zakład Służby Kryminalnej CSP

W niniejszym artykule zdefiniowano termin cyberbezpieczeństwo, a także przedstawiono najbardziej popularne zagrożenia z tego obszaru, na które obecnie narażone są instytucje publiczne. Ponadto opisano sposoby postępowania w przypadku wybranych cyberataków oraz metody zapobiegania zagrożeniom systemów informatycznych wykorzystywanych przez te instytucje. Wskazano, że niezmiennie najsłabszym ogniwem obszaru bezpieczeństwa informatycznego jest użytkownik końcowy, czyli człowiek. Podkreślono więc ogromną rolę nieustannych szkoleń dla użytkowników.

Cyberbezpieczeństwo to ramowy termin obejmujący współcześnie swym zakresem ogół wypracowanych praktyk, technik oraz procesów wykorzystywanych dla zapewnienia bezpieczeństwa: układom sieci informatycznych, działającemu w ich środowisku oprogramowaniu czy też zasobom danych gromadzonych i przetwarzanych w ramach baz[1]. Bezpieczeństwo obszaru cyber jest więc ukierunkowane na neutralizację ataków wymierzonych w systemy informatyczne czy też uniemożliwienie intruzowi wszelkich działań pozwalających na nieautoryzowany dostęp do aplikacji[2].

Upraszczając nieco tę kwestię, z punktu widzenia użytkownika końcowego, można stwierdzić, że cyberbezpieczeństwo to niepodatność systemów informatycznych na interakcje prowadzące do złamania standardów obejmujących normy: poufności, integralności, dostępności oraz autentyczności, wykorzystywanych w trakcie konwersji danych.

Kwestia obszaru cyberbezpieczeństwa może być dyskusyjna, jest więc nieco inna z punktu widzenia administratora sieci i użytkownika końcowego, nie ulega jednak wątpliwości, że zarówno jednym, jak i drugim zależy na bezawaryjnej i bezpiecznej pracy systemu informatycznego[3].

Cyberbezpieczeństwo jest stosunkowo nową dziedziną wiedzy, która znajduje zastosowanie w codziennym życiu osób prywatnych, ale jest kluczowa przede wszystkim dla przedsiębiorstw i instytucji. Znajduje do niego pełne zastosowanie ponadczasowa maksyma, która mówi, że lepiej zapobiegać niż leczyć. W zakresie cyberbezpieczeństwa jest naprawdę wiele obszarów, w których należy zachować szczególną ostrożność.

W niniejszym artykule chciałbym skupić się na najbardziej powszechnych aktualnie zagrożeniach dla systemów informatycznych oraz danych należących do instytucji publicznych[4].

ZAGROŻENIE 1. NIEZABEZPIECZENIE DYSKÓW PAMIĘCI URZĄDZEŃ BIUROWYCH

Warto podkreślić, że kardynalnym i nagminnym błędem popełnianym obecnie przez instytucje publiczne w obszarze cyberbezpieczeństwa jest chęć obniżenia kosztów obsługi urządzeń biurowych. Zamiast nabywać sprzęt na własność jest on pozyskiwany w ramach wynajmu czy też opłaty za świadczoną usługę.

Pozornie wszystko jest w porządku, zaoszczędzono pieniądze podatnika, a serwis często psującego się sprzętu spoczywa na dostarczycielu usługi. Jeśli analizujemy tę istotną kwestię, każdemu pracownikowi biurowemu jako pierwsze na myśl przychodzi użytkowanie urządzeń wielofunkcyjnych (drukarka, skaner, kopiarka), których ceny kształtują się często na poziomie kilkunastu czy kilkudziesięciu tysięcy złotych. Oczywiście, nowoczesna technologia i jakość mają wysoką cenę, w tym wypadku bardzo często pomija się jednak kwestię bezpieczeństwa. Współczesne urządzenia wielofunkcyjne mają wbudowane dyski pamięci, które rejestrują treść każdej wykonanej czynności. Tak więc firma zewnętrzna, która w ramach wygranego przetargu świadczy usługi biurowe dla instytucji, pod pretekstem serwisu sprzętu może wymieniać regularnie niniejsze dyski, co potencjalnie daje bezcenną wiedzę, którą można wykorzystać w nielegalny sposób[5]. Informacje z biurowych urządzeń wielofunkcyjnych można pozyskiwać nie tylko metodą fizycznego przejmowania wymiennych dysków, lecz także bardziej wysublimowanymi sposobami, wymagającymi wiedzy fachowej[6]. Jest to możliwe, ponieważ administratorzy w instytucjach bardzo często zapominają o odłączeniu „kombajnów" od publicznego Internetu[7]. Pozostawia to włamywaczowi otwartą furtkę, gdyż często pomijany jest element zapory, która blokuje zarówno przychodzący, jak i wychodzący ruch sieciowy z publicznym Internetem.

Brak wspomnianej zapory zabezpieczającej urządzenie wielofunkcyjne często idzie w parze z brakiem hasła autoryzującego proces drukowania[8]. W instytucjach niejednokrotnie pomija się opcje skonfigurowania urządzenia pod indywidualne potrzeby użytkownika, pozostawiając ustawienia fabryczne, które nadają użytkownikowi szerokie kompetencje, co również stanowi lukę, przez którą można przeprowadzić cyberatak. Czy drukarka obsługuje przesyłanie plików przez FTP? Czy jest to potrzebne w codziennym życiu? Jeśli nie, dobrze gdyby administrator dezaktywował tę funkcję.

ZAGROŻENIE 2. URZĄDZENIA USB

Kolejnym obszarem wielu zagrożeń cyberbezpieczeństwa w instytucjach są urządzenia USB, często mylnie kojarzone jedynie z pendrive'ami. Należy jednak mieć na uwadze, iż w tej grupie urządzeń znajdują się również: zewnętrzne dyski twarde, modemy, aparaty fotograficzne, myszki czy klawiatury. Poprzez ten sprzęt, pozbawiony zabezpieczeń i nadzoru administratora, może dojść do wycieku danych czy zainfekowania komputera złośliwym oprogramowaniem[9].

Administratorzy instytucji publicznych często dalej pozbawieni są komercyjnych programów do monitorowania urządzeń USB, a ze swojej strony nie blokują portów USB, gdyż mocno utrudniałoby to pracę użytkowników końcowych. W dużych firmach prywatnych, gdzie obszar IT jest istotnym filarem działalności przedsiębiorstwa, obecnie często wykorzystuje się oprogramowanie z grupy roboczo zwanej Ekran System, które pozwala na: kontrolowanie i monitorowanie urządzeń USB podłączanych do komputera, otrzymywanie alertów o podłączanych urządzeniach, a także finalnie blokowanie podłączonego urządzenia. Powszechne zastosowanie w instytucjach oprogramowania rodzaju Ekran System nie tylko zabezpieczyłoby je przed wszelkimi wyciekami danych poprzez USB, lecz także dałoby możliwość nagrywania bieżącej działalności na komputerze poszczególnych urzędników, co ułatwiłoby wykrycie ewentualnego wycieku danych czy popełnionego błędu.

Problematyka pamięci przenośnej, dotycząca przede wszystkim pendrive'ów, jest też istotna w odniesieniu do osób, które przychodzą do urzędów załatwić ważną dla nich sprawę, przynosząc dokument zapisany w pliku[10]. W większości przypadków nie zarzucamy petentowi złej woli, jednak dostarczony przez taką osobę nośnik danych może być w różnym stanie technicznym, jak i zainfekowany różnego rodzaju wirusami, a tym samym stanowić zagrożenie dla sprzętu komputerowego instytucji. W skrajnych przypadkach możemy mieć do czynienia z działaniem w złej woli[11] polegającym na przedłożeniu urzędnikowi spreparowanego nośnika, który po włożeniu do portu USB uruchomi funkcję AutoRun, często aktywną na wielu komputerach[12]. Funkcja ta uruchamia się automatycznie w momencie, gdy komputer wykryje obecność dysku USB w porcie USB. W tej samej chwili wirus znajdujący się na dysku USB zostanie przeniesiony i uaktywniony na komputerze biorcy. Jest to skrajnie niebezpieczne, ponieważ urzędnik, który zaufał takiej osobie, nie zdaje sobie sprawy z tego, co naprawdę się wydarzyło. A skala zagrożenia jest szeroka. Przenośne dyski mogą bowiem infekować komputery poprzez konie trojańskie czy złośliwe oprogramowanie umożliwiające dostęp stron trzecich do komputera i informacji.

ZAGROŻENIE 3. DOSTĘP DO INTERNETU I PRACA ZDALNA

Kolejną drażliwą kwestią jest częste bagatelizowanie przez instytucje publiczne środków bezpieczeństwa w trakcie korzystania przez użytkowników końcowych z dobrodziejstw Internetu. Tę lukę bezpieczeństwa w dużej mierze pomniejszyły firmy komercyjne w dobie epidemii Covid-19, kiedy to na szeroką skalę praca przeniosła się z biur do prywatnych mieszkań pracowników. Możliwość wykonywania obowiązków zapewniona była właśnie dzięki sieci Internet. Dla zwiększenia poziomu bezpieczeństwa przesyłania danych zaczęto stosować VPN (*Virtual Private Network*)[13]. VPN z zasady zapewnia bezpieczeństwo sieci i pozwala oszczędzać przepustowość łącz internetowych. Poniżej wymieniono podstawowe zalety korzystania z VPN w środowisku pracy[14].

Korzystanie z VPN zapewnia:

1) **prywatność i anonimowość –** VPN kamufluje prawdziwe IP użytkownika, dokonując jego konwersji na inne zdalne IP, co sprawia, że działania użytkownika w Internecie są dużo trudniejsze do śledzenia, co zwiększa bezpieczeństwo danych;
2) **szyfrowanie danych** – wszystkie pakiety danych przesyłane pomiędzy komputerem użytkownika końcowego a serwerem VPN są szyfrowane, co wyraźnie utrudnia ich przechwycenie, a zarazem odczytanie przez osoby nieuprawnione;
3) **bezpieczne połączenia w publicznych sieciach** – korzystając z publicznych sieci Wi-Fi, w takich miejscach jak urzędy, centra handlowe, dworce, lotniska czy kawiarnie, należy pamiętać o korzystaniu z usługi VPN, gdyż ona znacząco zmniejszy zagrożenia pozyskania naszych danych[15];
4) **bezpieczne przesyłanie plików –** VPN ma szczególną wartość w sytuacji, kiedy mamy do czynienia z przesyłaniem plików zawierających poufne dane, ponieważ zapewnia im zabezpieczenie przed bezprawnym dostępem;
5) **większe bezpieczeństwo pracy zdalnej –** w sytuacjach nadzwyczajnych, w takich jak wspomniana już epidemia Covid-19, VPN zapewnia pracownikom zdalny dostęp do wewnętrznych zasobów i sieci instytucji w sposób dużo bardziej bezpieczny; niestety, obecnie z różnych względów nie we wszystkich instytucjach publicznych wykorzystuje się możliwości sieci VPN[16].

Najlepsze zabezpieczenia zdadzą się jednak na nic, gdy zawiedzie zdrowy rozsądek i dołączy do tego brak elementarnej wiedzy o komputerowym środowisku pracy. Przeprowadzane w urzędach szkolenia z zakresu cyberbezpieczeństwa mają bardzo często charakter formalny, gdyż nie są przeprowadzane od podstaw, a większość uczestników tak naprawdę nie wie, o czym dokładnie jest mowa.

ZAGROŻENIE 4. OSZUSTWO TYPU PHISHING

Polska Policja kilkunastokrotnie odnotowała już zgłoszenia ze strony instytucji, których urzędnicy zostali zręcznie zmanipulowani przez świetnie przygotowanych i poinformowanych oszustów. Głośnym echem odbiła się sprawa z lipca 2013 r., kiedy to oszust podszywający się pod firmę sprzątającą napisał do warszawskiego metra mail informujący o zmianie rachunku bankowego, na który miały być kierowane płatności za wykonane dla metra usługi. Księgowość metra dała się nabrać i w odpowiedzi na prośbę oszusta poprosiła jedynie o wysłanie wniosku w formie pisemnej. Oszust był dobrze przygotowany i przesłał do działu finansów metra tradycyjne pismo zawierające nowy rachunek bankowy dla dokonywania wpłat. Taka inżynieria społeczna zadziałała, nikt z księgowości metra nie zadzwonił do firmy sprzątającej celem weryfikacji całego procesu. W ten sposób w ręce oszusta wpadło 560 000 zł[17].

Do jeszcze bardziej spektakularnego oszustwa doszło w listopadzie 2018 r., gdy to przestępcy podszywający się pod amerykańskiego producenta samolotów, które latają w Polskich Liniach Lotniczych „LOT", przesłali przez Internet do księgowości firmy podrobioną fakturę. Faktura miała na celu wyłudzenie płatności rzekomo za kolejną ratę w ramach realizacji kontraktu. Tym razem na rachunek bankowy oszusta wpłynęło 2 600 000 zł[18].

Taki rodzaj przestępstw nazywany jest potocznie phishingiem, a same ataki przeprowadzane są najczęściej przy pomocy wiadomości e-mail lub SMS. Cyberprzestępcy w tym przypadku podszywają się m.in. pod firmy kurierskie, urzędy administracji, operatorów telekomunikacyjnych, instytucje czy też partnerów biznesowych. Zdecydowana większość phishingu ukierunkowana jest na osoby fizyczne, ale jeśli istnieją szanse zaatakowania z powodzeniem instytucji czy przedsiębiorstwa, to przestępcy na pewno taką próbę podejmą. W wypadku phishingu czynnik ludzki jest kluczowym obszarem jako najsłabsze ogniwo systemu, na który ukierunkowany jest atak[19].

ZAGROŻENIE 5. RANSOMWARE

Inny bardzo poważny obszar zagrożeń dla domeny instytucji publicznych stanowią ataki z grupy ransomware. Ransomware to termin powstały ze zbitki wyrazowej zaczerpniętej z języka angielskiego, łączącej ze sobą dwa terminy: *ransom* – oznaczający okup oraz *software* – tłumaczone jako oprogramowanie. Z punktu widzenia technicznego są to przestępcze działania, których skutkiem jest blokada oraz zaszyfrowanie plików danych znajdujących się na nośnikach danych. Z reguły osobom przeprowadzającym takie działania zależy na wyłudzeniu okupu, co ma być warunkiem przywrócenia stanu uprzedniego danych. Celem takich działań bywają także instytucje publiczne, od których oczywiście trudniej wymusić haracz, jednak perspektywa przedostania się informacji o ataku do mediów publicznych sprawia, że i one często podejmują negocjacje z przestępcami[20].

ZAGROŻENIE 6. ZŁOŚLIWY SPAM

Niestety, sposobów zaatakowania instytucji publicznych jest wiele. Do najpopularniejszych zaliczamy jednak rozsyłanie złośliwego spamu (tzw. malspam), czyli niepożądanych wiadomości służących do rozsyłania szkodliwego oprogramowania. Takie e-maile zawierają szczególnie niebezpieczne elementy w postaci zainfekowanych załączników (np. dokumenty PDF lub Word) lub linków do złośliwych stron. Użytkownik końcowy, wchodząc w zainfekowany link czy otwierając spreparowany załącznik, sam autoryzuje rozpoczęcie ataku na jego system[21].

POSTĘPOWANIE W PRZYPADKU CYBERATAKU

Gdy atak stanie się faktem, nie należy ulegać presji przestępców dążących do zapłaty okupu. Nie ma bowiem żadnej gwarancji, że wywiążą się z warunków postawionych w ramach szantażu, odblokowując dane, ani czy nie zostaną one przez nich wykorzystane do popełniania kolejnych przestępstw. Od strony technicznej zaraz po tym, jak ofiara zorientowała się, że stała się celem ataku, powinna postąpić wedle względnie prostego algorytmu, który przedstawiono poniżej.

ALGORYTM POSTĘPOWANIA w przypadku cyberataku typu ransomware

- **Po pierwsze**, należy odłączyć sprzęt komputerowy od Internetu przy jednoczesnym pozostawieniu włączonego urządzenia, gdyż pamięć urządzenia może zawierać istotne informacje, które będą bardzo pomocne do analizy ataku ransomware[22].
- **Po drugie**, obowiązkowo powinno się zabezpieczyć plik z notatką dot. zaszyfrowania i okupu (ransome note) oraz przykładowe zaszyfrowane pliki.
- **Po trzecie**, należy niezwłocznie skontaktować się z działem IT instytucji i poinformować o zaistniałej sytuacji. Informatycy instytucji powinni zabezpieczyć odpowiednio materiał dowodowy dla organów ścigania oraz podjąć kroki dotyczące zniwelowania skutków ataku. Warto w takim wypadku odwiedzić stronę portalu NoMoreRansom.org, na której być może znajdziemy antidotum w postaci deskryptora, który pozwoli na odszyfrowanie zaatakowanych danych[23]. Ważne jest także, by instytucja, która doświadczyła infekcji systemów, skontaktowała[24] się z CERT NASK[25].

ZAPOBIEGANIE CYBERATAKOM

Naturalnie lepiej jest nie dopuszczać do ataków, niż niwelować ich skutki. Tu jednak muszą ze sobą współdziałać pracownicy działu IT z użytkownikami końcowymi komputerów. Aby czuć się względnie bezpiecznie, pracownicy instytucji publicznych powinni przestrzegać kilku prostych zasad.

Zasady bezpieczeństwa

Po pierwsze – regularnie sporządzać kopię zapasową danych, które znajdują się na komputerach. Ważne jest to, by kopia zapasowa znajdowała się w trybie offline i nie była zagrożona atakiem przeprowadzonym z sieci.
Po drugie – standardem w dzisiejszych czasach jest wspieranie systemów operacyjnych dodatkowym oprogramowaniem antywirusowym.
Po trzecie – żadne oprogramowanie antywirusowe nie będzie działało poprawnie bez aktualizacji i odpowiedniej konfiguracji.
Aż wreszcie **po czwarte** – systematyczne szkolenia użytkowników końcowych pozwolą unikać ewidentnie podejrzanych załączników i linków.

[1] K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne*, Warszawa 2017, s. 8.
[2] Szacuje się, że okres postępowania w przypadku cyberprzestępstwa wynosi ok. 200 dni, a zaledwie w przypadku 1% z nich zostaje wniesiony akt oskarżenia.
[3] M. Castells, *Społeczeństwo sieci,* Wydawnictwo Naukowe PWN, Warszawa 2008, s. 23.
[4] T. Marciniuk, *Administracja i eksploatacja systemów komputerowych, urządzeń peryferyjnych i lokalnych sieci komputerowych. Podręcznik do nauki zawodu technik informatyk,* Wydawnictwa Szkolne i Pedagogiczne, Warszawa 2019, s. 14.
[5] Tamże, s. 22.
[6] Tamże, s. 23.
[7] Tamże, s. 124.
[8] Hasła – krótkiego, ale silnego i skomplikowanego.
[9] T. Marciniuk, *Administracja i eksploatacja systemów komputerowych, urządzeń peryferyjnych i lokalnych sieci komputerowych. Podręcznik do nauki zawodu technik informatyk,* s. 125.
[10] Tamże, s. 142.
[11] USB Killer – pendrive o właściwościach niszczących płytę główną komputera poprzez zaaplikowanie przez port USB skumulowanego ładunku elektrycznego.
[12] T. Marciniuk, *Administracja i eksploatacja systemów komputerowych, urządzeń peryferyjnych i lokalnych sieci komputerowych. Podręcznik do nauki zawodu technik informatyk*, s. 143.
[13] M. Serafin, *Sieci VPN. Zdalna praca i bezpieczeństwo danych*, Wydawnictwo Helion, Warszawa 2008, s. 18.
[14] Tamże, s. 48.
[15] Tamże, s. 49.
[16] Tamże, s. 152.
[17] Niebezpiecznik, *560 000 PLN wyłudzono od warszawskiego metra*, https://niebezpiecznik.pl/post/560-000-pln-wyludzono-od-warszawskiego-metra/ [dostęp: 27.05.2024 r.].
[18] Business Insider Polska, *Złodzieje oszukali LOT. Linie straciły prawie 2 mln zł, https://businessinsider.com.pl/finanse/lot-oszukany-na-2-mln-zl-przelew-na-zle-konto/c6yghss* [dostęp: 27.05.2024 r.].
[19] J. Jancelewicz, *Socjotechnika, phishing i analiza zdarzeń,* Wydawnictwo Helion, Warszawa 2022, s. 32.
[20] M. Gliwiński, *Ataki na strony internetowe*, Wydawnictwo CSH, Warszawa 2008, s. 18.
[21] Tamże, s. 47.
[22] Tamże, s. 51.
[23] Tamże, s. 55.
[24] NASK, *Kim jesteśmy?*, https://www.nask.pl/? [dostęp: 27.05.2024 r.].
[25] CERT Polska – zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet.

Bibliografia

Business Insider Polska, *Złodzieje oszukali LOT. Linie straciły prawie 2 mln zł, https://businessinsider.com.pl/finanse/lot-oszukany-na-2-mln-zl-przelew-na-zle-konto/c6yghss* [dostęp: 27.05.2024 r.].
Castells M., *Społeczeństwo sieci,* Wydawnictwo Naukowe PWN, Warszawa 2008.
Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo – zagadnienia definicyjne*, Warszawa 2017.
Jancelewicz J., *Socjotechnika, phishing i analiza zdarzeń*, Wydawnictwo Helion, Warszawa 2022.
Marciniuk T., *Administracja i eksploatacja systemów komputerowych, urządzeń peryferyjnych i lokalnych sieci komputerowych. Podręcznik do nauki zawodu technik informatyk*, Wydawnictwa Szkolne i Pedagogiczne, Warszawa 2019.
NASK, *Kim jesteśmy?*, https://www.nask.pl/? [dostęp: 27.05.2024 r.].
Niebezpiecznik, *560 000 PLN wyłudzono od warszawskiego metra*, https://niebezpiecznik.pl/post/560-000-pln-wyludzono-od-warszawskiego-metra/ [dostęp: 27.05.2024 r.].
Serafin M., *Sieci VPN. Zdalna praca i bezpieczeństwo danych*, Wydawnictwo Helion, Warszawa 2008.

Summary

Cybersecurity in public institutions. Threats and ways to protect

This article defines the term ”cybersecurity” as well as presents the most popular threats in this area to which public institutions are currently exposed. Moreover, ways of dealing with selected cyberattacks and methods of preventing threats to the information systems used by these institutions, are described. It was pointed out that the weakest link in the area of cybersecurity is invariably the end user, i.e. the human being. Thus, the huge role of continual user training was stressed.

Tłumaczenie: Katarzyna Olbryś

Zagrożenia w Policji wynikające z uruchomienia niezidentyfikowanych plików

MALWARE

kom. Sławomir Sobolewski
Wydział Ochrony Systemów Informatycznych
Biuro Łączności i Informatyki
Komenda Główna Policji

podkom. Kamil Jurczyk
Wydział Ochrony Systemów Informatycznych
Biuro Łączności i Informatyki
Komenda Główna Policji

Współczesny policjant, niezależnie od rodzaju wykonywanych zadań, korzysta na co dzień z systemów teleinformatycznych Policji. Niniejszy artykuł ma na celu zwrócenie uwagi na kilka kluczowych elementów przekładających się na bezpieczeństwo użytkowników policyjnych sieci teleinformatycznych.

Policja jako jedna z formacji podlegających MSWiA realizuje swoje zadania na podstawie ustawy o Policji[1]. Codzienna służba policjantów jest trudna oraz wymaga ogromnego poświęcenia w różnych aspektach. Do tych aspektów możemy zaliczyć specyfikę zadań realizowanych przez funkcjonariuszy prewencji, ruchu drogowego, kryminalnych, walczących z przestępczością gospodarczą, techniki operacyjnej, szkół Policji oraz pozostałych. Mocno zróżnicowane zadania przekładają się na wysoki poziom podziału kompetencji pomiędzy funkcjonariuszami. Służba polegająca na patrolach pieszych i zmotoryzowanych, udziale w zabezpieczeniach, prowadzeniu dochodzeń w sprawach przestępstw i wykroczeń czy analizie danych zebranych przy użyciu sprzętu technicznego wymaga w obecnych czasach dostępu do systemów teleinformatycznych Policji. Najważniejsze systemy przetwarzające dane przechowywane są w ramach redundantnych ośrodków przetwarzania danych, obsługiwanych przez Biuro Łączności i Informatyki Komendy Głównej Policji. Celem istnienia Biura jest m.in. wspomaganie funkcjonowania oraz cyfryzacja określonych obszarów znajdujących się w naszej formacji. Same działania są ukierunkowane na daleko idące usprawnienia oraz innowacje technologiczne. Zdecydowana większość zadań Biura Łączności i Informatyki KGP odbywa się poza zasięgiem poszczególnych jednostek, a proces udostępniania usług jest w pełni przezroczysty dla ich odbiorców.

W zależności od rodzaju realizowanych zadań do podstawowych policyjnych sieci zalicza się Policyjną Sieć Transmisji Danych (PSTD) oraz Centralny Węzeł Internetu (CWI). Każda z wymienionych sieci posiada swoje zastosowanie. Zależy to od rodzaju przetwarzanych danych oraz udostępnianych narzędzi, które są wykorzystywane w służbie. Do głównych różnic należy zaliczyć stopień otwartości na publiczną sieć Internet. Sieć PSTD jest z założenia zamknięta, co sprawia, że przetwarzanie danych odbywa się bez dostępu do sieci Internet. Techniczne uwarunkowania mają za zadanie zminimalizować możliwe próby przeprowadzenia bezpośredniego, bezprawnego ataku na urządzenia, systemy, aplikacje oraz dane znajdujące się wewnątrz naszej formacji. Do tych danych należy zaliczyć przede wszystkim dane osobowe, szczegóły dotyczące prowadzonych śledztw, wykroczeń drogowych, dokumenty służbowe i wiele innych. Ponadto prowadzona jest wymiana danych z innymi służbami krajowymi (np. Strażą Graniczną), w tym służbami specjalnymi oraz międzynarodowymi, jak np. Europol i Interpol. Sieć PSTD zawiera wiele systemów i aplikacji, które są krytyczne dla sprawnego funkcjonowania naszej formacji,

jak np. KSIP, SWD, SWOP itp. Z drugiej strony – część istotnych informacji możliwa jest do uzyskania wyłącznie z sieci Internet. Dlatego też obecnie rolę „pośrednika" pełni sieć CWI. Z uwagi na skalę działań oraz wagę przetwarzanych informacji zdecydowano o wykorzystywaniu niezależnych i oddzielnych stanowisk komputerowych dla każdej z tych sieci.

Podstawową i najważniejszą siecią policyjną jest zamknięta sieć PSTD, która daje możliwość między innymi sprawdzenia w trakcie legitymowania (za pośrednictwem stacji komputerowych oraz mobilnych terminali noszonych), czy wprowadzone dane należą do osoby poszukiwanej. Możliwość uzyskania nieautoryzowanego dostępu do centralnych zasobów sieci PSTD mogłaby prowadzić do odczytu, modyfikacji lub usunięcia informacji decydujących o postępowaniu lub śledztwie. Są to kluczowe informacje z punktu widzenia nie tylko Policji, ale również całego państwa. Dlatego też kwestie bezpieczeństwa, a dokładniej mówiąc cyberbezpieczeństwa, wewnątrz naszej formacji stanowią ważny element, który ma wpływ na bezpieczne i dobre funkcjonowanie państwa prawa.

Komórką kształtującą oraz odgrywającą wiodącą rolę związaną z szeroko rozumianym cyberbezpieczeństwem w sieci PSTD jest Wydział Ochrony Systemów Informatycznych, znajdujący się w Biurze Łączności i Informatyki Komendy Głównej Policji. Wydział ten odpowiada między innymi za dostęp do centralnych zasobów, autoryzację użytkowników oraz bezpieczne przetwarzanie danych, z wykorzystaniem najnowszych technologii (w tym projektowanie infrastruktury teleinformatycznej). Istotnym elementem zabezpieczania połączenia jest zestawianie tuneli kryptograficznych i wymiana danych z innymi podmiotami odgrywającymi ważne role w strukturach państwa. Jednocześnie należy zauważyć, że niezależnie od prowadzonych działań inżynieryjnych, rozwiązań technologicznych oraz kampanii informacyjnych, również użytkownik jest odpowiedzialny za bezpieczeństwo danych, z których korzysta. Poniżej zostaną omówione podstawowe, stosowane przez cyberprzestępców oraz twórców szkodliwego oprogramowania, techniki ataku na stacje końcowe.

Jedną z podstawowych technik wykorzystywanych przez cyberprzestępców wobec użytkowników każdej sieci jest użycie szkodliwego oprogramowania (malware) do przeprowadzania infekcji na stacjach końcowych (należących do ich użytkowników). Jest to zazwyczaj pierwszy krok i nazywany jest „kampanią malware". Kampanie mają swoje cele i kierunki ataków, np. państwa, regiony, konkretne firmy lub instytucje. Głównym celem kampanii jest uruchomienie w systemie operacyjnym szkodliwego pliku i umożliwienie infekcji, która może prowadzić do np. eskalacji uprawnień, szyfrowania danych lub wykorzystania systemu jako botnet. Cyberprzestępcy wykorzystują wiele technik, aby nakłonić użytkownika do uruchomienia pliku na jego komputerze.

Pierwsza z omawianych technik polega na ukryciu pliku wykonywalnego .exe (ang. *executable*) w innym rozszerzeniu, co może minimalizować czujność użytkownika, np. fotografia .jpg (ang. *Joint Photographic Experts Group*) zamiast fotografia.exe. Technika ta jest prosta w wykonaniu i może dotyczyć również innych rozszerzeń (doc, pdf, xml itp.). Analiza wymaga podstawowego wglądu w strukturę binarną samego pliku.

Zrzut ekranu znajdujący się poniżej (rys. 1) przedstawia jeden i ten sam plik malware pod nazwą „Hydra" zawierający szkodliwe oprogramowanie, zapisany w dwóch różnych formatach .exe oraz .jpg. Pomimo iż sam system operacyjny wyświetla każdy z tych plików z innym rozszerzeniem, to podstawowa analiza wskazuje, że mamy do czynienia z programem graficznym (GUI) przygotowanym na platformę MS Windows w formacie PE32 (ang. *Portable Executable*).

Dodatkowo, pewność w ręcznej analizie co do faktycznego rozszerzenia dają nam tak zwane ang. *magic number* znajdujące się wewnątrz pliku. To za ich sprawą system interpretuje zachowanie pliku i podejmuje decyzję, jakie narzędzie będzie w stanie go obsłużyć (np. plik muzyczny = Windows Media Player). Dla każdego pliku wykonywalnego „magicznymi numerami" będą *4D 5A*, które w łańcuchach znaków posiadają oznaczenie *MZ*.

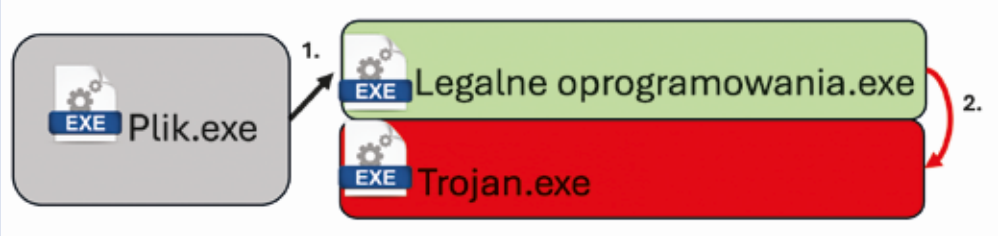
Kolejnym elementem jest sama informacja *This program cannot be run in DOS mode*, która oznacza brak możliwości uruchomienia pliku w trybie DOS. Jest to element pozostałości z przeszłości. Nagłówek *MZ* został zachowany dla zgodności wstecznej, co pozwala starszym systemom DOS rozpoznać plik jako wykonywalny.

Kolejną próbą ukrycia malware może być technika wykorzystywana w tzw. trojanach, czyli plikach udających prawdziwe, „legalne" oprogramowanie. Pliki te charakteryzują się zazwyczaj dwutorowym działaniem. Jedną ze ścieżek może być faktyczne uruchomienie np. instalatora programu ALLPlayer.exe, jednocześnie drugą ścieżką

Ryc. 1. Porównanie pliku wykonywalnego .exe ze sfabrykowanym plikiem .jpg.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Tekst zdekodowany
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	,.....@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	.....
00000030	00	00	00	00	00	00	00	00	00	00	00	00	C8	00	00	00	.....È...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°..´.Í!¸.LÍ!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....$.....
00000080	AD	31	38	81	E9	50	56	D2	E9	50	56	D2	E9	50	56	D2	.18.éPVÒéPVÒéPVÒ
00000090	2A	5F	09	D2	EB	50	56	D2	E9	50	57	D2	4D	50	56	D2	*_.ÒëPVÒéPWÒMPVÒ

Ryc. 2. „Magiczne numery” pliku wykonywalnego.



Ryc. 3. Jeden z wariantów uruchomienia zainfekowanego pliku trojan.

może być uruchomienie kawałka szkodliwego kodu wymierzonego w użytkowników i ich systemy.
Cała procedura zapewnia pełne ukrycie obecności oraz działania szkodliwego oprogramowania. Skutkiem takiej infekcji może być uzyskanie dostępu do danych, przejęcie kontroli nad systemem operacyjnym, zakłócenie działania systemu (spowolnienie, błędy, awarie) oraz wiele innych. W trakcie niskopoziomowej analizy można zwrócić uwagę na elementy związane z tworzeniem nowych procesów w systemie operacyjnym, uruchomianiem innych programów, otwieraniem plików lub nazw URL. Jednym z działań może być zapisywanie danych w przestrzeni adresowej innego procesu, co często zdarza się we „wstrzykiwaniu” złośliwego kodu. Ponadto wykorzystuje się tzw. instalacje haków (ang. *hooks*) za sprawą funkcji *SetWindowsHookEx* do przechwytywania i monitorowania wiadomości pochodzących z systemu operacyjnego.
W celu zapewnienia ciągłości działania szkodliwego oprogramowania w systemie operacyjnym po jego kontrolowanym lub niekontrolowanym zamknięciu stosuje się specjalne modyfikacje systemu. Zazwyczaj odpowiada za to właściwy wpis w rejestrze systemu Windows. Modyfikacja odbywa się za sprawą otwarcia klucza rejestru (*RegOpenKeyEx*) z uprawnieniami do zapisu (*KEY_WRITE*). Proces konfiguracji rejestru (*RegSetValueEx*) polega na wykorzystaniu nazwy oraz ścieżki do złośliwego kodu malware (MyTrojan). Działanie to zapewnia automatyczne uruchamianie przy każdym starcie systemu Windows szkodliwego oprogramowania (zapewniając trwałość i unikanie wykrycia).
Odpowiedzią na pytanie, dlaczego użytkownik zazwyczaj nie widzi wszystkich modyfikacji w swoim systemie, jak np. uruchomionego Wiersza Polecenia lub PowerShell, jest fakt wykorzystania kolejnej techniki ukrywania. Za pomocą dodatkowych modyfikacji w funkcji wShowWindow *(=SW_HIDE)* oraz nShow *(=SW_HIDE)* użytkownikowi nie „wyskakują” okienka na poziomie GUI (wszystko wykonuje się w tle).
W celu zobrazowania potencjalnych działań pliku malware na stacji użytkownika w środowisku laboratoryjnym przygotowano próbkę testową (bez funkcji ukrywania) symulującą szkodliwe oprogramowanie. Utworzony program posiada podstawowe funkcjonalności inwigilujące (keylogger).
Po uruchomieniu pliku użytkownik w pierwszej kolejności otrzymuje widok okna realizującego wyświetlenie pliku ustawa.pdf (to, czego użytkownik oczekiwał). Następnie uruchamiany jest kolejny moduł (to, czego użytkownik nie oczekuje) wyświetlający informacje o systemie i zalogowanym użytkowniku oraz sprawdzane jest połączenie z siecią Internet. To właśnie za sprawą dostępu do sieci Internet pobierane są kolejne wersje szkodliwego oprogramowania (i aktualizowane jego

```
void InstallTrojan() {
    char szPath[MAX_PATH];
    GetModuleFileName(NULL, szPath, MAX_PATH);
    HKEY hKey;
    RegOpenKeyEx(HKEY_CURRENT_USER, "Software\\Microsoft\\Windows\\CurrentVersion\\Run", 0, KEY_WRITE, &hKey);
    RegSetValueEx(hKey, "MyTrojan", 0, REG_SZ, (const BYTE*)szPath, strlen(szPath) + 1);
    RegCloseKey(hKey);
```

Ryc. 4. Pseudokod odpowiadający za wprowadzenie zmian w rejestrze systemu Windows.

Ryc. 5. Uruchomiony keylogger w systemie bez funkcji ukrywania.

funkcjonalności) lub przesyłane są dane zainfekowanej stacji użytkownika na serwer cyberprzestępcy. Przy wykorzystaniu luki w oprogramowaniu możliwe jest dostosowanie ustawień zapory systemu (wyłączenie zapory). Nasza próbka zawiera wyłącznie funkcję sprawdzenia, czy wszystkie elementy zapory są obecnie aktywne. Kolejnym etapem działania jest uruchomienie przeglądarki internetowej i wyświetlenie informacji o zainfekowaniu. Zazwyczaj informacja o zainfekowaniu jest starannie ukrywana przed użytkownikiem. Ostatnim z etapów jest uruchomienie modułu keyloggera, który zbiera i zapisuje do pliku *.txt aktywność użytkownika systemu Windows. Te informacje łatwo mogą zostać przesłane do dowolnego miejsca na świecie.

Podsumowanie

Każdy z użytkowników ma wpływ, pośrednio i bezpośrednio, na bezpieczeństwo danych w policyjnych sieciach teleinformatycznych. Zaleca się, aby stacje robocze były wykorzystywane zgodnie z ich przeznaczeniem i polityką bezpieczeństwa. Odradza się pobierania i instalacji oprogramowania z niezidentyfikowanych źródeł. Zaleca się ostrożność w otwieraniu załączników lub linków od nieznajomych nadawców. Wymaga się, aby każda ze stacji służbowych miała uruchomioną zaporę systemową i zainstalowany policyjny system antywirusowy. Ponadto skonfigurowane do pracy stacje robocze nie mogą być celowo modyfikowane w nieuprawniony sposób do własnych celów użytkownika (własna reinstalacja lub konfiguracja systemu). Zabrania się przepinania stacji roboczych lub innych urządzeń służbowych pomiędzy siecią PSTD i CWI.
Pamiętajmy, że cyberbezpieczeństwo formacji to również nasze bezpieczeństwo. Wszyscy jesteśmy za nie odpowiedzialni.

[1] Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2024 r. poz. 145).

Bibliografia:

Fortinet, *What Is A Keylogger? Definition and Types*, https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers [dostęp: 17 czerwca 2024 r.].
McGowan E., *Trojan viruses: Detecting and removing*, https://us.norton.com/blog/malware/what-is-a-trojan [dostęp: 17 czerwca 2024 r.].
Microsoft, *RegOpenKeyExA function (winreg.h)*, https://learn.microsoft.com/en-us/windows/win32/api/winreg/nf-winreg-regopenkeyexa [dostęp: 17 czerwca 2024 r.].
Microsoft, *SetWindowsHookExA function (winuser.h)*, https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-setwindowshookexa [dostęp: 17 czerwca 2024 r.].
Microsoft, *ShowWindow function (winuser.h)*, https://learn.microsoft.com/en-us/windows/win32/api/winuser/nf-winuser-showwindow [dostęp: 17 czerwca 2024 r.].
Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2024 r. poz. 145).
Wikipedia, *DOS MZ executable*, https://en.wikipedia.org/wiki/DOS_MZ_executable [dostęp: 17 czerwca 2024 r.].

Summary

Threats in the Police resulting from running unidentified files (malware)

The Polish Police performs almost all of its tasks based on ICT systems, which are located in an internal network structure called the Police Data Transmission Network (Policyjna Sieć Transmisji Danych). Personal data and other information must be well guarded by both hardware, software and the human factor, which can be provided in this case through the education process. This article will describe the basic techniques that enable cyber criminals to get a user to run malware. The goal is to raise awareness among police officers and employees about cyber security threats caused by social engineering and other factors.

Tłumaczenie: autorzy

Co robimy źle, a moglibyśmy robić lepiej

W OCHRONIE DZIECI PRZED ZAGROŻENIAMI W SIECI

Fot. https://pl.freepik.com

Anna Rywczyńska

Kierowniczka Działu Profilaktyki Cyberzagrożeń,
Koordynatorka Polskiego Centrum Programu Safer Internet,
NASK Państwowy Instytut Badawczy

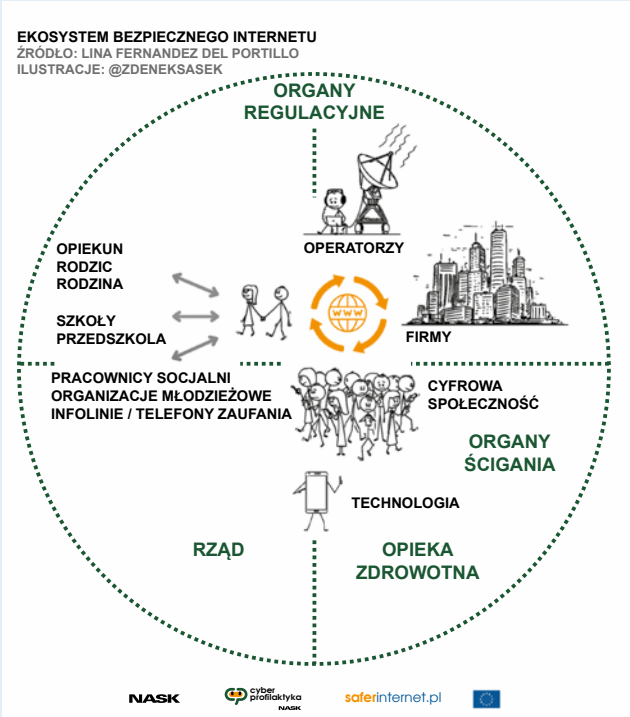
Celem artykułu jest omówienie licznych wyzwań i błędów dotyczących ochrony dzieci i młodzieży przed zagrożeniami w sieci oraz wskazanie, co możemy poprawić. Wiele dzieci napotyka różne niebezpieczeństwa online, w tym cyberprzemoc, narażenie na nieodpowiednie treści oraz ryzykowne kontakty z obcymi. Czas poświęcany w szkołach na edukację w zakresie bezpieczeństwa w internecie jest niewystarczający, należy wprowadzić bardziej zintegrowane podejście, które uwzględnia przenikanie się doświadczeń online i offline.

WSTĘP

Dorośli mają tendencję do szybkiej oceny i skupiania się na skutkach, a nie przyczynach problematycznego korzystania z internetu przez najmłodszych użytkowników. Kluczowe znaczenie ma zrozumienie różnorodnych przyczyn długiego czasu spędzanego przed ekranem przez dzieci, takich jak problemy emocjonalne, brak zainteresowań czy presja rówieśników, i nawoływanie do rozwiązania tych podstawowych problemów. Ponadto niezmiernie istotne jest rozwijanie umiejętności korzystania z mediów i krytycznego myślenia u dzieci. Ze względu na postęp technologiczny stworzenie bardziej bezpiecznego środowiska online wymaga szerszej i głębszej współpracy pomiędzy rodzicami, nauczycielami i firmami technologicznymi.

BEZPIECZEŃSTWO W SIECI W STATYSTYCZNEJ KLASIE

Wchodząc do klasy, z którą mamy porozmawiać o bezpieczeństwie w sieci, najprawdopodobniej spotkamy się nie z jednym problemem związanym z wykorzystywaniem internetu, ale z wieloma. Statystycznie w 25-osobowej klasie nastolatków[1]: 12 osób spotkało się w internecie z sytuacjami, kiedy ich znajomi byli atakowani i wyzywani (44,6%), 4 osoby spotkały się z osobą dorosłą poznaną w sieci (17%), 7 osób otrzymało od kogoś nagie zdjęcia (32,7%), 7 osób próbowało, bez skutku, ograniczyć czas spędzany w mediach społecznościowych, ponad połowa mierzy się z poczuciem osamotnienia, 31% wzięło udział w wyzwaniu internetowym, które mogło negatywnie wpłynąć na ich zdrowie, 6 osób obejrzało tzw. patostre-



Ryc. 1. Ekosystem bezpiecznego internetu. Autor: A. Ficak, za Lina Fernandez del Portillo.

amy (wulgarne, obsceniczne i nacechowane), z czego 3 nie zdawały sobie sprawy z tego, co oglądają, i że są to treści nieodpowiednie. Aż 17 osób boi się internetowego hejtu. Większość osób siedzących w ławkach spędza przed ekranem swojego telefonu ponad 5 i pół godziny na dobę, a 2 osoby w tej klasie ponad 12 godzin.

BŁĄD PIERWSZY

Czas, który dzisiaj szkoły, nauczyciele mogą poświęcić na spotkania profilaktyczne w obszarze bezpieczeństwa w sieci, jest dużo za krótki, zwłaszcza jeśli weźmiemy pod uwagę, jak złożoną kwestią jest obecność dzieci i młodzieży w internecie. Jednym z „grzechów" świata dorosłych jest to, że chcemy te światy: internetowy i poza siecią rozdzielać grubą kreską, nie widząc, jak bardzo się przenikają. Chcemy oddzielnie mówić o przemocy w sieci, a oddzielnie o agresji na szkolnych korytarzach czy podwórkach, oddzielnie mówić o dobrostanie psychicznym, o budowaniu w dzieciach poczucia własnej wartości, o przeciwdziałaniu uzależnieniom i ryzykownym zachowaniom, tymczasem każde spotkanie z młodymi ludźmi może być dla nas próbą zrozumienia złożoności ich dzisiejszej rzeczywistości, nakładających się na siebie procesów społecznych, relacji rówieśniczych, w których dostęp do internetu jest jednym ze składników, a nie zawsze źródłem kryzysów.

BŁĄD DRUGI

Kolejny „grzech" osób zajmujących się profilaktyką to zbyt szybko wyciągane wnioski, brak uważności i wnikliwego przyjrzenia się problemowi. Często skupiamy się na skutkach problemów dziecka, a nie na ich przyczynie. Jednym z dobrych przykładów jest kwestia czasu, jaki dzieci spędzają przed ekranami. Problematyczne używanie internetu może mieć różne powody. Dzieci mogą szukać w internecie ucieczki przed problemami emocjonalnymi lub konfliktami. Internet może stanowić formę odskoczni, gdzie mogą zapomnieć o codziennych trudnościach i negatywnych emocjach. Dla innych dzieci będzie miejscem, w którym mogą znaleźć akceptację, zwłaszcza dla tych, które mają niskie poczucie własnej wartości i „polubienia" – pozytywne komentarze w sieci sprawiają, że czują się szczęśliwsze. W przypadku braku bliskich relacji w najbliższym otoczeniu to wirtualne społeczności mogą być miejscem, gdzie dziecko będzie szukało poczucia przynależności i wsparcia, którego może mu brakować w życiu codziennym. Internet może być dla dzieci miejscem, w którym czują się komfortowo, mogą być sobą i znaleźć ludzi, którzy je rozumieją. Bardzo często nadużywanie internetu jest spowodowane brakiem innych zainteresowań, brak pasji lub hobby może skłaniać je do długotrwałego przesiadywania w sieci.

Bardzo ważnym czynnikiem kształtującym zachowania dzieci, również te związane z mediami cyfrowymi, jest presja ze strony rówieśników – czują, że aby nadążyć za rówieśnikami, być na bieżąco z trendami, muszą spędzać jak najwięcej czasu w sieci. Prowadzi to do zjawiska FOMO (ang. *fear of missing out*), czyli strachu, który nastolatkowie zaczynają odczuwać, kiedy nie mogą być online, przed tym, że coś stracą, jakaś informacja ich ominie i zostaną przez to społecznie wykluczeni. Ekran to też często uspokajacz. Dzieci, które nie nauczyły się skutecznie radzić sobie z emocjami, często przez to, że ich rodzice stosowali ekran jako regulator ich trosk i zmartwień, mogą uciekać się do internetu jako formy samoregulacji. Korzystanie z internetu może być dla nich sposobem na kontrolowanie napięć czy stresu.

Nawet z tej krótkiej wyliczanki możliwych powodów, dla których dzieci zamykają się na świat zewnętrzny, widać, że kluczowa jest determinacja w dotarciu do tych powodów i – w zależności od wyciągniętych wniosków – dalsze działanie. Praca w tym obszarze zawsze będzie wymagała, czy to od nauczyciela, pedagoga, czy też funkcjonariusza Policji, odpowiednich kompetencji miękkich, takich jak empatia, cierpliwość oraz umiejętność komunikacji. Trzeba być w stanie zbudować zaufanie oraz okazać wsparcie dla ofiar, jednocześnie zachowując profesjonalizm i etykę. Pamiętajmy, że nasze wnioski mogą też okazać się pozytywne, możemy dowiedzieć się, że dziecko swój czas przy technologii cyfrowej spędza efektywnie, kreatywnie, że jest to jego pasja, a wtedy nasze działanie musi być inne – ułatwiające rozwój w obszarze technologii informacyjno-teleinformatycznych (ang. *ICT – Information and Communication Technologies*), a jednocześnie nacechowane troską o zdrowie fizyczne i emocjonalne – bo zawsze, niezależnie od przyczyny, długotrwałe korzystanie z internetu może mieć wiele negatywnych konsekwencji.

Problematykę nadużywania ekranów przez młodych ludzi konsultowaliśmy z przedstawicielami działającego przy Państwowym Instytucie Badawczym NASK Młodzieżowego Panelu Doradczego „Cyfrowa Przyszłość Ucznia" i to, co młodzi ludzie podkreślali, to potrzeba rozwijania w nich motywacji do tego, aby pracowali nad zdrowym bilansem aktywności, motywacji do tego, aby

szukać rozrywki, relacji oraz rozwiązywania swoich problemów poza siecią. W przypadkach, kiedy wydłużony czas w sieci wynika z innych, wskazanych powyżej problemów, naszym priorytetem powinno być nie ograniczanie czasu w sieci, ale pomoc w radzeniu sobie z tymi sytuacjami, przed którymi do sieci uciekają. Włączmy w rozwiązywanie takiego problemu całe środowisko wokół dziecka – rodziców, nauczycieli, pedagoga szkolnego, jeśli jednak dziecko boi się bądź nie jest gotowe na mówienie o swoich problemach w swoim bliskim otoczeniu – przekazujmy numer telefonu zaufania dla dzieci i młodzieży (116 111), gdzie pracujący konsultanci mogą stanowić bezpieczną przestrzeń, w której dziecko może otworzyć się ze swoimi trudnościami.

BŁĄD TRZECI

Kolejnym błędem ze strony dorosłych jest stawianie granic w odniesieniu do naszych odpowiedzialności i ról. Chcielibyśmy pokroić jak tort przestrzenie, w których znajdują się dzieci, i ustalić, jak dawniej było można, że to, co dzieje się w szkole, to odpowiedzialność szkoły, a to, co w domu, to rodziców i opiekunów, a jeszcze treści i usługi, z których dzieci korzystają, to odpowiedzialność firm etc. Aktywności w sieci niestety nie da się tak podzielić – żeby dzieci były bezpieczne, potrzebna jest współpraca. Nic nie dadzą najlepsze zabezpieczenia przed szkodliwymi treściami czy wdrażane metody weryfikacji wieku, jeśli rodzic nie będzie rozumiał, że portale społecznościowe naprawdę nie powinny być dostępne dla dziecka poniżej 13. roku życia, że oznaczenia wiekowe gier i aplikacji mają swoje uzasadnienie i instalowanie ich wbrew rekomendacjom producentów może być dla ich dzieci niebezpieczne. Cóż da nam licytowanie się, kto pierwszy ma reagować, w przypadku np. incydentu cyberprzemocy w grupie klasowej na aplikacji WhatsApp? Zarówno nauczyciele, jak i rodzice muszą podjąć działania jak najszybciej. Wsparcie dla ofiary oraz podjęcie działań wobec sprawców powinny być priorytetem dla wszystkich. Dzisiaj wielkim wyzwaniem jest fakt, że dzieci i młodzież mają tak mało zaufania do dorosłych, że będziemy w stanie mądrze i szybko pomóc, że bardzo często (38,5%) nie mówią nikomu o tym, że doświadczyły przemocy. Kiedy pytamy dlaczego, odpowiadają, że boją się, że po ingerencji dorosłych „będzie jeszcze gorzej", że lepiej „przeczekać, aż samo minie", że „rodzice zabiorą im telefon".

WYZWANIA W DZIEDZINIE CYBERBEZPIECZEŃSTWA DZIECI

Branża informatyczna, szczególnie wielkie platformy internetowe, stoją dzisiaj przed wielkim wyzwaniem, które może zmienić aktualną sytuację bezpieczeństwa dzieci online. Akt o usługach cyfrowych ma celu m.in. poprawę bezpieczeństwa dzieci w internecie i walkę z zagrożeniami, które pojawiły wraz z rozwojem wielkich serwisów internetowych, takimi jak: brak odpowiedniej ochrony danych osobowych, nadmierna ekspozycja na nieodpowiednie treści (algorytmy często promujące treści kontrowersyjne, szokujące lub nieodpowiednie, co może narażać dzieci na szkodliwe treści, w tym pornografię, przemoc czy treści o charakterze ekstremistycznym), niedostateczne narzędzia do ochrony przed cyberprzemocą, brak odpowiednich narzędzi do zgłaszania i usuwania treści lub zachowań zagrażających dzieciom, brak wystarczających opcji kontroli rodzicielskiej, co utrudnia rodzicom monitorowanie i zarządzanie aktywnością swoich dzieci w internecie, czy też kwestia rozwijania produktów projektowanych w taki sposób, aby maksymalnie zwiększyć zaangażowanie użytkowników.

Ryc. 2. Statystyczne problemy w 25-osobowej klasie nastolatków. Autor: A. Ficak.

Wielkim wyzwaniem jest promowanie korzyści dla dzieci wynikających z technologii cyfrowej, budowanie cyfrowego obywatelstwa, przy jednoczesnej trosce o bezpieczeństwo. Wszyscy interesariusze muszą znaleźć równowagę między rewolucją cyfrową a priorytetem ochrony bezpieczeństwa najmłodszych. Dostęp choćby do globalnej sieci informacji to niezaprzeczalny atut współczesnego społeczeństwa. Jednakże, jak każda moc, wymaga ona odpowiedzialnego i świadomego użytkowania. Pomimo bogactwa wiedzy dostępnej w internecie, bez właściwej edukacji medialnej i umiejętności krytycznego myślenia, stajemy w obliczu ryzyka wprowadzenia w błąd czy manipulacji przez fałszywe lub tendencyjne informacje. Edukacja medialna staje się kluczowym elementem w budowaniu społeczeństwa, które potrafi skutecznie wykorzystać potencjał dostępnych zasobów internetowych. Brak odpowiednich umiejętności weryfikacji informacji może prowadzić do przypadkowego lub celowego rozpowszechniania dezinformacji. Fałszywe informacje mogą wywoływać panikę, wprowadzać w błąd, a nawet destabilizować społeczeństwo. Wydaje się, że dzisiaj zbyt często chcemy mówić o edukacji medialnej w oderwaniu od innych procesów edukacyjnych, a przecież nauka odpowiedniego zarządzania informacją, nauka weryfikacji treści mogłaby być częścią większości zajęć przedmiotowych.

Ogromny błąd dorosłych to narażanie dzieci i nastolatków na niebezpieczne kontakty – zbyt wczesne wpuszczenie dzieci w świat mediów społecznościowych nie tylko źle wpłynie na ich dobrostan psychiczny, każąc im się porównywać z sieciowymi celebrytami, ale też naraża je na ryzyko kontaktu z przestępcami seksualnymi, którzy różnymi technikami, również poprzez oswajanie młodych osób z treściami o charakterze pornograficznym, będą chcieli pozyskać zdjęcia czy filmy intymne.

W NASK od 20 lat działa zespół Dyżurnet, który reaguje na zgłoszenia dotyczące materiałów przedstawiających wykorzystywanie seksualne dziecka. Od dłuższego czasu zespół ten alarmuje, że rozwija się zjawisko produkowania własnoręcznie, lecz nie z własnej woli, tego rodzaju materiałów przez młode osoby, które później często stają się ofiarami szantażu na tle seksualnym. W ostatnim czasie przestępstwa te dodatkowo się nasilają na skutek zjawiska DeepNudes. Wykorzystując zaawansowane algorytmy sztucznej inteligencji, aplikacje pozwalają na generowanie autentycznie wyglądających obrazów nagich postaci na podstawie zwykłych zdjęć. DeepNudes tworzy obrazy o bardzo wysokiej jakości, które trudno odróżnić od prawdziwych zdjęć. Dzięki prostocie użycia i dostępności aplikacji osoby zainteresowane tworzeniem fałszywych obrazów pornograficznych mogą szybko i łatwo generować tego typu treści. To prowadzi do zwiększenia dostępności i rozpowszechniania fałszywych obrazów pornograficznych z udziałem dzieci, które mogą być wykorzystywane przez przestępców do szantażu oraz nękania i eksploatacji dzieci.

PODSUMOWANIE

Nie ma pojedynczego rozwiązania, które mogłoby zmniejszyć ryzyka, na które dzieci są narażone podczas korzystania z internetu. Musi być wdrożone wieloaspektowe podejście, aby skutecznie radzić sobie z szerokim spektrum zagrożeń. Takie podejście łączy w sobie zarówno kwestie regulacji prawnych, samoregulacji, jak i w szczególności powszechną edukację. Nie uciekniemy od swoich ról i obowiązków – nie może nas od tego zwolnić brak biegłości w obsłudze sieci. Dzisiaj bezpieczeństwo w sieci to nie tylko technologia, ale przede wszystkim niezbędne kompetencje społeczne. Rodzice i edukatorzy mają obowiązek prowadzić i wspierać młodych ludzi, być nie tylko „stróżami czasu", ale przede wszystkim przewodnikami po tym, co w sieci dobre. Międzynarodowe organizacje, rządy i przemysł mają obowiązek zapewnienia, że środowisko online jest zabezpieczone. Ogromnie ważna jest również rola funkcjonariuszy prewencji, którzy bardzo często prowadzą kampanie edukacyjne i warsztaty dla rodziców, nauczycieli i dzieci na temat bezpieczeństwa online, identyfikują zagrożenia internetowe i przedstawiają sposoby ochrony przed nimi, monitorują aktywność w sieci, w tym działania przestępcze, i mogą podejmować skuteczne działania w celu ochrony dzieci.

[1] *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców*, red. R. Lange, Warszawa 2023, Państwowy Instytut Badawczy NASK, file:///C:/Users/951104/Downloads/Thinkstat_RAPORT_nastolatki-3_0_ONLINE.pdf [dostęp: 17.05.2024 r.].

Bibliografia:

NASK, *Co robią nasze dzieci w sieci, czyli Raport z najnowszego badania NASK „Nastolatki 3.0"*, https://www.nask.pl/pl/aktualnosci/5316,Co-robia-nasze-dzieci-w-sieci-czyli-Raport-z-najnowszego-badania-NASK-Nastolatki.html [dostęp: 17.05.2024 r.].

Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców, red. R. Lange, Warszawa 2023, Państwowy Instytut Badawczy NASK, file:///C:/Users/951104/Downloads/Thinkstat_RAPORT_nastolatki-3_0_ONLINE.pdf [dostęp: 17.05.2024 r.].

Summary

What we are doing wrong and could be doing better in protecting children from online dangers

The purpose of the article is to discuss the numerous challenges and mistakes in protecting children and young people from online dangers and to point out what we can improve. Many children face various online dangers, including cyberbullying, exposure to inappropriate content and risky interactions with strangers. The time spent on online safety education in school is insufficient, and a more integrated approach that takes into account the intersection of online and offline experiences should be introduced. Adults tend to be quick to judge and focus on the effects rather than the causes of problematic Internet use by the youngest users. It is crucial to understand the various causes of children's long time spent in front of a screen, such as emotional problems, lack of interest or peer pressure, and to exhort them to solve these underlying problems. Moreover, it is extremely important to develop media literacy and critical thinking skills in children. Due to advances in technology, creating a safer online environment requires broader and deeper cooperation between parents, teachers and technology companies.

Tłumaczenie: Katarzyna Olbryś

DZIAŁANIA PROFILAKTYCZNE w obszarze cyberbezpieczeństwa dzieci i młodzieży

Fot. https://pl.freepik.com

st. sierż. Agnieszka Korż

Zakład Służby Prewencyjnej CSP

Niniejsza publikacja dotyczy zagadnień profilaktyki zagrożeń w wirtualnym świecie, który w dzisiejszych czasach jest głównym środkiem przekazywania wszelkich norm i wartości, miejscem, gdzie wiele osób, przede wszystkim bardzo młodych, buduje swoją tożsamość. Autorka ma nadzieję, że artykuł ten nie tylko przybliży problematykę cyberzagrożeń, lecz także zainicjuje lub udoskonali działania profilaktyczne podejmowane w tym obszarze.

W dniach 21–23 maja br. w Centrum Szkolenia Policji w Legionowie Biuro Prewencji Komendy Głównej Policji przeprowadziło seminarium szkoleniowe pn. „Nowe wyzwania dla współczesnej profilaktyki w obszarze cyberzagrożeń oraz handlu ludźmi, ze szczególnym uwzględnieniem dzieci i młodzieży".

Wydarzenie zorganizowane zostało dla policjantów koordynatorów ds. profilaktyki społecznej z komend wojewódzkich Policji, Komendy Stołecznej Policji, a także wykładowców szkół policyjnych realizujących zajęcia dydaktyczne w tym zakresie. Miało na celu poszerzenie wiedzy na temat współczesnych trendów dotyczących handlu ludźmi i zjawisk z nimi powiązanych, zwiększenie kompetencji w obszarach bezpieczeństwa finansowego i mobilnego w cyberprzestrzeni, a także wymianę doświadczeń dotyczących przedsięwzięć realizowanych oraz planowanych w tych obszarach.

Prowadzący seminarium zaznaczyli, że niezwykle istotną lekturą dla współczesnej profilaktyki w obszarze cyberzagrożeń jest publikacja *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców*. Badanie zostało zrealizowane przez NASK-PIB (Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy). Raport przedstawia, jak kształtuje się cyfrowy świat oraz polska młodzież, a także, jakie zjawiska korelują z młodzieżową aktywnością cyfrową, również tą negatywną. Raport jest wynikiem piątej fali badań, których każda edycja zawiera bloki stałych zagadnień, mierzących dynamikę wybranych zjawisk (czas, narzędzia, miejsce, inicjacja w zakresie problematycznego użytkowania internetu itd.) oraz tzw. bloki „sezonowe" związane z bieżącymi trendami cyfrowymi. W prezentowanym badaniu zwrócono szczególną uwagę na media społecznościowe i towarzyszące im problemy społeczne: samotność, samoocenę, seksualizację, uzależnienie, internetowe wyzwania itd. Raport prezentuje także deklaracje rodziców badanych nastolatków w celu konfrontacji rzeczywistych praktyk nastolatków z przekonaniami czy wyobrażeniami ich rodziców[1]. Tym samym daje policjantom realizującym zadania z zakresu profilaktyki społecznej obraz zagadnień i problematyki związanych z cyberaktywnością dzieci i młodzieży.

Raport odnotowuje wyraźny wzrost ilości czasu korzystania z internetu przez nastolatki w dni powszednie. Obecnie jest to 5 godzin 36 minut (vs. w 2020 r. – 4 godziny 50 minut). Prawie 90% nastolatków najczęściej korzysta z internetu w domu, a blisko co drugi – także w drodze, w podróży. Częściej niż co czwarty nastolatek jest online również w szkole. Najbardziej popularnym urządzeniem do korzystania z internetu jest smartfon. Najczęściej wskazywane przez młodzież aktywności online to rozrywka i komunikacja, m.in: słuchanie muzyki, kontakty ze znajomymi i rodziną za pomocą komunikatorów, czatów, oglądanie filmów i seriali, granie w gry online oraz korzystanie z serwisów społecznościowych. Co trzeci nastolatek deklaruje, że korzysta z internetu do odrabiania lekcji, natomiast tylko co szesnasty włącza sieć w celu poszerzania wiedzy[2].

Nadmienić należy również, że z przedmiotowego badania wynika, iż niemal połowa młodych ludzi spotyka się w internecie z sytuacjami, w których ich znajomi są atakowani i wyzywani (44,6%). Z ośmieszaniem i poniżaniem kogoś w sieci zetknął się co trzeci nastolatek (ośmieszanie – 33,2%, poniżanie 29,6%). Kiedy nastolatki doświadczają przemocy, najczęściej nie reagują i nikomu o tym nie mówią. Bierność w sytuacjach doświadczania przemocy w sieci wzrasta w stosunku do poprzednich lat (2022 r. – 38,5%, 2020 r. – 32,4%). Nastolatki bez względu na wiek, płeć czy miejsce zamieszkania obserwują różne formy cyberprzemocy. Ponadto w odpowiedzi na pytanie: „Czy spotkałeś/spotkałaś się z którymś z poniższych rodzajów przemocy internetowej?" wskazują takie formy przemocy, jak: zastraszanie, szantażowanie, rozpowszechnianie kompromitujących materiałów[3].

W odróżnieniu od „tradycyjnej" przemocy zjawisko cyberprzemocy charakteryzuje wysoki poziom anonimowości sprawcy, więc w tym przypadku traci na znaczeniu przewaga mierzona cechami fizycznymi czy społecznymi, a dodatkowym atrybutem sprawcy cyberprzemocy staje się umiejętność wykorzystywania możliwości, jakie dają media elektroniczne. Charakterystyczna dla problemu szybkość rozpowszechniania materiałów kierowanych przeciwko ofierze oraz ich powszechna dostępność w sieci sprawiają, że jest to zjawisko szczególnie niebezpieczne[4]. W celu ochrony przed cyberprzemocą można wykorzystywać istniejące regulacje zarówno prawa karnego, jak i cywilnego. W szczególności mowa tu o przestępstwach zniesławienia lub zniewagi, naruszenia wizerunku, stalkingu, podszywania się pod kogoś, groźby, włamania do się do sieci teleinformatycznych. W przypadku tych przestępstw ściganie sprawcy cyberprzemocy następuje po złożeniu wniosku przez osobę pokrzywdzoną.

Podstawą do wymierzenia kary są m.in. następujące artykuły Kodeksu karnego:[5]

– 190 k.k. (groźba karalna),
– 190a k.k. (uporczywe nękanie, podszywanie się),
– 191 k.k. (zmuszenie do określonego działania),
– 191a k.k. (naruszenie intymności seksualnej, utrwalenie wizerunku nagiej osoby bez jej zgody),
– 212 k.k. (zniesławienie),
– 216 k.k. (zniewaga),
– 267 k.k. (bezprawne uzyskanie informacji, włamanie się do sieci teleinformatycznych),
– 269 k.k. (uszkodzenie danych informatycznych),
– 269a k.k. (zakłócanie systemu komputerowego),
– 287 k.k. (oszustwo komputerowe).

Odwołując się do wniosków z raportu *Nastolatki 3.0*, należy wskazać, że młodzież korzystała z wielu stron internetowych i aplikacji o bardzo zróżnicowanej tematyce, w tym m.in.: patostreamów – wulgarnych, obscenicznych i nacechowanych przemocą widowisk lub transmisji internetowych nadawanych na żywo w serwisach streamingowych, np. YouTube, Twitch. Wyniki badań wskazują, iż co czwarty nastolatek ogląda tzw. patostreamy, a blisko co szósty nie jest w stanie określić, czy oglądane przez niego treści mają cechy patostreamu i czy są wulgarne lub nacechowane przemocą[6]. Kontakt z negatywnymi informacjami, których młody człowiek nie potrafi odpowiednio zinterpretować i którym bezgranicznie wierzy, może prowadzić u niego do trwałego pogorszenia nastroju, obniżenia poczucia bezpieczeństwa, a w efekcie do wypaczenia obrazu rzeczywistości. Możliwe konsekwencje kontaktu dziecka ze szkodliwymi treściami to:

– lęk, niepokój, obniżenie poczucia bezpieczeństwa,
– wypaczony obraz rzeczywistości,
– pogorszenie nastroju,
– demoralizacja i zachowania sprzeczne z normami społecznymi,
– znieczulenie na losy ofiar przemocy,
– agresywna postawa wobec innych,
– ryzykowne zachowania i działania antyspołeczne,
– fałszywe poglądy na sferę seksualności[7].

Wyraźnie najpopularniejszym serwisem z tej kategorii jest Pornhub.com – odwiedzony przez ponad jedną czwartą osób z grupy 1,3 mln użytkowników w wieku 7–19 lat. Młodzież odwiedzała również strony związane z podejmowaniem ryzykownych zachowań, m.in. wprowadzających w świat hazardu. Przykładem tego jest kategoria zakładów bukmacherskich. Ponad 800 tysięcy przedstawicieli młodzieży weszło na stronę STS.pl, a prawie pół miliona na stronę Betclic.pl. Ważną kwestią podnoszoną w raporcie jest wzrost liczby osób nastoletnich, które decydują się na spotkanie z osobą dorosłą, poznaną w internecie (2022 r. – 17,9%, 2020 r. – 14,1%). Co czwarty nastolatek nikogo nie poinformował o takim zdarzeniu (2022 r. – 25,3%, 2020 r. – 24,5%)[8]. W tym obszarze istnieje realne zagrożenie dla dzieci i młodzieży.

Należy również wspomnieć o ryzykownych zachowaniach dzieci w sieci w postaci sextingu. Termin powstał z połączenia słów „sex" i „texting". Na początku dotyczył wysyłania smsów, ale wraz z rozwojem technologii i komunikatorów zmienił się jego charakter oraz sposób komunikacji. W wielu przypadkach materiały przesyłane sobie przez młodych pozostają tylko między nimi, natomiast zdarza się, że zdjęcie lub film trafią w niepowołane ręce. Może tak się stać w wyniku konfliktu, zemsty, chęci zaimponowania innym lub kradzieży danych, kradzieży telefonu, włamania na profil czy konto[9]. Według danych z raportu w szkole średniej, co drugi nastolatek potwierdza, że otrzymał treści z czyimś nagim wizerunkiem. Co czwarty uczeń 7 klasy szkoły podstawowej otrzymuje tego rodzaju materiały, dotyczy to zarówno chłopców, jak i dziewcząt[10].

Niezmiernie ważne jest, aby w trakcie spotkań profilaktycznych uświadamiać młodzież w zakresie odpowiedzialności prawnej, o tym, że z pozoru dla nich niewinne zachowanie może wypełnić znamiona przestępstwa z art. 200a § 2 Kodeksu karnego, zgodnie z którym karze grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2 podlega ten, kto „za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej małoletniemu poniżej lat 15 składa propozycję obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych, i zmierza do jej realizacji". W świetle prawa, zgodnie z ustawą z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich (Dz. U. z 2024 r. poz. 560), osoby prawomocnie skazane wyrokiem sądu podlegają wpisowi do Rejestru Sprawców Przestępstw na Tle Seksualnym. Skutkiem tego wpisu może być nadmierna represja i stygmatyzacja takiej osoby w społeczeństwie, może to również rzutować na przyszłość nieletniego w dorosłym życiu.

Mimo że dane osób nieletnich nie są powszechnie dostępne, to dostęp do nich może uzyskać m.in: pracodawca czy podmiot prowadzący działalność związaną z wychowaniem, edukacją, wypoczynkiem, leczeniem małoletnich lub z opieką nad nimi.

W świetle powyższego niezwykle ważne jest zapobieganie problemowi poprzez podejmowanie zajęć profilaktycznych w szkołach i placówkach poświęconych zagrożeniom czynami zabronionymi i czynami karalnymi przeciwko wolności seksualnej i obyczajności, w tym w cyberprzestrzeni, oraz zagadnieniom odpowiedzialności prawnej nieletnich, a także działań prewencyjnych poprzez sprawne przekazanie informacji organom właściwym do prowadzenia postępowania karnego w przypadku uzasadnionego podejrzenia popełnienia przestępstwa oraz poprzez upowszechnianie informacji o punktach i miejscach świadczących specjalistyczną pomoc i udzielających wsparcia małoletnim pokrzywdzonym czynami zabronionymi, czynami karalnymi przeciwko wolności seksualnej i obyczajności oraz o rodzaju świadczonej pomocy i wsparcia.

Należy również wspomnieć, iż przepisy dotyczące standardów ochrony małoletnich znajdujące się w art. 22b i 22c ustawy z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniem przestępczości na tle seksualnym i ochronie małoletnich zostały zmienione ustawą z dnia 28 lipca 2023 r. o zmianie ustawy – Kodeks rodzinny i opiekuńczy oraz niektórych innych ustaw (Dz. U. poz. 1606), czyli tzw. ustawą Kamilka, która weszła w życie 15 lutego 2024 r. Zmiany wprowadzone dzięki tej ustawie zakładają m.in. wdrożenie procedury *Serious Case Reviews*. Chodzi o obowiązek analiz najpoważniejszych przypadków przemocy wobec najmłodszych. Istotne jest również wprowadzenie „Standardów Ochrony Małoletnich" w różnych instytucjach (m.in. szkołach, szpitalach, ale również obiektach turystycznych), a także zmiany w zakresie instytucji reprezentanta dzieci. W pomoc najmłodszym ofiarom przemocy angażuje się Sieć Pomocy Pokrzywdzonym, prowadzona w ramach Funduszu Sprawiedliwości. Ministerstwo Sprawiedliwości wraz z ekspertami przeprowadziło prace nad stworzeniem ogólnopolskiej strategii walki z przestępczością seksualną wobec dzieci, której efektem jest Krajowy Plan Działania na rzecz ochrony dzieci przed przestępstwami na tle seksualnym[11].

Podsumowując wnioski płynące z przywołanego raportu, a także z udziału w wyżej wspomnianym seminarium, należy podkreślić, że obok pozytywnych aspektów aktywności małoletnich w cyberprzestrzeni występuje duże zagrożenie związane z narażeniem najmłodszych na nielegalne lub niechciane treści, cyberprzemoc, a także wiele zagrożeń wynikających z naruszenia prywatności i danych osobowych.

Wraz ze wzrostem ilości czasu spędzanego w sieci zwiększa się także ryzyko styczności z materiałami o charakterze pornograficznym, treściami szkodliwymi, mową nienawiści i dezinformacją, jak również ryzyko niechcianego kontaktu, uwodzenia, wykorzystywania i przemocy. Istotną kwestią są także skutki społeczne, czyli: zaniedbywanie codziennych obowiązków przez małoletnich, poczucie osamotnienia, brak umiejętności nawiązywania lub podtrzymywania relacji społecznych, zerwanie takich relacji w grupie rówieśniczej, niepokój towarzyszący konieczności konfrontowania się z innymi osobami bezpośrednio, brak umiejętności kreatywnego spędzania czasu czy organizowania sobie czasu wolnego (ciągłe narzekanie na nudę). Natomiast od strony fizjologicznej korzystanie z nowości technologicznych w nieodpowiedniej pozycji powoduje ogromne obciążenie dla układu ruchu, tzn. syndrom SMS-owej szyi (*Text Neck Syndrome*), który jest zespołem dolegliwości bólowych doświadczanych przez osoby długotrwale korzystające ze smartfonów, tabletów i komputerów. Nadmierne korzystanie z urządzeń elektronicznych może również skutkować wadami wzroku, problemami ze snem, bólami głowy, nadgarstka, tikami nerwowymi, zaburzeniami odżywania, zespołem przewlekłego zmęczenia, szumami w uszach.

Podsumowanie

Seminarium szkoleniowe pn. „Nowe wyzwania dla współczesnej profilaktyki w obszarze cyberzagrożeń oraz handlu ludźmi ze szczególnym uwzględnieniem dzieci i młodzieży" dało uczestnikom możliwość poszerzenia wiedzy na temat współczesnych trendów związanych z handlem ludźmi, a także na temat cyberzagrożeń, co wpłynie na skuteczność podejmowanych działań przez funkcjonariuszy w zwalczaniu przestępczości, działań wykrywczych oraz działań prewencyjnych w postaci podejmowanych przedsięwzięć profilaktycznych, w tym również z udziałem podmiotów pozapolicyjnych, tj. instytucji rządowych i organizacji pozarządowych.

[1] *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców*, red. R. Lange, Warszawa 2023, Państwowy Instytut Badawczy NASK, file:///C:/Users/951104/Downloads/Thinkstat_RAPORT_nastolatki-3_0_ONLINE.pdf [dostęp: 27.06.2024 r.].
[2] Tamże.
[3] Tamże.
[4] Ł. Wojtasik, *Cyberprzemoc – charakterystyka zjawiska, skala problemu, działania profilaktyczne*, https://www.sp118.pl/userdata/projekty/internet/cyberprzemoc.pdf [dostęp: 27.06.2024 r.].
[5] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2024 r. poz. 17).
[6] *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców*, red. R. Lange.
[7] J. Piechna, *Szkodliwe treści w internecie. Nie akceptuję, reaguję!*, NASK Państwowy Instytut Badawczy, Warszawa 2019, https://cyberprofilaktyka.pl/publikacje/Szkodliwe%20tre%c5%9bci%20w%20internecie_www.pdf [dostęp: 27.06.2024 r.].
[8] *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców*, red. R. Lange.
[9] Serwis Rzeczypospolitej Polskiej, *Sexting: czy wiesz o nim wszystko?*, https://www.gov.pl/web/niezagubdzieckawsieci/sexting-czy-wiesz-o-nim-wszystko [dostęp: 27.06.2024 r.].
[10] *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów i rodziców*, red. R. Lange.
[11] Ministerstwo Sprawiedliwości, *Ustawa Kamilka podpisana przez Prezydenta RP*, https://www.gov.pl/web/sprawiedliwosc/ustawa-kamilka-podpisana-przez-prezydenta-rp [dostęp: 27.06.2024 r.].

Summary

Preventive actions in the area of cybersecurity of children and youth

This article concerns the issues discussed during a training seminar called "New challenges for contemporary prevention in the area of cyberthreats and human trafficking, with particular reference to children and youth," which was carried out by the Prevention Bureau of the National Police Headquarters on May 21–23, 2024 at the Police Training Centre in Legionowo. The seminar provided an opportunity to exchange experience on the events planned and performed by police officers for social prevention from the provincial police headquarters and the Warsaw Metropolitan Police, as well as by police school intructors who conduct classes in this area.

Tłumaczenie: Katarzyna Olbryś

KONFISKATA POJAZDU MECHANICZNEGO

w świetle nowych przepisów

Fot. 1. https://pixabay.com/pl/photos/samochód-awangarda-holowniczy-8196862/.

podkom. Rafał Bloch

Zakład Służby Kryminalnej CSP

W niniejszym artykule omówiono nowy środek prawnokarny w postaci przepadku pojazdu mechanicznego bądź jego równowartości za wybrane rodzaje przestępstw przeciwko bezpieczeństwu w komunikacji. Regulacja ta została ujęta w art. 44b Kodeksu karnego i obowiązuje od dnia 14 marca 2024 r. Podkreślono, że zmiany w przepisach polskiego prawa dotyczące wprowadzenia surowszych konsekwencji w ruchu kołowym są odpowiedzią na dużą liczbę wypadków drogowych oraz powodowanie zagrożenia bezpieczeństwa w ruchu, a także mają mieć wydźwięk prewencyjny. Konfiskata auta za określone przewinienia drogowe ma na celu odstraszenie np. nietrzeźwych kierujących od poruszania się pojazdem mechanicznym w ruchu drogowym. Analiza przepisu dotyczącego przepadku pojazdu mechanicznego została przedstawiona na tle regulacji prawnych w tym zakresie obowiązujących w innych państwach europejskich.

Przepadek pojazdu mechanicznego lub jego równowartości – art. 44b k.k.

Ustawa z 7 lipca 2022 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. poz. 2600, z późn. zm.) oraz ustawa z dnia 7 lipca 2023 r. o zmianie ustawy – Kodeks postępowania cywilnego, ustawy – Prawo o ustroju sądów powszechnych, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz. U. poz. 1860) wprowadziły nowy środek prawnokarny w postaci przepadku pojazdu mechanicznego bądź jego równowartości za wybrane rodzaje przestępstw przeciwko bezpieczeństwu w komunikacji. Regulacja ta obowiązuje od dnia 14 marca 2024 r. i została ujęta w art. 44b Kodeksu karnego[1], zgodnie z którym:

§ 1.

W wypadkach wskazanych w ustawie sąd orzeka przepadek pojazdu mechanicznego[2] prowadzonego przez sprawcę w ruchu lądowym[3].

§ 2.

Jeżeli w czasie popełnienia przestępstwa pojazd nie stanowił wyłącznej własności sprawcy albo po popełnieniu przestępstwa sprawca zbył, darował lub ukrył podlegający przepadkowi pojazd, orzeka się przepadek równowartości pojazdu. Za równowartość pojazdu uznaje się wartość pojazdu określoną w polisie ubezpieczeniowej na rok, w którym popełniono przestępstwo, a w razie braku polisy – średnią wartość rynkową pojazdu odpowiadającego, przy uwzględnieniu marki, modelu, roku produkcji, typu nadwozia, rodzaju napędu i silnika, pojemności lub mocy silnika oraz przybliżonego przebiegu, pojazdowi prowadzonemu przez sprawcę, ustaloną na podstawie dostępnych danych, bez powoływania w tym celu biegłego.

§ 3.

Jeżeli ustalenie średniej wartości rynkowej pojazdu odpowiadającego pojazdowi, o którym mowa w § 1, w sposób określony w § 2 nie jest możliwe ze względu na szczególne cechy tego pojazdu, zasięga się opinii biegłego.

§ 4.

Przepadku pojazdu mechanicznego oraz przepadku równowartości pojazdu określonego w § 2 nie orzeka się, jeżeli sprawca prowadził niestanowiący jego własności pojazd mechaniczny wykonując czynności zawodowe lub służbowe polegające na prowadzeniu pojazdu na rzecz pracodawcy. W takim wypadku sąd orzeka nawiązkę w wysokości co najmniej 5000 złotych na rzecz Funduszu Pomocy Pokrzywdzonym oraz Pomocy Postpenitencjarnej.

§ 5.

Przepadku pojazdu mechanicznego oraz przepadku równowartości pojazdu nie orzeka się, jeżeli orzeczenie przepadku pojazdu mechanicznego jest niemożliwe lub niecelowe z uwagi na jego utratę przez sprawcę, zniszczenie lub znaczne uszkodzenie.

Zgodnie z brzmieniem powyższego przepisu w sytuacjach wskazanych w ustawie sąd orzeka przepadek pojazdu mechanicznego prowadzonego przez sprawcę w ruchu lądowym. Okoliczność modalna miejsca wskazuje wyłącznie na ruch lądowy, gdyż w ruchu wodnym i powietrznym sytuacje te występują znacznie rzadziej i statystycznie mają marginalne znaczenie. W sytuacji gdy w czasie popełnienia przestępstwa pojazd nie stanowił wyłącznej własności sprawcy albo po popełnieniu przestępstwa sprawca ukrył, darował lub zbył podlegający przepadkowi pojazd, orzeka się przepadek równowartości pojazdu. Oznacza to, że bez względu na kwestie własności pojazdu sprawca poniesie konsekwencje w formie rzeczowej bądź pieniężnej.

Legislator określił pojęcie równowartości pojazdu w oparciu o wartość z polisy ubezpieczeniowej zawartej na rok popełnienia czynu zabronionego w postaci przestępstwa, a w razie braku zawarcia takiej polisy – średnią wartość rynkową. Istotne jest to, że badanie wartości rynkowej jest obowiązkiem sądu, gdyż w tej mierze nie będzie powołany biegły. Rozwiązanie to może przysparzać pewnych praktycznych trudności. Ustawodawca zezwala na zasięgnięcie opinii biegłego, gdy ustalenie wartości rynkowej będzie niemożliwe ze względu na indywidualne szczególne cechy pojazdu, powodujące jego „oryginalność". W pozostałych sytuacjach sąd jest zobligowany do przeprowadzenia własnych ustaleń faktycznych. Przypadek ten występuje tylko, gdy pojazd nie ma polisy ubezpieczeniowej. Przepadek pojazdu mechanicznego nie dotyczy sytuacji, gdy sprawca będzie prowadził niestanowiący jego własności pojazd, wykonując czynność zawodową lub służbową polegającą na prowadzeniu pojazdu na rzecz pracodawcy. W tej sytuacji sąd orzeka nawiązkę w wysokości co najmniej 5000 zł na rzecz Funduszu Pomocy Pokrzywdzonym oraz Pomocy Postpenitencjarnej. Przyjęte rozwiązanie może być tematem dyskusyjnym, gdyż nietrzeźwy kierowca, prowadzący w ramach czynności zawodowych nienależącą do siebie „ciężarówkę" lub autobus, może stworzyć poważne zagrożenie bezpieczeństwa w ruchu lądowym. Czyn popełniony przez takiego sprawcę cechuje się dość wysoką społeczną szkodliwością, a od takiego kierującego oczekiwalibyśmy wzmożonego poszanowania zasad w ruchu kołowym bądź pieszym. W sytuacji niedostosowania się do obowiązujących przepisów oczekuje się konsekwencji adekwatnych do popełnienia czynu.

Nie orzeka się również przepadku pojazdu mechanicznego ani równowartości pojazdu, gdy jest to niemożliwe lub niecelowe z uwagi na jego zniszczenie, znaczne uszkodzenie lub utratę.

Utrata pojazdu obejmuje wszystkie przypadki, gdy sprawca stracił posiadanie pojazdu, np. pojazd zajęty w skutek egzekucji lub skradziony. Uszkodzenie pojazdu należy rozumieć jako znaczne, czyli takie, że orzeczenie przepadku staje się niemożliwe lub niecelowe. Niecelowość orzekania przepadku pojazdu wchodzi w grę np. gdy uszkodzenia są na tyle duże, że jest prawdopodobne, iż nie zostanie on dopuszczony do ruchu, lub uszkodzenie pojazdu jest na tyle duże, że orzeczenie przepadku nie będzie realną dolegliwością dla sprawcy.

Komentowany przepis oznacza, że przepadkowi podlega pojazd bądź równowartość pojazdu, którym porusza się sprawca. Wysokość dolegliwości majątkowej nie jest uzależniona od wagi czynu, a od wartości pojazdu mechanicznego, która może być bardzo zróżnicowana.

W obowiązującym stanie prawnym od 14 marca 2024 r. konfiskata pojazdu mechanicznego zostanie orzeczona albo będzie mogła być orzeczona w ruchu lądowym dla sprawcy, który:

1) sprowadził katastrofę (art. 173 § 1 lub 2 k.k.), a także sprowadził katastrofę z następstwem w postaci śmierci człowieka lub ciężkiego uszczerbku na zdrowiu wielu osób (art. 173 § 3 lub 4 k.k.), sprowadził bezpośrednie niebezpieczeństwo katastrofy (art. 174 k.k.), wypadku komunikacyjnego (art. 177 § 1 k.k.) lub wypadku komunikacyjnego z następstwem w postaci śmierci osoby lub ciężkiego uszczerbku na jej zdrowiu (art. 177 § 2 k.k.):
   a) znajdując się pod wpływem środków odurzających lub w stanie nietrzeźwości lub
   b) zbiegł z miejsca zdarzenia, nawet nie znajdując się pod wpływem środków odurzających lub w stanie nietrzeźwości lub
   c) zażywając środek odurzający lub spożywając alkohol po popełnieniu tych przestępstw, a przed pod-

daniem go przez uprawniony organ badaniu w celu ustalenia w organizmie obecności środka odurzającego lub zawartości alkoholu, przy czym orzeczenie przepadku jest obligatoryjne, jeżeli zawartość alkoholu w organizmie sprawcy jest wyższa niż 1 promil we krwi lub 0,5 mg/dm^3;

2) prowadził pojazd pod wpływem środka odurzającego (przepadek pojazdu będzie orzeczony bez względu na stężenie tego środka w organizmie) lub w stanie nietrzeźwości (art. 178a § 1 k.k.), chyba że zawartość alkoholu w organizmie będzie niższa niż 1,5 promila we krwi lub 0,75 mg/dm^3 w wydychanym powietrzu albo nie prowadziła do takiego stężenia;
3) prowadził pojazd pod wpływem środka odurzającego lub w stanie nietrzeźwości po wcześniejszym prawomocnym skazaniu za prowadzenie pojazdu mechanicznego pod wpływem środka odurzającego lub w stanie nietrzeźwości lub za przestępstwo określone w art. 173 k.k., 174 k.k., 177 k.k. albo 355 § 2 k.k. popełnione pod wpływem środka odurzającego lub popełnione w stanie nietrzeźwości albo za prowadzenie pojazdu pod wpływem środka odurzającego lub w stanie nietrzeźwości w okresie obowiązywania zakazu prowadzenia pojazdów mechanicznych, czyli w ramach tzw. recydywy, niezależnie od stopnia stanu nietrzeźwości, nawet jeśli stężenie alkoholu w organizmie sprawcy było mniejsze niż 1,5 promila we krwi lub 0,75 mg/dm^3 w wydychanym powietrzu (art. 178a § 4 k.k.).

Należy jednak pamiętać, że przedmiotem tymczasowego zajęcia może być prowadzony przez sprawcę pojazd mechaniczny, który w chwili popełnienia ww. przestępstwa jest wyłącznie jego własnością. Podstawę wstępnej weryfikacji powinny stanowić ustalenia danych o pojeździe, dokonane w trybie art. 129 ust. 2 pkt 21 ustawy – Prawo o ruchu drogowym[4] w Centralnej Ewidencji Pojazdów[5].

Od 14 marca 2024 r. wszedł również w życie art. 295 § 1a Kodeksu postępowania karnego, który stanowi:

W razie popełnienia przestępstwa, za które orzeka się przepadek pojazdu mechanicznego, o którym mowa w ***art. 44b*** *Kodeksu karnego (przepadek pojazdu mechanicznego prowadzonego przez sprawcę lub równowartości pojazdu), Policja dokonuje tymczasowego zajęcia pojazdu mechanicznego prowadzonego przez sprawcę w czasie popełnienia tego przestępstwa*[6].

Wprowadzenie powyższej kwalifikacji daje możliwość tymczasowego zajmowania przez Policję pojazdu mechanicznego na poczet jego przepadku. W sytuacji obligatoryjnego orzeczenia przepadku pojazdu należy sporządzić protokół tymczasowego zajęcia pojazdu mechanicznego. Zasadne będzie więc dokonanie protokołu oględzin pojazdu celem udokumentowania jego stanu w chwili zabezpieczenia w trybie procesowym. Ponadto może to ułatwić ustalenie jego wartości.

Warto dodać, że obecnie trwają prace w Ministerstwie Sprawiedliwości nad kolejną zmianą przepisów, tak aby sąd otrzymał fakultatywną możliwość orzeczenia przepadku pojazdu lub jego równowartości, a nie jak jest dotychczas – obligatoryjnie. Ponadto MS rozważa rozszerzenie tych przepisów na ruch wodny i powietrzny, a więc konfiskacie będzie mogła podlegać również np. motorówka lub awionetka.

Konfiskata auta w Europie

Polska nie jest jedynym krajem w Europie, gdzie można stracić auto za przewinienia drogowe. Najczęściej jest ono konfiskowane za jazdę pod wpływem alkoholu, ale nie tylko. Spośród krajów europejskich najbardziej restrykcyjne przepisy drogowe obowiązują obecnie **w Austrii**. Od marca 2024 r. austriackie prawo przewiduje możliwość konfiskaty i sprzedaży samochodu na aukcji. Sankcja ta dotyczy przypadków przekroczenia prędkości o 60 km/h i więcej na obszarach miejskich lub ponad 70 km/h poza obszarami miejskimi. Jeśli kierowca dopuszcza się recydywy, samochód może zostać trwale skonfiskowany i zlicytowany, podobnie jak w Polsce po tymczasowym zajęciu. W szczególnych przypadkach – zwłaszcza przy przekroczeniu prędkości o ponad 80 km/h na obszarze miejskim lub 90 km/h poza miastem – istnieje ryzyko, że pojazd ulegnie konfiskacie i licytacji za pierwsze wykroczenie[7]. Dodatkowo na konfiskatę pojazdu naraża się ten, kto jeździ po odebraniu prawa jazdy z powodu przekroczenia prędkości lub przekroczy prędkość bez prawa jazdy. Odebranie auta nastąpi zawsze, nawet gdy kierowca nie jest jego właścicielem[8].

W Niemczech obowiązują mniej restrykcyjne przepisy – utrata auta nastąpi jedynie, gdy nie będziemy mieli ważnego ubezpieczenia. Samochód nie zostanie też skonfiskowany, jeśli kierowca nie jest jego właścicielem[9].

Z kolei **we Francji** kierowca może stracić auto za różne przewinienia. Pożegnać się z samochodem mogą tam ci, którzy przekroczyli limit prędkości o ponad 50 km/h; mieli powyżej 0,5 promila alkoholu: spowodowali kolizję, a następnie oddalili się z miejsca wypadku; nie wykupili obowiązkowego ubezpieczenia bądź poruszają się bez prawa jazdy. Jeżeli kierowca jest właścicielem pojazdu, to pojazd ten jest konfiskowany. W innym przypadku odbierana jest jego równowartość w unijnej walucie[10].

W Danii auto odbierane jest kierowcy, który prowadzi je, mając 2 promile lub więcej, był skazany przez sąd za szczególnie niebezpieczną jazdę albo nie ma ubezpieczenia[11].

We Włoszech utrata samochodu grozi za brak OC lub gdy zdecydowanie przesadzimy z alkoholem – potrzeba do tego aż 3,15 promila lub więcej[12].

W Luksemburgu utrata auta nastąpi, jeśli mamy powyżej 0,5 promila alkoholu, ale przy okazji musimy popełnić takie wykroczenie więcej niż raz w krótkim odstępie czasu. Nie jest określone w jak krótkim. Trzeba jednak być właścicielem pojazdu, aby go utracić[13].

Ciekawymi przypadkami są Finlandia i Szwajcaria.

W Finlandii auto można stracić za wykorzystanie go do kradzieży paliwa, a także innych przestępstw umyślnych. Dzieje się tak również w przypadku, kiedy kierowca wielokrotnie jeździł bez prawa jazdy albo samochód nie ma ubezpieczenia. Auta nie odbiera się, jeśli kierowca nie jest jego właścicielem[14].

W Szwajcarii pojazd będzie skonfiskowany, gdy spowodujemy nadmierny hałas, zwłaszcza nocą. Takie same konsekwencje powoduje przekroczenie prędkości o 50 km/h na autostradzie, a także prowadzenie pojazdu, jeśli ma się 0,5 promila lub więcej. Trzeba jednak zaznaczyć, że wtedy dokonuje się oceny, czy konfiskata jest konieczna, aby zapobiec kolejnym przestępstwom. Interesujące jest także

podejście do odbierania samochodu nienależącego do kierowcy. Może być on odebrany, ale tylko w sytuacji, gdy jego właściciel uczestniczył w tych czynach zabronionych. Auta konfiskuje się również **w Belgii**, w przypadku gdy kierowca jechał pod wpływem alkoholu i miał powyżej 0,5 promila, bez ubezpieczenia lub prawa jazdy. Pojazd może być zabrany, nawet jeśli nie należy do kierowcy, ale jedynie wtedy, gdy właściciel z pełną świadomością go udostępnił[15].

Na Litwie konfiskata auta następuje po przekroczeniu limitu 0,4 promila lub w przypadku ucieczki z miejsca zdarzenia drogowego. **W Estonii** natomiast samochód jest odbierany za rażące przekroczenie prędkości lub za jazdę pod wpływem alkoholu, co jest dość proste, bowiem limit w tym kraju wynosi 0,0 promila. **Na Łotwie** przesłanką do odebrania pojazdu jest przekroczenie limitu 0,5 promila alkoholu. Ani na Litwie, ani na Łotwie nie odbiera się samochodu kierowcy, jeśli nie jest on właścicielem tego pojazdu. W Estonii zaś warunki odebrania auta kierowcy niebędącemu jego właścicielem są podobne jak w Belgii[16].

[1] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. 2024 r. poz. 17).

[2] Pojęcie pojazdu mechanicznego, stosowane w Kodeksie karnym i Kodeksie wykroczeń, nie zostało zdefiniowane ustawowo. Sąd Najwyższy w 2007 r. dokonał dookreślenia tego pojęcia, wskazując, że oznacza ono pojazd zaopatrzony w poruszający nim silnik, taki jak: pojazd samochodowy, maszyna rolnicza, motocykl, lokomotywa kolejowa, helikopter, samolot, statek wodny, a także pojazd szynowy zasilany z trakcji (tramwaj, trolejbus).

[3] Pojęcie ruchu lądowego obejmuje nie tylko ruch odbywający się na drogach publicznych i w strefach zamieszkania lub strefach ruchu, ale też na terenach budowlanych i przemysłowych, lotniskach, na drogach leśnych itp., a więc ruch odbywający się we wszelkich miejscach dostępnych do powszechnego użytku, na których odbywa się rzeczywisty ruch pojazdów. […] Do dróg wewnętrznych należą m.in. drogi dojazdowe do gruntów rolnych i leśnych, drogi leśne, drogi w osiedlach mieszkaniowych, parkingi, place przed dworcami autobusowymi, kolejowymi i portami, drogi prowadzące do obiektów użytkowanych przez przedsiębiorców, pętle autobusowe czy drogi znajdujące się na zamkniętym terenie kopalni, fabryki, budowy. Natomiast do miejsc dostępnych dla ruchu pojazdów nie mogą zostać zaliczone miejsca, w których nie odbywa się ruch ogólnodostępny, a jedynie w danym miejscu dopuszczone jest do ruchu wąskie grono osób – np. podwórka przydomowe, warsztat samochodowy, grunty rolne czy łąki (wyrok Sądu Najwyższego z dnia 26 lutego 2020 r., sygn. IV KK 265/19, SIP «Lex» nr 3079480).

[4] Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2023 r. poz. 1047, z późn. zm.).

[5] Pismo nr KR-DŚ-883/2024 Dyrektora Biura Kryminalnego KGP z dnia 8 marca 2024 r.

[6] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2024 r. poz. 37).

[7] Pasternak LEGAL, *Konfiskata samochodu – nowe przepisy 2024*, https://pasternaklegal.pl/konfiskata-samochodu-nowe-przepisy-2024/#Konfiskata_auta_w_Europie [dostęp: 3 czerwca 2024 r.].

[8] M. Pokorzyński, *W tych krajach konfiskują auta nie tylko za alkohol. Za co jeszcze?*, https://www.auto-swiat.pl/wiadomosci/aktualnosci/w-tych-krajach-konfiskuja-auta-nie-tylko-za-alkohol-za-co-jeszcze/l6rx212 [dostęp: 3 czerwca 2024 r.].

[9] Tamże.

[10] Tamże.

[11] Tamże.

[12] Tamże.

[13] Tamże.

[14] Tamże.

[15] Tamże.

[16] Tamże.

Bibliografia

Kodeks karny, Komentarz, red. J. Majewski, Wolters Kluwer Polska, 2024.

Kodeks Karny. Komentarz aktualizowany, red. M. Mozgawa, https://sip.lex.pl/komentarze-i-publikacje/komentarze/kodeks-karny-komentarz-aktualizowany-587736803 [dostęp: 4 czerwca 2024 r.].

Kodeks karny. Komentarz, red. V. Konarska-Wrzosek, wyd. IV, Wolters Kluwer Polska, 2023.

Pasternak LEGAL, *Konfiskata samochodu – nowe przepisy 2024*, https://pasternaklegal.pl/konfiskata-samochodu-nowe-przepisy-2024/#Konfiskata_auta_w_Europie [dostęp: 3 czerwca 2024 r.].

Pokorzyński M., *W tych krajach konfiskują auta nie tylko za alkohol. Za co jeszcze?*, https://www.auto-swiat.pl/wiadomosci/aktualnosci/w-tych-krajach-konfiskuja-auta-nie-tylko-za-alkohol-za-co-jeszcze/l6rx212 [dostęp: 3 czerwca 2024 r.].

Rogozińska Ż., *Przepadek pojazdu mechanicznego od marca 2024 r.*, https://sip.legalis.pl/document-full.seam?documentId=nzuxk4zogi3danbvgy3dony&refSource=-guide [dostęp: 25 czerwca 2024 r.].

Stefański R., *Glosa do wyroku SN z dnia 25 października 2007 r.,* sygn. III KK 270/07, „Prokuratura i Prawo" 2008, nr 5.

Ustawa z dnia 7 lipca 2023 r. o zmianie ustawy – Kodeks postępowania cywilnego, ustawy – Prawo o ustroju sądów powszechnych, ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz. U. poz. 1860).

Ustawa z 7 lipca 2022 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. poz. 2600, z późn. zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. 2024 r. poz. 17).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2024 r. poz. 37).

Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2023 r. poz. 1047, z późn. zm.).

Wyrok Sądu Najwyższego z dnia 26 lutego 2020 r., sygn. IV KK 265/19, SIP «Lex» nr 3079480.

Summary

Forfeiture of a motor vehicle in the light of new legal provisions

This article discusses a new criminal legal measure in the form of forfeiture of a motor vehicle or its equivalent for selected types of crimes against safety of communication. This regulation is included in Article 44b of the Penal Code and came into force on March 14, 2024. It is emphasized that the changes in Polish law relating to the introduction of harsher consequences in vehicular traffic are a response to causing threats to traffic safety as well as the large number of road accidents. They are also expected to have preventive overtones. The forfeiture of a car for certain traffic offenses is intended to deter, for example, intoxicated drivers from operating a motor vehicle in traffic. The analysis of the provision on the forfeiture of a motor vehicle is presented against the background of legal regulations in this area in other European countries.

Tłumaczenie: Katarzyna Olbryś

Konferencja Ratownictwa Wodnego

„ON DUTY 2024” GDYNIA

kom. Kinga Czerwińska

Zespół Policji Wodnej
Zakład Szkoleń Specjalnych CSP

W dniach 24–26 maja br. w Gdyni po raz piąty odbyła się Konferencja Ratownictwa Wodnego „On Duty”. Jej celem były wymiana doświadczeń i rozwijanie współpracy w celu zwiększenia skuteczności ratownictwa wodnego i poprawy bezpieczeństwa na wodzie i terenach przywodnych. Wzięli w niej udział m.in. przedstawiciele służb, szkół i uczelni, firm i instytucji związanych ratownictwem wodnym. Specjalistyczny sprzęt do ratownictwa wodnego zaprezentowało ponad 20 wystawców. Przedsięwzięcie obejmowało dwa dni wykładów, prelekcji i warsztatów w obiektach Akademii Marynarki Wojennej oraz trzeci dzień – pokazy i praktyczne testowanie sprzętu na wodach Zatoki Puckiej.

Przedsięwzięcie zostało zorganizowane przez Jakuba Friedenbergera, koordynatora Ratownictwa Wodnego w Komendzie Wojewódzkiej Straży Pożarnej w Gdyni, w ścisłej współpracy z Akademią Marynarki Wojennej w Gdyni, Kosakowo Sport sp. z o.o., Stowarzyszeniem „Morska Baza Szkoleniowa Mechelinki”, Kawasaki Polska, Ochotniczą Strażą Pożarną Ratownictwo Wodne Gdynia.

W konferencji wzięło udział 150 osób, w tym prelegenci z Austrii, Belgii, Kanady, Portugalii, Szwecji i oczywiście przedstawiciele z Polski, m.in.: z Akademii Pożarniczej, Centralnej Szkoły PSP w Częstochowie, Politechniki Morskiej w Szczecinie, Policji pomorskiej, Akademii Policji w Szczytnie, a także ratownicy specjalistycznych grup ratownictwa wodno-nurkowego Państwowej Straży Pożarnej, Morskiej Służby Poszukiwania i Ratownictwa, Państwowej Straży Rybackiej, Wojsk Obrony Terytorialnej, Grupy Krynickiej GOPR, Polskiego Związku

Fot. 1. Prezentacja sprzętu ratowniczego podczas konferencji.

Fot. 2.

Fot. 3.

Fot. 2–3. Prezentacja sprzętu ratowniczego podczas konferencji.

Surfingu, przedstawiciele podmiotów uprawnionych do wykonywania ratownictwa wodnego, tj. Świętokrzyskiego WOPR, Żyrardowskiego Powiatowego WOPR, OSP Karwia, Wodnej Służby Ratowniczej, WOPR Oddział Żywiec i Miejskiego WOPR w Oświęcimiu. W ciągu trzech dni zajęć zaprezentowało się 23 wystawców, odbyły się 33 wykłady oraz kilkanaście warsztatów praktycznych z wykorzystaniem sprzętu wystawianego podczas części teoretycznej.

Pierwszy dzień konferencji „On Duty 2024” poświęcony był głównie wystawcom, którzy prezentowali swój sprzęt w holu Biblioteki Głównej Akademii Marynarki Wojennej oraz przedstawiali nowości i zalety tego sprzętu.

W tym dniu odbyły się również warsztaty na wielofunkcyjnym basenie szkoleniowym (z ruchomym dnem) Głównej Akademii Marynarki Wojennej, gdzie można było wypróbować w praktyce pływanie w składanych płetwach oraz przećwiczyć holowanie i wyławianie specjalistycznych fantomów basenowych.

Zaprezentowany został m.in. skuter podwodny (fot. 4) Seabob. To jednostka, która nie wymaga uprawnień do prowadzenia, a jej elektryczny napęd sprawia, że jest całko-

Fot. 4.

Fot. 5.

Fot. 6.

Fot. 7.

Fot. 8.

Fot. 9.

Fot. 4–9. Warsztaty na pływalni Akademii Marynarki Wojennej w Gdyni.

Fot. 4. Skuter podwodny typu Seabob.

Fot. 5. Płetwy składane (kompaktowe) Folding Fins.

Fot. 6. Hełm nurkowy wyposażony w układ oddechowy.

Fot. 7. Pneumatyczne sanie lodowe.

Fot. 8–9. Manekin Ruth Lee.


Fot. 10.

Fot. 11.

Fot. 10–11. Wykłady i prelekcje podczas konferencji.

wicie ekologiczna. Choć wygląda jak zabawka, może być wykorzystywana również w ratownictwie. Do jej najważniejszych cech należą zwinność w wodzie i jej niska masa – ok. 30 kg. Działa na zasadzie wypierania wody – woda zasysana jest przez silnie obracający się wirnik i wypychana do kanału pod wysokim ciśnieniem, dając tym samym siłę napędową.

Podczas warsztatów dużym zainteresowaniem wśród uczestników cieszyły się kompaktowe płetwy Folding Fins (fot. 5). Jest to produkt, który odbiega od tradycyjnych płetw z uwagi na swoją konstrukcję, dzięki czemu jest skierowany do każdego użytkownika – od rekreacyjnego nurkowania do w pełni profesjonalnego, jak to jest w przypadku jednostek specjalnych. Oprócz swej innowacji w składaniu płetwy te mają również 4-punktowy system dopasowania, co pozwala na wielostopniową regulację i pewne pozycjonowanie stopy płetwonurka. Płetwy zostały również skonstruowane zgodnie z zasadami biomimetyki, co daje im wysoki współczynnik wydajności przy bardzo niskim zapotrzebowaniu energetycznym.

Drugiego dnia konferencji odbyły się wykłady i prelekcje poświęcone głównie ratownictwu wodnemu, współpracy pomiędzy służbami pracującymi na akwenach oraz bezpieczeństwu i higienie pracy na statkach.

Szczególnie istotne z punktu widzenia instruktora prowadzącego szkolenia dla policji wodnej były wykłady dotyczące:

– bezpieczeństwa podczas eksploatacji szybkich łodzi,
– biomechanicznych przyczyn urazów u operatorów szybkich łodzi oraz sposobów zapobiegania im,
– bezpieczeństwa na lodzie w kontekście uprawiania i rozwoju sportów wodnych oraz zabezpieczania imprez na zamarzniętych zbiornikach (morsowanie),
– zastosowania najnowocześniejszych narzędzi w ochronie ciała przed hipotermią,
– ochrony sternika przed wychłodzeniem lub przegrzaniem poprzez zastosowanie odzieży ochronnej z nowoczesnych materiałów, a także ochrony głowy przez specjalistyczne kaski ochronne.

Niezwykle ciekawym prelegentem okazał się Mariusz Szymański, który choć z zawodu jest fryzjerem, techniką podwodną zajmuje się od ponad 20 lat. Jest m.in. konstruktorem składanych płetw Foldingfins, których używa kilka jednostek specjalnych na świecie. Bierze on udział w kilku projektach badawczych, m.in. dla Akademii Marynarki Wojennej w Gdyni pod nazwą: „Wieloczujnikowy system monitoringu portów morskich". W 2003 r. odbudował i przetestował Bojowy Pojazd Podwodny „Błotniak", który zaprezentował i omówił szczegółowo podczas konferencji.

Kontynuując tematykę podwodną, należy wspomnieć o prezentacji Michała Kosuta, który jest instruktorem nurkowania, a od 2001 r. zawodowo związany jest z rekreacyjną branżą nurkową. Przedstawił on systemy bezpieczeństwa podczas nurkowania w drugim pod względem głębokości kompleksie nurkowym na świecie, a pierwszym w Europie, tj. „Deepspot" w Mszczonowie, którego jest dyrektorem. Przybliżył ryzyko związane z działalnością w obszarze nurkowania rekreacyjnego zarówno z butlą, jak i na wstrzymanym oddechu. Podał stosowane przez nich rozwiązania zmniejszające ryzyko zdarzeń nurkowych i medycznych


Fot. 12.


Fot. 13.

Fot. 12–13. Manekin Ruth Lee do symulacji ratownictwa medycznego z treningiem medycznym.

Fot. 14.

Fot. 15.

Fot. 16.

Fot. 17.

Fot. 14–15. Specjalistyczne fantomy przeznaczone do ćwiczeń z ranami silnie krwawiącymi.

Fot. 16–17. Warsztaty z tzw. pakowania ran.

przy okazji operacji nurkowej, przybliżył procedury i postępowanie w takich przypadkach na podstawie własnych doświadczeń i zdarzeń w „Deepspot”.
Bardzo interesujące były również wykłady z pierwszej pomocy, w tym rozwiązania organizacji samych apteczek stosowanych przez służby, aplikacji Pierwszy Ratownik czy wykorzystanie pulsoksymetrii w ratownictwie medycznym. Uwagę przykuwały manekiny wykorzystywane do scenariuszy edukacyjnych stosowanych w ratownictwie wodnym i medycznym. Ich realistyczny wygląd, bezwładność i ciężar zapewniają realistyczne warunki treningów, pomagając osiągać lepsze wyniki w późniejszych, prawdziwych sytuacjach kryzysowych. Powłoka tych fantomów umożliwia im pływalność we wszystkich wodach, zarówno na pływalniach, jak i wodach otwartych, jak jeziora, rzeki czy wody morskie, pomagając

Fot. 18. Pojazd osobisty typu RYŚ.

Fot. 19. Pojazd Mule na gąsienicach służący m.in. do wodowania jednostek pływających bezpośrednio z plaży.

Fot. 20. Ponton z silnikiem doczepnym.

Fot. 21. Fantom Ruth Lee.

Zdjęcia: Kinga Czerwińska.

utrzymać ciało w odpowiedniej pozycji sugerującej tonięcie. Manekiny pozwalają ćwiczyć umiejętności ratowania w przypadku zalania płuc oraz suchego tonięcia.
Jedno z ostatnich wystąpień tego dnia dotyczyło ryzyka, jakie niesie ze sobą praca służb, w których misją najwyższą jest ratowanie życia innych, czyli: wypalenia zawodowego, depresji, stresu. Temat szczegółowo omówił, także na swoim przykładzie, dr Marek Dąbrowski, który jest współpomysłodawcą i współtwórcą programu ECMO, czyli pozaustrojowego wspomagania funkcji życiowych. Jego prezentacja porównywała ratowników do postaci superbohaterów, którzy nie są wolni do strachu i lęku. Przytoczył badania Christiny Maslach, profesor psychologii Uniwersytetu Kalifornijskiego, która stwierdziła, że na wypalenie zawodowe najbardziej narażone są osoby, których praca wymaga intensywnych zadań, jak np. nauczyciele, lekarze, pracownicy mundurowi i ratownicy. Przeanalizował przyczyny powstawania tego syndromu, jego wpływ na codzienne życie i objawy oraz przekazał strategie radzenia sobie z nim poprzez akceptację i zrozumienie emocji, które są naturalne i nieodzowne w naszym życiu. Zaakcentował potrzebę stosowania odpowiednich technik, czyli medytacji, aktywności fizycznej i otwartej komunikacji, aby odpowiednio kontrolować emocje prowadzące do stanu wypalenia zawodowego. Przypomniał również o roli, jaką powinien spełniać pracodawca w przeciwdziałaniu wypaleniu zawodowemu u swych pracowników.
Kolejną prezentację wygłosił Michał Baranowski, strażak prowadzący kampanię edukacyjną „RatoPasy". Okazuje się, że ratownicy, niosąc pomoc innym, często zapominają o własnym bezpieczeństwie – strażacy, ratownicy, policjanci nie zapinają pasów, jadąc na wezwanie. W policyjno-wodniackim środowisku dotyczy to nienakładania kamizelek asekuracyjnych podczas pływania łodzią służbową. Prelegent przedstawił statystyki, z których jednoznacznie wynika, że tylko 10% strażaków zapina pasy podczas jazdy na akcję. Jest to o tyle przerażające, że najczęstszą przyczyną zgonów w czasie służby są właśnie wypadki drogowe. Przypomina się stara maksyma mówiąca, że „dobry ratownik to żywy ratownik".
W tym dniu odbyły się również warsztaty z pierwszej pomocy na polu walki, tj. zaopatrywania silnie krwawiących ran przy użyciu najnowszych trenażerów do pakowania ran. Warsztaty te przeprowadził Dariusz Rogoziński, twórca „czerwonej taktyki" (ewakuacji medycznej i udzielania pierwszej pomocy członkom grup specjalnych na polu walki) w Polsce, który doświadczenie na polu walk zdobył, służąc w Samodzielnym Pododdziale Antyterrorystycznym Policji we Wrocławiu. Tym bogatym doświadczeniem w zwalczaniu terroru kryminalnego w Polsce podzielił się w wystąpieniu pt. „Jak przeżyć zamach terrorystyczny".
Podczas trzeciego dnia – typowo warsztatowego – można było zaznajomić się w praktyce z nowinkami technologicznymi oraz wypróbować najnowszą odzież ochronną, prowadzenie łodzi z technicznymi nowościami i poruszanie się pojazdem osobistym w wersji taktycznej typu ATV.
Uczestnictwo w tej konferencji pozwoliło autorce, policjantce Zespołu Policji Wodnej CSP, na zdobycie wiedzy i wymianę doświadczeń z przedstawicielami służb i instytucji działających w zakresie ratownictwa wodnego oraz na zapoznanie z nowoczesnymi trendami w ratownictwie na całym świecie.

Summary

The Water Rescue Conference "On Duty"

The author of this article, a policewoman of the Water Police Team of the Special Training Unit at the Police Training Centre in Legionowo, brings closer the most important information about the Water Rescue Conference „On Duty", which she attended on 24–26 May 2024. The conference was aimed at exchanging experience and developing cooperation in order to increase the effectiveness of water rescue and improve the safety on water and in adjacent areas. It was attended by, among others, representatives of services, schools and universities, companies and institutions related to water rescue, including foreign ones. Specialized equipment for water rescue was presented by over 20 exhibitors. The event encompassed two days of lectures, talks and workshops in the facilities of the Naval Academy in Gdynia, and the third day – demonstrations and practical testing equipment on the waters of the Puck Bay.

Tłumaczenie: Katarzyna Olbryś

Wykorzystanie SKUTERA WODNEGO w pracy policji wodnej

Fot. 1. Skuter wodny. Zdj. K. Czerwińska.

kom. Kinga Czerwińska

Zakład Szkoleń Specjalnych CSP

Zapewnienie bezpieczeństwa na obszarach wodnych przez Policję wymaga zarówno odpowiednich umiejętności funkcjonariuszy, jak i wyposażenia w odpowiedni sprzęt. Takie cechy skuterów wodnych jak m.in.: małe rozmiary, niewielkie zanurzenie, duża prędkość, ekonomika eksploatacji oraz możliwość doposażenia w platformę ratowniczą sprawiły, że coraz częściej są one wykorzystywane przez policyjnych „wodniaków". W 2019 r. w Komisariacie Wodnym Policji w Poznaniu wprowadzono pierwsze skutery wodne w policyjnych barwach – szybkie i zwinne jednostki o napędzie strugowodnym. Pod koniec roku 2023 było ich już kilkanaście na całą Polskę, w tym 2 skutery w Centrum Szkolenia Policji w Legionowie – w Bazie Szkoleniowej w Kalu.

WSTĘP

Ochrona bezpieczeństwa i porządku publicznego m.in. na wodach przeznaczonych do powszechnego korzystania jest jednym z podstawowych zadań Policji[1]. Służbę na wodach i terenach przywodnych pełnią policjanci komisariatów wodnych Policji, komórek wodnych Policji lub policjanci wyznaczeni z innych jednostek i komórek organizacyjnych Policji[2]. Do ich zadań należy m.in.: zapewnienie bezpieczeństwa kąpiących się, pływających i uprawiających sporty wodne, niesienie pomocy tonącym, prowadzenie akcji ratowniczych i poszukiwawczych, ściganie i zatrzymywanie sprawców przestępstw i wykroczeń, kontrola organizatorów imprez, a także dróg wodnych, w tym ochrona przyrody i środowiska naturalnego[3].

O ile realizacja zadań Policji w zakresie bezpieczeństwa i porządku może odbywać się przy wykorzystaniu wszystkich dostępnych sił, o tyle zadania na wodach realizują policjanci posiadający specjalistyczne kwalifikacje i przeszkolenie. Zadania policji wodnej na wodach śródlądowych, morskich i terenach nadmorskich realizuje pięć komisariatów specjalistycznych Policji – w Warszawie, Krakowie, Poznaniu, Wrocławiu i Gdańsku – oraz 6 komórek wodnych – na terenie województwa kujawsko-pomorskiego (w Bydgoszczy, Toruniu, Włocławku), mazowieckiego (w Radomiu), warmińsko-mazurskiego (w Olsztynie) i zachodniopomorskiego (w Szczecinie). Są to nieetatowe zespoły działające przede wszystkim w sezonie letnim.

Wypełnianie przez policję wodną obowiązków, do których należy m.in. dbanie o bezpieczeństwo osób przeby-

wających nad wodą, niesienie pomocy tonącym, ochrona środowiska, kontrola wałów przeciwpowodziowych, akcje ratownicze podczas katastrof i klęsk żywiołowych, wymaga korzystania ze specjalistycznego sprzętu. Gdy powstawały pierwsze struktury policyjne w niepodległej Polsce, po 123 latach zaborów, policjantom wodnym wystarczały łodzie pychowe z niewielkimi doczepnymi silnikami. Jednakże szybkie zmiany w technologii oraz coraz nowsze sposoby rozrywki i spędzania wolnego czasu na wodzie wymusiły ewolucję, a raczej rewolucję w wyposażeniu policyjnych jednostek wodnych. Dzisiaj policjanci wodni, oprócz łodzi motorowych, mają do dyspozycji również samochody terenowe i osobowe (także o napędzie elektrycznym), quady, poduszkowce, łodzie o napędzie śmigłowym, a nawet rowery i drony, czyli bezzałogowe statki powietrzne. W 2019 r. w Komisariacie Wodnym Policji w Poznaniu wprowadzono pierwsze skutery wodne w policyjnych barwach – szybkie i zwinne jednostki o napędzie strugowodnym. Od tego czasu coraz więcej takich jednostek pojawia się we flocie poszczególnych komisariatów i jednostek wodnych. Pod koniec roku 2023 było ich już kilkanaście na całą Polskę, w tym 2 skutery w Centrum Szkolenia Policji w Legionowie – w Bazie Szkoleniowej w Kalu.

HISTORIA SKUTERÓW

Skuter wodny to nic innego jak rodzaj motorówki, służącej początkowo do uprawiania sportu i rekreacji. Pierwsze skutery o nazwie Amanda Water Scooter wyprodukowała brytyjska firma Vincent Motorcycle Company już w roku 1955. Była to jednoosobowa maszyna z silnikiem o pojemności 200 cm^3. Jednakże firma upadła, zanim uruchomiła w pełni produkcję swojego wynalazku[4].

Po kilku latach prób konstruowania skuterów, związanych zarówno z wyborem materiału do budowy kadłuba, jak i z wykorzystaniem rodzaju napędu, pod koniec lat 70. ubiegłego wieku firma Bombardier, doświadczona w produkcji skuterów śnieżnych, wyprodukowała skuter See Doo. Niestety i ten prototyp nie spełnił wymagań, które przed nim stawiano. Produkcję pierwszego stojącego skutera, z silnikiem o pojemności 400 cm^3, rozpoczęto dopiero w roku 1974, kiedy to uważany za ojca skutera wodnego, Clayton Jacobsen II, uzyskał patent na napęd strugowodny i podpisał umowę z japońską firmą Kawasaki[5].

Pierwsza produkcja otworzyła furtkę dla rozwoju i produkcji różnych tego typu pojazdów poruszających się na wodzie za pomocą napędu strugowodnego. Skutery ewoluowały pod względem pojemności silnika, techniki poruszania się na nich (ze stojących do siedzących) i liczby miejsc (dwu- i trzyosobowych). W latach 90. ubiegłego wieku silniki dwusuwowe ustąpiły miejsca czterosuwowym, czyniąc skutery wodne łatwiejszymi w eksploatacji. Ciągłe zmiany technologii i trendy światowe, m.in. w ekologii, wyznaczyły nowy kierunek dla rozwoju skuterów wodnych. Obecnie dostępne są już skutery o napędzie elektrycznym, które wcale nie ustępują miejsca tym spalinowym (fot. 2). Eksperymentu z zastosowaniem silnika elektrycznego w skuterze wodnym podjął się węgierski start-up, Narke Jet Ltd. W 2018 r. na targach Cannes Yachting Festival zaprezentował prototyp swojego PWC (Personal Watercraft), model Narke Electrojet GT45[6]. Moc silnika to 71 kW, co zapewnia rozwijanie maksymalnej prędkości 75 km/h i umożliwia 1,5 godziny niezapomnianych wrażeń na wodzie.

Zalety skuterów wodnych, czyli ich niewielkie zanurzenie, duża zwrotność oraz przyspieszenie, sprawiły, że zaczęto wykorzystywać je nie tylko do zabawy, ale również do ratownictwa wodnego. W latach 90. jedna z czołowych zawodniczek mistrzostw świata w skuterach wodnych Shawn Alladio w Kalifornii (fot. 3) zainicjowała wykorzystanie skuterów w ratownictwie przy zabezpieczaniu wyścigów skuterowych. Tak powstała K38 – organizacja o zasięgu międzynarodowym, która wyznaczyła standardy ratownictwa skuterowego na świecie[7].

Fot. 2. Skuter elektryczny Narke GT95.
Źródło: A. Rejs, *Narke GT95 – elektryczny skuter*, //yachtsmen.eu/wp-content/uploads/2021/03/Narke8-2.jpg / [dostęp: 18.01.2024 r.].

Fot. 3. Shawn Alladio K38.
Źródło: SurferToday, *Shawn Alladio: the discreet woman who saves big wave surfers*, https://www.surfertoday.com/surfing/shawn-alladio-the-discreet-woman-who-saves-big-wave-surfers [dostęp: 12.06.2024 r.].

SKUTERY WODNE W RATOWNICTWIE WODNYM W POLSCE

Ratowanie tonącego to wielkie zagrożenie dla osoby, która się tego podejmie. Woda to żywioł, a różnorodność akwenów wpływa na wiele zmiennych podczas akcji ratunkowej. Aby szlachetna postawa podczas udzielania pomocy osobie w wodzie nie zakończyła się poświęceniem własnego życia przez ratownika, niezbędna jest nie tylko znajomość problematyki, odpowiednie wyszkolenie, ale również sprzęt. Na to, czy akcja się powiedzie, ma wpływ wiele czynników. Najważniejszy z nich to czas.

Skutery w ratownictwie wodnym pojawiły się na początku XXI w. i są coraz bardziej popularne, a na niektórych akwenach wręcz niezbędne. Szczególnie wymagające zbiorniki wodne z rejonami tzw. płytkowodzia – jak np. plaże nadmorskie, potrzebują zastosowania sprzętu o wyjątkowych możliwościach. Użycie skuterów wodnych pozwala na pływanie z dużą prędkością po wodach o niskim stanie, co umożliwia sprawne podjęcie akcji i bezpieczną ewakuację osób z wody. Dzięki dodatkowemu wyposażeniu skutera w platformę ratowniczą zespoły ratownicze działają z jeszcze większą skutecznością. Pierwsze specjalistyczne szkolenie dla ratowników z wykorzystaniem skuterów odbyło się w 2008 r. w Rowach. Szkolenie to przeprowadzone zostało przez włosko-polską kadrę instruktorską – operatorów K38[8].

Obecnie prowadzone są centralne szkolenia specjalistyczne WOPR, tzw. ratownictwo z użyciem skutera wodnego. Szkolenie to trwa 22 godziny dydaktyczne. Zakres szkolenia obejmuje:

- budowę skutera oraz zasady manewrowania jednostką,
- wyposażenie osobiste operatora K38 oraz skutera ratowniczego,
- przygotowanie skutera do pracy oraz jego obsługę eksploatacyjną,
- wodowanie skutera,
- równowagę i balans na skuterze,
- techniki ratowania poszkodowanego aktywnego i pasywnego z użyciem skutera ratowniczego,
- symulowane akcje ratownicze z użyciem skutera ratowniczego.

Po ukończonym szkoleniu i zdanym egzaminie kursant zdobywa międzynarodowy certyfikat operatora skutera ratowniczego K38 Rescue International (poziom 3).

W ratownictwie skuterowym najlepiej sprawdzają się jednostki trzyosobowe. Wpływa na to ich duża stateczność na wodzie oraz wystarczająca ilość miejsca dla załogi. O ile marka skutera nie ma znaczenia, to jego moc jak najbardziej. Doświadczeni instruktorzy z LifeGuard

Fot. 4. Skutery z platformami ratowniczymi w Bazie Szkoleniowej w Kalu.
Zdj. K. Czerwińska.

Gdynia stwierdzają, że 100 KM to minimalna wartość dla zapewnienia wystarczającej mocy nautycznej jednostki motorowej. Dodatkowym elementem przy skuterze ratowniczym jest możliwość podpięcia platformy ratowniczej (LIFESLED), którą można zastosować w każdych warunkach (ma dużą wyporność oraz absorbuje wibracje podczas płynięcia), a także w ratownictwie lodowym i surfingowym.

SKUTERY W POLICJI POLSKIEJ

Ogólna charakterystyka skuterów wodnych w Policji

Pierwsze skutery wodne w Policji pojawiły się w Komisariacie Rzecznym Policji w Warszawie, ale wyłącznie na zasadach testowania ich przydatności do służby, i były to skutery firmy Yamaha. Nigdy jednak nie weszły do floty stołecznego komisariatu specjalistycznego. Dopiero w 2009 r. dwa skutery wodne Yamaha VX z platformami ratowniczymi wzbogaciły flotę szkoleniową Centrum Szkolenia Policji w Legionowie. Od tego czasu skutery wodne zaczęły zasilać poszczególne komendy wojewódzkie Policji. I tak na koniec roku 2023 były:

– 2 skutery w Komendzie Wojewódzkiej Policji w Szczecinie,
– 1 skuter w Komendzie Wojewódzkiej Policji w Olsztynie,
– 2 skutery w Komendzie Wojewódzkiej Policji w Bydgoszczy,
– 2 skutery w Komendzie Wojewódzkiej Policji w Białymstoku,
– 2 skutery w Komendzie Wojewódzkiej Policji w Poznaniu,
– 1 skuter w Komendzie Wojewódzkiej Policji zs. w Radomiu,
– 2 skutery w Komendzie Wojewódzkiej Policji we Wrocławiu,
– 2 skutery w Centralnym Pododdziale Kontrterrorystycznym Policji „BOA" Komendy Stołecznej Policji w Warszawie,
– 2 skutery w Centrum Szkolenia Policji w Legionowie, w Bazie Szkoleniowej w Kalu.

Jeśli chodzi o specyfikację policyjnych skuterów wodnych, to nie jest ona jednolita. W policyjnej flocie mamy skutery firmy Yamaha (10 sztuk) oraz SeaDoo Bombardier (6 sztuk). Prawie każdy skuter ma inną specyfikację, jeśli chodzi o model, pojemność silnika, moc silnika oraz liczbę miejsc czy udźwig. Jednakże moc silnika we wszystkich skuterach wykorzystywanych w Policji nie jest mniejsza niż 100 KM, tj. ok 74 kW. Skuter używany w ratownictwie powinien posiadać dostateczną moc – 100 KM zapewnia wystarczające właściwości nautyczne jednostki motorowej[9].

Niezbędne uprawnienia do kierowania skuterami wodnymi w Policji

Głównym i niezbędnym uprawnieniem do pełnienia służby na wodzie w Policji jest patent żeglarski młodszego stermotorzysty. Uprawnienie to może zostać uzyskane poza służbą lub w ramach kursu specjalistycznego prowadzonego dla policjantów wykonujących zadania na terenach wodnych i przywodnych w Centrum Szkolenia Policji w Legionowie. Stermotorzysta żeglugi śródlądowej to osoba, która w imieniu armatora (właściciela) kieruje statkiem i załogą, nadzoruje i odpowiednio ponosi odpowiedzialność za statek, przewożone osoby i ładunek oraz bezpieczeństwo żeglugi. Patent żeglarski stermotorzysty żeglugi śródlądowej uprawnia do kierowania tzw. małym statkiem (w tym skuterem wodnym) oraz łodzią przewozową o napędzie mechanicznym. Jest to patent zawodowy na wodach śródlą-

Fot. 5. Skuter na wyposażeniu Bazy Szkoleniowej w Kalu. Zdj. K. Czerwińska.

Fot. 6. Skuter wodny KWP Olsztyn, KPP w Giżycku. Źródło: Komenda Powiatowa Policji w Giżycku, *Czerwcowy weekend na wodzie. Podsumowanie*, https://gizycko.policja.gov.pl/o06/aktualnosci/106762,Czerwcowy-weekend-na-wodzie-Podsumowanie.html [dostęp: 18.01.2024 r.].

Fot. 7. Skutery wodne o mocy silnika 230 KM. Źródło: I. Liszczyńska, *KWP – Policyjni wodniacy na skuterach*, https://www.policja.pl/pol/aktualnosci/177752,KWP-Policyjni-wodniacy-na-skuterach.html [dostęp: 12.06.2024 r.].

Fot. 8. Ćwiczenia z platformą ratowniczą podczas kursu w Bazie Szkoleniowej w Kalu. Zdj. K. Czerwińska.

dowych wydawany przez urzędy żeglugi śródlądowej, co różni go od patentu sternika motorowodnego, który jest patentem amatorskim wydawanym przez Polski Związek Motorowodny i Narciarstwa Wodnego.

W ramach szkoleń dla policjantów wodnych, tj. kursu specjalistycznego dla policjantów wykonujących zadania na wodach i terenach przywodnych oraz kursu specjalistycznego dla policjantów prowadzących łodzie służbowe w trudnych warunkach atmosferycznych, przeprowadzane są zajęcia z obsługi i manewrowania skuterem wodnym wraz z platformą ratowniczą. Stanowią one jednak niewielką część poszczególnych kursów.

Dla porównania w ratownictwie wodnym prowadzone są centralne szkolenia specjalistyczne, w tym szkolenie z zakresu ratownictwa z użyciem skutera ratowniczego na poziomie stażysty bądź operatora[10]. Szkolenie to obejmuje 22 godziny dydaktyczne w 3-dniowym systemie szkolenia, a jego celem jest przygotowanie ratownika do wykonywania działań w zakresie ratownictwa wodnego z użyciem skutera ratowniczego w stopniu potrzebnym do udzielenia pomocy na akwenach wodnych. Szkolenie obejmuje nauczanie i doskonalenie technik ratowniczych nieobjętych programami kursów na poszczególne stopnie ratownicze. Absolwent tego szkolenia, po jego pozytywnym zaliczeniu według karty umiejętności, uzyskuje specjalizację operatora skutera ratowniczego i jest przygotowany do wykonywania zadań z zakresu ratownictwa wodnego przy użyciu skutera ratowniczego, a w szczególności do:

1) pełnienia funkcji operatora skutera ratowniczego:
   a) posługiwania się skuterem z platformą lub bez niej podczas akcji ratunkowej,
   b) kierowania zespołem ratowniczym podczas akcji ratunkowej;
2) znajomości zasad:
   a) prowadzenia skutera z platformą i bez niej,
   b) manewrowania skuterem w różnych warunkach hydrologicznych,
   c) przygotowania skutera do postoju chwilowego, nocnego i zimowania,
   d) przygotowania skutera do transportu,
   e) wydawania poleceń i komend jako kapitan statku,
   f) autoratownictwa.

Absolwent posiada wiedzę i umiejętności w zakresie:

1) autoratownictwa i autoasekuracji;
2) udzielania pierwszej pomocy zgodnie z ustawą z dnia 8 września 2006 r. o Państwowym Ratownictwie Medycznym (Dz. U. z 2024 r. poz. 652);
3) prowadzenia działań ratowniczych w ramach systemu KSRG, Państwowego Ratownictwa Medycznego i innych systemów bezpieczeństwa państwa;
4) zasad współpracy z podmiotami używającymi jednostek pływających[11].

Zalety i wady skuterów wodnych oraz ich przydatność w Policji[12]

Jednostki, które na swoim wyposażeniu posiadają skutery wodne, bardzo pozytywnie je oceniają. Do najczęściej wymienianych zalet należą:

– z uwagi na niewielkie rozmiary skutery wodne mogą być sprawnie przemieszczane z miejsca na miejsce i wodowane niemal w każdym miejscu, co wpływa na usprawnienie patrolowania akwenów mniej dostępnych;
– niewielkie zanurzenie jednostki, specyfika strugowodnego napędu, a także mobilność i zwrotność pozwalają na wykorzystanie skuterów na wodach o niskim stanie wody;
– szybkość przemieszczania się jednostki pozwala na adekwatną reakcję na popełniane wykroczenia i przestępstwa;
– skuter może być wykorzystywany w trudnych warunkach atmosferycznych i wymagających akwenach z uwagi na zafalowanie, prądy czy pływy;
– skuter wyposażony w platformę ratowniczą podnosi efektywność i skuteczność akcji ratowniczej;
– skutery wodne są oszczędne w eksploatacji, jeśli chodzi o zużycie paliwa.

Z wad natomiast wymieniane są najczęściej:
– duże wymagania w zakresie umiejętności od sternika poruszającego się na skuterze;
– duże zmęczenie fizyczne sternika przy dłuższym użytkowaniu oraz mniejszy komfort użytkowania przy skrajnych warunkach atmosferycznych;
– zwiększone ryzyko zamoczenia lub utracenia niezbędnych podczas służby przedmiotów, jak notatnik służbowy, bloczek mandatowy itp. z uwagi na brak możliwości ich zabezpieczenia (małe i nieszczelne bakisty);
– brak centralnych szkoleń zawodowych (policyjnych) dla operatorów skuterów wodnych;
– brak uregulowań prawnych (policyjnych) umożliwiających wyposażenie funkcjonariuszy wykonujących zadania służbowe na skuterach wodnych (tj. w pianki, buty i rękawice neoprenowe, kaski itp.).

WNIOSKI

Praca policji wodnej nierozerwalnie związana jest z udzielaniem pomocy osobom tonącym. Woda jednak to nieobliczalny żywioł. Aby nieść ratunek w obliczu zagrożenia, niezbędne są nie tylko umiejętności, ale również odpowiedni sprzęt. O powodzeniu akcji ratunkowej w dużej mierze decyduje również czas, którego upływ działa na niekorzyść tonącego. Dla osoby udzielającej pomocy w wodzie takie wyzwanie to ogromny wysiłek fizyczny i psychiczny. Aby zminimalizować obciążenie wynikające z tych czynników, konieczne jest ciągłe doskonalenie, treningi pływackie oraz wyposażenie techniczne ratownika/policjanta. Pojawienie się skuterów wodnych zrewolucjonizowało wodniacki „światek". Za tymi zmianami podąża ratownictwo wodne, dostosowując się do wymagań, jakie się przed nimi pojawiły.

Wydaje się, że wyposażenie jednostek wodnych w skutery wodne jest wręcz pożądane, aby skutecznie dostosować organy ścigania do szybkiego rozwoju turystyki motorowodnej, a także aby zapewnić najwyższe standardy bezpieczeństwa na wodach ogólnodostępnych. Należy uwzględnić tu nie tylko ujednolicenie sprzętu oraz niezbędne dodatkowe wyposażenie, włączając w to strój ochronny, ale również odpowiednie wyszkolenie na poziomie centralnym.

[1] Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2024 r. poz. 145), art. 1 ust. 2 pkt 2.
[2] Zarządzenie nr 1386 Komendanta Głównego Policji z dnia 17 listopada 2009 r. w sprawie metod i form wykonywania zadań przez policjantów pełniących służbę na wodach i terenach przywodnych (Dz. Urz. KGP z 2013 r. poz. 71), § 3.
[3] Tamże, § 6.
[4] Wynalazki i odkrycia, *Skuter wodny*, https://wynalazki.andrej.edu.pl/wynalazki/32-s/1375-wodny [dostęp: 18.01.2024 r.].
[5] M. Matejowski, A. Jarosiewicz, J. Friedenberger, *Ratownictwo wodne z użyciem skutera wodnego*, Słupsk–Gdynia 2010, s. 12.
[6] A. Rejs, *Narke GT95 – elektryczny skute*r, https://yachtsmen.eu/2021/narke-gt95-elektryczny-skuter/ [dostęp: 18.01.2024 r.].
[7] M. Matejowski, A. Jarosiewicz, J. Friedenberger, *Ratownictwo wodne z użyciem skutera wodnego*, s. 13.
[8] Tamże, s. 5–6.
[9] Tamże, s. 25.
[10] WOPR, *Centralne szkolenia specjalistyczne WOPR, patenty i uprawnienia przydatne w ratownictwie wodnym*, http://zgwopr.eu/images/Zestawienie_CSS_i_Patentow.pdf [dostęp: 4.03.2024 r.].
[11] WOPR, *Program szkolenia przygotowującego specjalistę operator skutera ratowniczego,* http://zgwopr.eu/images/PROGRAMY_CSS/05.2._Program_szkolenia_Ratownik_na_skuterze_z_platform%C4%85_-08.pdf [dostęp: 4.03.2024 r.].
[12] Wiedzę na temat przydatności skuterów wodnych w Policji, ich zalet i wad zaczerpnięto z opinii koordynatorów wodnych poszczególnych komend oraz instruktorów Zespołu Wodnego Zakładu Szkoleń Specjalnych Centrum Szkolenia Policji w Legionowie.

Summary

The use of a water scooter in the work of water police

The work of the water police is inextricably linked with providing assisstance to drowning people. However, water is an incalculable element. In order to bring rescue in the face of danger, not only skills are necessary, but also the right equipment. Equipping water units with water scooters is even desirable to effectively adapt law enforcement agencies to the rapid development of motorboat tourism, as well as to ensure the highest safety standards on public waters. Except for motorboats, water policemen use cars, ATVs, hovercraft, propeller-driven boats, and even bicycles and drones. In 2019, the first water scooters in police colors – fast and agile jet-propelled craft – were introduced at the Water Police Station in Poznan. By the end of 2023, there were more than a dozen of them for the whole of Poland, including 2 scooters at the Police Training Center in Legionowo – at the Training Centre in Kal.

Tłumaczenie: Katarzyna Olbryś

BEZPIECZEŃSTWO OSOBISTE PRZEWODNIKA PSA

podczas tropienia śladów ludzkich

Fot. 1. Przewodnik z psem służbowym podczas tropienia śladów ludzkich. Zdj. P. Mrozowski.

podkom. Piotr Mrozowski
Zakład Kynologii Policyjnej CSP

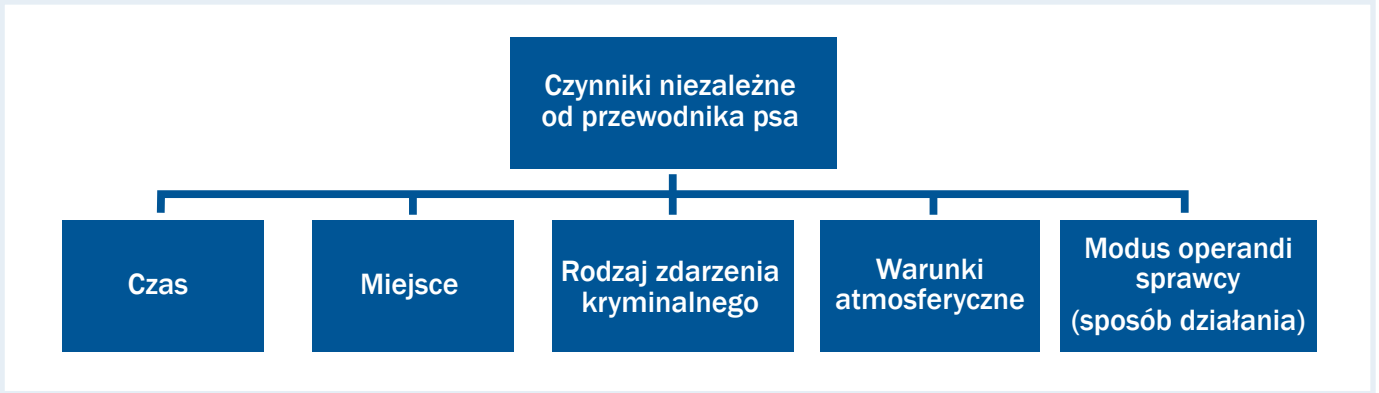
asp. szt. Daniel Tatera
Zakład Kynologii Policyjnej CSP

O tym, że pies służbowy zwiększa bezpieczeństwo osobiste policjanta, wiadomo nie od dziś. Już pierwsi polscy kynolodzy policyjni[1] zauważali ten fakt. Psy w polskiej Policji pojawiły się właśnie po to, by poprawić bezpieczeństwo funkcjonariuszy. Już w 1922 r. pisano o tym w ten sposób:
Zadania psa policyjnego jako środka pomocniczego w służbie bezpieczeństwa publicznego w ogólności są: Podniesienie pewności przewodnika, podniesienie zdolności wpływu na publiczność, powstrzymanie od usiłowania przestępstwa...[2]

Posiadanie nawet najlepiej wyszkolonego psa służbowego nie zwalnia policjanta od zachowania podstawowych zasad bezpieczeństwa. Tym bardziej, że samo prowadzenie psa – szczególnie kategorii patrolowo-tropiącej, czyli charakteryzującej się określonym poziomem nieufności i odruchów obrończych, wymaga szczególnej rozwagi i umiejętności.
Na gruncie współczesności warto zauważyć, że policjanci – przewodnicy psów oraz ich podopieczni są narażeni na różnego rodzaju zagrożenia, które mogą pojawić się podczas użycia psa służbowego. Zdefiniowanie taktyki bezpiecznego i skutecznego prowadzenia psa służbowego – czy to podczas tropienia śladów, czy przeszukania terenu – jest rzeczą bardzo trudną, głównie z powodu wielu czynników niezależnych od policjanta. Rozważania teoretyczne nie zastąpią tutaj doświadczeń praktycznych, co nie znaczy, że kwestie te nie powinny znaleźć odzwierciedlenia w literaturze adresowanej do współczesnych kynologów policyjnych.

ZABEZPIECZENIE OSOBOWE

Zgodnie z zarządzeniem nr 91 Komendanta Głównego Policji z dnia 4 października 2022 r. przez tzw. zabezpieczenie osobowe rozumiemy ogół osób uczestniczących w czynnościach tropienia śladów ludzkich, przeszukania terenu, przeszukania pomieszczeń[3] wspierających przewodnika psa.



Schemat 1. Czynniki niezależne od przewodnika psa na miejscu zdarzenia kryminalnego. Źródło: opracowanie P. Mrozowski.

Taktyka użycia psa w terenie otwartym (wiejskim, leśnym) różni się zasadniczo od taktyki użycia psa w terenie zurbanizowanym. Obydwa rodzaje użycia są jednak narażone na różne zagrożenia, które dzięki udziałowi osób ubezpieczających mogą zostać w znacznym stopniu zminimalizowane. Co istotne, zgodnie z obowiązującymi przepisami, przewodnik psa podczas wykonywania czynności jest bezpośrednio ubezpieczany przez co najmniej jednego policjanta. Zadania osoby ubezpieczającej czynności przewodnika psa zostały szczegółowo określone w ww. zarządzeniu KGP:

1) ostrzeganie przewodnika przed niebezpieczeństwem;
2) oznakowanie wykrytych miejsc ze śladami pobytu osób tropionych;

Fot. 2 i 3. Tropienie śladów ludzkich. Ubezpieczenie i asekuracja przewodnika przy ruchu ulicznym. Zdj. P. Mrozowski.

3) zabezpieczenie przed zniszczeniem przedmiotów odnalezionych przez psa na trasie tropienia i w miejscach przeszukania;
4) utrzymywanie łączności radiowej;
5) wykonywanie poleceń przewodnika, uzasadnionych zaistniałymi okolicznościami[4].

Ważne, by osoba ubezpieczająca przewodnika psa nie była osobą „przypadkową", uczestniczącą *ad hoc* w czynnościach. Chodzi raczej o osobę mającą świadomość swojej roli i odpowiedzialności w dość trudnym procesie tropienia śladów ludzkich. Sama definicja tropienia śladów nie jest dokładnie sprecyzowana w przepisach resortowych[5]. W dużym uproszczeniu mówimy o przemieszczaniu się psa węszącego zapach ludzki po tzw. ścieżce śladu[6]. Chodzi tu o podążanie za indywidualnym zapachem[7] wydzielanym przez osobę[8] przebywającą na miejscu zdarzenia i na trasie odejścia z miejsca zdarzenia. Mówimy zatem o konieczności podążania przez policjanta z psem w bliżej nieokreślone miejsca. Lokalizacje te mogą znajdować się bardzo blisko miejsca zdarzenia[9]. Mogą też być oddalone wiele kilometrów od niego. To właśnie ta niewiadoma wynikająca z użycia psa podczas tropienia śladów ludzkich i przemieszczania się w różne miejsca rodzi wiele implikacji.

Dobór osób ubezpieczających powinien odbywać się w sposób przemyślany. Przewodnik psa powinien uświadomić osobę ubezpieczającą o jej obowiązkach, a także o sposobie poruszania się po ścieżce śladu[10], zachowaniu wskazanej odległości od psa i sposobie postępowania w przypadku wystąpienia zagrożenia zewnętrznego[11] dla przewodnika czy psa. Tylko takie przygotowanie osoby do ubezpieczania przewodnika i psa podczas czynności może gwarantować sukces. Zgodnie z ww. zarządzeniem nr 91 Komendanta Głównego Policji[12] obecność osoby ubezpieczającej jest obligatoryjna. Warto w tym miejscu przypomnieć zapominane często uprawnienie do przybierania osób do czynności wynikające z przepisów policyjnych – konkretnie z art. 22 ust. 1 ustawy o Policji[13]:

Policja przy wykonywaniu swoich zadań może korzystać z pomocy osób niebędących policjantami. […]

Autorzy tego artykułu zachęcają, by na miejscach zdarzeń w trudnym terenie, np. bagiennym, leśnym, górzystym, korzystać z pomocy osób przybranych do czynności. Mogą to być okoliczni mieszkańcy znający doskonale teren, myśliwi, a także przedstawiciele różnych grup zawodowych –

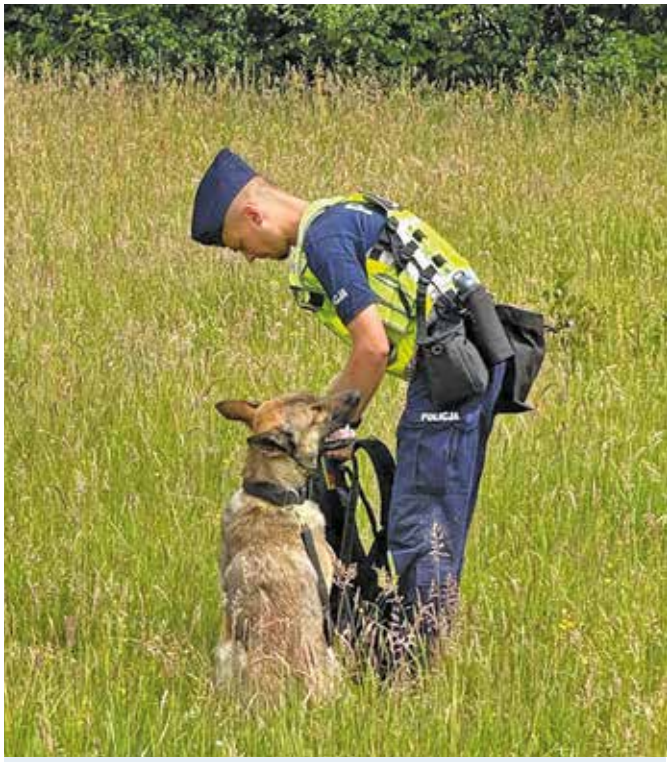
strażacy, leśnicy, wojskowi itp. Osoby te zazwyczaj są chętne do pomocy, znają okoliczną ludność, a przede wszystkim charakterystyczne miejsca w terenie – co w przypadku poszukiwania osób zaginionych ma niebagatelne znaczenie.
Warto się również zastanowić w tym miejscu, po co właściwie przewodnikowi potrzebna jest taka osoba? Przewodnik psa policyjnego kategorii tropiącej i patrolowo-tropiącej to osoba, której zadaniem jest użycie psa policyjnego na miejscu zdarzenia kryminalnego. Podczas tropienia śladów ludzkich przewodnik musi dobrać odpowiednią taktykę do zaistniałej sytuacji, a podczas samej czynności tropienia bacznie obserwować odruchy zwierzęcia. Potrzebna jest mu zatem pomoc, szczególnie w zakresie utrzymywania łączności radiowej, pomoc przy zabezpieczaniu odnalezionych przedmiotów, rozpytaniu napotkanych w trakcie tropienia świadków czy też w najtrudniejszej sytuacji, czyli doprowadzeniu przez psa do konkretnej osoby czy posesji. Odnalezienie tropionej osoby przez psa stanowi zawsze taktyczne wyzwanie, ponieważ kategorie odnajdywanych osób są różne. Mogą być to osoby zaginione – potrzebujące pomocy medycznej, nieporadne, nieprzytomne. Mogą być to również sprawcy zdarzeń kryminalnych – agresywni przy próbach ich zatrzymania. Udział osoby ubezpieczającej w tych czynnościach jest zatem konieczny, by zapewnić prawidłowy i bezpieczny przebieg czynności. Dodatkowo, pies tropiący ślad zapachowy oraz same działania policyjne z użyciem zwierząt zawsze wzbudzają duże zainteresowanie osób postronnych, osób mieszkających w pobliżu miejsca zdarzenia lub gapiów. Osoby te pomimo widocznych na obrożach napisów „Policja" niejednokrotnie próbują pogłaskać pracujące zwierzę, co może przerwać pracę psa oraz wywołać niepożądane odruchy bezwarunkowe zwierzęcia. Osoba ubezpieczająca ma ograniczyć takie wpływy osób postronnych na działania policjanta i psa. Niektórzy przewodnicy, świadomi zainteresowania zwierzęciem policyjnym, prewencyjnie umieszczają na obroży psa służbowego specjalne naszywki informujące, że jest to pies pracujący i nie należy mu przeszkadzać, a tym bardziej go głaskać[14].

ZABEZPIECZENIE TECHNICZNE

Prawidłowe prowadzenie psa wymaga odpowiedniego wykorzystania sprzętu służbowego. Przewodnicy psów policyjnych dysponują specjalistycznym sprzętem w postaci smyczy, lin i szorek z napisem „Policja".
W niektórych jednostkach organizacyjnych Policji psy tropiące są wyposażone w odbiorniki GPS pozwalające na określenie lokalizacji psa w terenie[15]. W kontekście zabezpieczenia technicznego warto wspomnieć o dodatkowym i zdaniem autorów niezbędnym wyposażeniu. Przewodnik psa powinien posiadać miniapteczkę[16], latarkę lub latarkę czołową, zapasowe baterie lub akumulatory[17] oraz co najmniej dwie kamizelki odblaskowe.

Fot. 4. Pies policyjny ze specjalną naszywką na obroży informującą o pracy psa. Zdj. D. Bartoszek.

Fot. 5 i 6. Tropienie w porze nocnej z osobą ubezpieczającą, z wykorzystaniem oświetlenia taktycznego. Zdj. P. Mrozowski.



Fot. 7. Przewodnik psa przygotowujący psa do tropienia śladów ludzkich, wyposażony w dodatkową kamizelkę odblaskową. Zdj. H. Wawrzkiewicz.

Kamizelki te mogą okazać się pomocne podczas długotrwałych działań nocnych. Jedną kamizelkę powinien nosić przewodnik psa, drugą osoba ubezpieczająca. Działanie takie zapewnia bezproblemowy kontakt wzrokowy nawet w trudnym terenie – szczególnie w nocy. Opisywane wyposażenie powinno zawierać również zapas wody umożliwiający napojenie psa podczas przerwy w tropieniu[18]. Do katalogu tego autorzy dodatkowo zaliczyliby fakultatywnie zwykły multitool[19]. To ostatnie narzędzie może być konieczne do użycia podczas przypadkowego zaplątania się psa w gęste krzaki, żywopłoty lub sidła (wnyki)[20] podczas działań w terenie leśnym. Statystki i dane z Lasów Państwowych pokazują, że takie zagrożenie jest nadal bardzo realne[21].

TAKTYKA I TECHNIKA PROWADZENIA PSA W RÓŻNYCH WARUNKACH TERENOWYCH

Głównym problemem związanym z omawianym tematem jest brak możliwości przewidzenia potencjalnego miejsca i czasu użycia psa służbowego. Podobnie trudno przewidzieć trasę tropienia – przemieszczania się psa czy jego zachowanie podczas przeszukania terenu leśnego. Na potrzeby niniejszego artykułu skupmy się na dwóch kryteriach podziału: użyciu psów w terenach polnych, leśnych i terenach miejskich. Zdefiniowanie taktyki według innych kryteriów wymagałoby osobnego opracowania.

TEREN LEŚNY, POLNY

Niewątpliwie teren polny, leśny jest prostszy do prowadzenia psa służbowego podczas czynności. W takim terenie wzrasta jednak realnie szansa napotkania dzikich zwierząt lub bezpańskich psów.

Ukształtowanie terenu to kolejny problem. Teren może być trudny, z dużą liczbą rozpadlin. Szczególnie niebezpieczne są niezabezpieczone studnie lub włazy do studzienek najczęściej na terenach opuszczonych, a także pustostany. Podobnie pokonywanie przeszkód terenowych, cieków wodnych na trasie tropienia może stanowić problem i autorzy zdecydowanie zalecają obejście przeszkody i próbę dokonania nawęszenia na wysokości miejsca, do którego doprowadził pies. W terenie takim dopuszczalne jest użycie psa na długiej linie. Jej długość i samą taktykę użycia przewodnik powinien dobrać zależnie do potrzeb.

Rozległe lasy to kolejne wyzwanie – szczególnie w kontekście poszukiwania osób zaginionych. Przemieszczanie

Fot. 8 i 9. Przykładowe wnyki i sidła stosowane przez kłusowników.

Źródło: Komenda Główna Policji, *Ochrona przyrody i przestrzeganie prawa to nasza wspólna odpowiedzialność*, https://policja.pl/pol/aktualnosci/244936,Ochrona-przyrody-i-przestrzeganie-prawa-to-nasza-wspolna-odpowiedzialnosc.html?search=29575360669059 [dostęp: 26.05.2024 r.].

Fot. 10 i 11. Tropienie śladów ludzkich w terenie polnym i leśnym. Zdj. P. Mrozowski.

się w takim terenie zwłaszcza przy dużej gęstości poszycia może stanowić problem, podobnie jak odnalezienie osób, rzeczy na trasie tropienia i konieczność podania dokładnej lokalizacji. Problemy te w dzisiejszych czasach znacznie zniwelowały mapy internetowe lasów państwowych[22]. Podobnie wiedza z zakresu poruszania się i orientowania w terenie leśnym powinna stanowić podstawę taktyki i techniki prowadzenia psa przez przewodnika.

Fot. 12 i 13. Słupek oddziałowy, podział lasu na sektory. Źródło: Polska przez weekend, *Co zrobić gdy zgubimy się w lesie? – podstawy orientacji w terenie leśnym*, https://polskaprzezweekend.pl/co-zrobic-gdy-zgubimy-sie-lesie/ [dostęp: 26.05.2024 r.].

TEREN MIEJSKI

W terenie miejskim wzrasta ryzyko zagrożeń podczas czynności. To, co było widoczne z daleka w terenie polnym, staje się niewidoczne. Zatem blok, obiekt, zaparkowany samochód stanowi miejsce potencjalnego przebywania osoby tropionej. W miejscu tym również można napotkać osoby postronne niezwiązane z czynnościami, często wychodzą nagle zza bloku lub z innych miejsc i nie są świadome prowadzenia działań policyjnych. Tylko dobór odpowiedniej taktyki prowadzenia psa do tych zastanych warunków środowiskowych na miejscu zdarzenia gwarantuje bezpieczeństwo prowadzonych czynności. W zasadzie czynność tropienia może zakończyć się wszędzie. Pies może doprowadzić do klatki schodowej, garażu, piwnicy, altanki śmietnikowej i wielu innych lokalizacji. W każdym z tych miejsc możliwe jest napotkanie osób przypadkowych, jak również poszukiwanych osób czy przedmiotów. Teren miejski to również miejsce wzmożonego ruchu ulicznego będącego potencjalnym zagrożeniem dla człowieka i psa. Szczególną ostrożność należy zachować przy pracy węchowej psa na pasach ruchu, przekraczaniu jezdni w trakcie tropienia śladów czy nawęszeń z pojazdów uczestniczących w zdarzeniach drogowych.

Tropienie śladów w takich warunkach przestrzennych powinno odbywać się ze szczególną rozwagą i świado-

Fot. 14 i 15. Tropienie śladów ludzkich w terenie miejskim. Zdj. P. Mrozowski.

Fot. 10. Asekuracja psa podczas tropienia śladów ludzkich. Zdj. H. Wawrzkiewicz.

mością zagrożeń. Istotna rola przypada w tym miejscu osobie ubezpieczającej, która – jak już było podkreślane wcześniej – ma zapewnić optymalne warunki do pracy przewodnika psa.

ZAKOŃCZENIE

Dobór odpowiedniej taktyki użycia psa do zdarzenia jest kluczem do sukcesu. Ważne jest również bezpieczeństwo osobiste policjanta i powierzonego mu zwierzęcia służbowego. Obligatoryjnie każdy przewodnik podejmujący czynności powinien być bezpośrednio ubezpieczany przez co najmniej jednego policjanta, a sama taktyka – czyli prowadzenie psa – musi być dobrana indywidualnie, w zależności od kontekstu zdarzenia. Niniejszy artykuł to próba ujęcia w zarysie kwestii bezpieczeństwa osobistego przewodnika psa podczas czynności tropienia, a także przybliżenie obowiązków spoczywających na osobach ubezpieczających te czynności.

[1] Mowa tu przede wszystkim o Alojzym Grimmie, Wiktorze Ludwikowskim i Janie Majewskim, P. Mrozowski, *Wiktor Ludwikowski. Zapomniany protoplasta kynologii policyjnej*, „Kwartalnik Policyjny" 2023, nr 3–4, s. 51.

[2] A. Grimm, *Jak używać psy policyjne*, Dom Książki Polskiej, Warszawa 1922, s. 18, https://polona.pl/item-view/fd5cd5ec-76c0-4495-86e9-f1e299e8cdf8?page=2 [dostęp: 10.07.2024 r.]. .

[3] Zarządzenie nr 91 Komendanta Głównego Policji z dnia 4 października 2022 r. w sprawie metod i form wykonywania zadań z użyciem psów służbowych w Policji (Dz. Urz. KGP poz. 225), § 40 ust. 1.

[4] Tamże, § 40 ust. 2.

[5] W myśl § 37 ust. 1 zarządzenia nr 91 KGP użycie psów do tropienia śladów ludzkich ma na celu ustalenie: drogi odejścia sprawcy z miejsca zdarzenia lub oddalenia się osoby zaginionej, miejsca ukrywania się sprawcy zdarzenia o charakterze kryminalnym lub miejsca pobytu osoby zaginionej, miejsca ukrycia lub porzucenia przedmiotów mających związek ze zdarzeniem lub ujawnienia śladów kryminalistycznych.

[6] Definicja ścieżki śladu wg Górnego to mieszanina widocznych (przedmiotów) i niewidocznych gołym okiem (łusek naskórka, kropelek potu) elementów pozostawionych przez człowieka poruszającego się w jakimś terenie, na ślad składają się także elementy terenu zmienione bądź uszkodzone na skutek kontaktu z człowiekiem (zgnieciona trawa, złamana gałązka), B. Górny *Nowoczesne szkolenie psów tropiących*, Multico Oficyna Wydawnicza, Warszawa 2004, s. 21.

[7] T. Jezierski, *Badania osmologiczne. Podstawy fizjologii węchu, uczenia się i etologii zwierząt*, „Zeszyty Metodyczne" 1999, nr 4, s. 16.

[8] Zapach człowieka stanowi indywidualny i niepowtarzalny bukiet zapachów, opadających w postaci molekuł zapachowych na podłoże. Na bukiet ten składają się zapachy wydzielane przez ciało człowieka w różnych stanach emocjonalnych i chorobowych, spożywane pożywienie, noszona odzież, stosowane kosmetyki czy zapachy powstałe w wyniku wykonywania określonego zawodu, G. Wiorowski, K. Lubryczyński, *Tresura psów służbowych. Tropienie śladów ludzkich,* Centrum Szkolenia Policji w Legionowie, Legionowo 2011, s. 8–9.

[9] Taktyka poszukiwań nakazuje niezwłocznie zorganizować i przeprowadzić penetrację terenu ostatniego miejsca pobytu osoby zaginionej i innych ustalonych miejsc, § 12 ust. 1 pkt 7 zarządzenia nr 48 Komendanta Głównego Policji z dnia 28 czerwca 2018 r. w sprawie prowadzenia przez Policję poszukiwania osoby zaginionej oraz postępowania w przypadku ujawnienia osoby o nieustalonej tożsamości lub znalezienia nieznanych zwłok oraz szczątków ludzkich (Dz. Urz. KGP poz. 77).

[10] Przemieszczanie takie powinno się odbywać co najmniej kilka do kilkunastu metrów za przewodnikiem, najlepiej w pobliżu linki od tropienia, która z reguły ciągnie się po podłożu za idącym przewodnikiem.

[11] Może być to przejeżdżający drogą samochód, dzikie zwierzę pojawiające się na ścieżce śladu czy osoba postronna wchodząca z boku na ścieżkę śladu, a niezauważona przez przewodnika.

[12] Zarządzenie nr 91 KGP, § 40 ust. 1: Podczas wykonywania czynności związanych z tropieniem śladów ludzkich, przeszukaniem terenu lub pomieszczenia, przewodnik jest bezpośrednio ubezpieczany przez co najmniej jednego policjanta.

[13] Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2024 r. poz. 145).

[14] Oznaczenia psa pracującego obligatoryjnie są stosowane do psów asystujących osobom niewidomym lub niedowidzącym oraz osobom niepełnosprawnej ruchowo. Oznaczenie takie ma formę widocznego naszycia na szorki psa „Pies asystujący w trakcie szkolenia" lub w przypadku psów wyszkolonych i posiadających stosowny certyfikat oznaczenie takie ma formę napisu „Pies asystujący", co wynika z § 12 ust. 1 i 2 rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 1 kwietnia 2010 r. w sprawie wydawania certyfikatów potwierdzających status psa asystującego (Dz. U. Nr 64, poz. 399).

[15] W obecnych czasach telefony wyposażone są w nadajniki GPS, więc monitorowanie trasy przemieszczania łatwo sprawdzić na różnego rodzaju aplikacjach do biegania czy tropienia.

[16] Wyposażoną w różnego rodzaju opatrunki, kleszczołapki czy wodę utlenioną do wywołania wymiotów w przypadku zatrucia psa.

[17] O oświetleniu taktycznym psa oraz konieczności posiadania zapasowych baterii przez przewodnika po raz pierwszy pisał A. Grimm w książce *Jak układać psy policyjne*, Warszawa 1921, s. 8, https://polona.pl/item-view/eccd3113-0ad9-474f-92a0-71281c65cd21?page=2 [dostęp: 10.07.2024 r.].

[18] Działanie takie jest ważne szczególnie w temperaturach powyżej 25 stopni Celsjusza oraz przy widocznych oznakach przegrzania organizmu zwierzęcia.

[19] Narzędzie wielofunkcyjne wyposażone w ostrze, śrubokręt oraz kombinerki.

[20] Pętla z drutu, linki stalowej bądź ze sznura zastawiana przez kłusowników na przesmykach (przejściach) zwierzyny tak, aby zwierzę musiało wejść w oko pętli zaciskającej wokół szyi lub tułowia i powodującej śmierć w męczarniach; narzędzie kłusownicze, Lasy Państwowe, *Wnyk, sidło*, https://www.lasy.gov.pl/pl/edukacja/slownik/w/wnyk-sidlo [dostęp: 11.10.2023 r.].

[21] E. Marszałek, *Kłusownictwo wciąż jest problemem*, https://www.lasy.gov.pl/pl/informacje/aktualnosci/klusownictwo-wciaz-jest-problemem [dostęp: 15.05.2024 r.].

[22] Lasy Państwowe, *Mapa lasów*, https://www.lasy.gov.pl/pl/nasze-lasy/mapa-lasow [dostęp: 26.05.2024 r.].

Summary

Personal safety of a dog handler while tracking human traces

The article roughly defines the issues of personal safety of a service dog handler while performing service tasks related to tracking human traces. It also outlines the tasks and requirements for persons who insure the activities of the dog handler during the handling of criminal events.

Tłumaczenie: Katarzyna Olbryś

Nazewnictwo i ewidencja psów służbowych

Fot. 2. REKRUT – pies służbowy Policji Państwowej. Źródło: „Na Posterunku" 1939, nr 25.

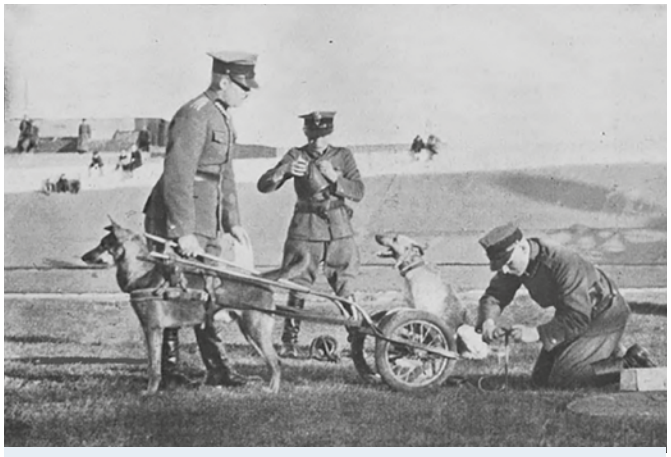
Fot. 1. Psy służbowe na kursie specjalistycznym dla przewodników psów patrolowo-tropiących do działania bez kagańca, który odbył się w Zakładzie Kynologii Policyjnej Centrum Szkolenia Policji w Legionowie na przełomie 2023 r. i 2024 r. Zdj. D. Bartoszek.

podkom. Piotr Mrozowski

Zakład Kynologii Policyjnej CSP

Dobór psów do użycia w Policji jest jednym z zadań realizowanych przez Zakład Kynologii Policyjnej Centrum Szkolenia Policji w Legionowie[1]. Realizacja tego zadania to wiele powiązanych czynności, które polegają m.in. na wyszukiwaniu i typowaniu psów do szkolenia, sprawdzeniu pod względem zdrowotnym, przeprowadzeniu prób charakteru oraz wycenie psów oferowanych do sprzedaży[2]. Na Zakładzie Kynologii Policyjnej Centrum Szkolenia Policji w Legionowie spoczywa też obowiązek elektronicznego oznakowania zakwalifikowanych[3] psów oraz obowiązek nadania psom imion służbowych. Obecnie przyjęte nazewnictwo psów służbowych w Policji jest dla nas oczywiste i mało kto zastanawia się, co spowodowało takie, a nie inne podejście do problematyki nazywania i ewidencjonowania zwierząt służbowych. Jednak geneza nazewnictwa psów policyjnych sięga aż do roku 1924, czyli 100 lat wstecz.

Ludzie od dawna traktowali psy jako swoich przyjaciół. W mentalności ludzkiej jest potrzeba nadawania nazw otaczającym przedmiotom i ulubionym zwierzętom. Imiona nadawane zwierzętom towarzyszącym odnosiły się niejednokrotnie do ich wyglądu[4], zachowań[5], cech charakteru[6], odwoływały się też do znanych i lubianych filmów czy poszczególnych bohaterów literackich[7]. W językoznawstwie ukształtowana nazwa własna zwierzęcia określana jest terminem zoonim[8]. Zoonim potrzebny jest człowiekowi do nawiązania kontaktu ze zwierzęciem i zwróceniem na siebie jego uwagi. W przypadku utrzymania większego pogłowia nazewnictwo ma szczególne znaczenie i pozwala na odróżnienie poszczególnych osobników stada[9].



Fot. 3. Rozwijanie kabla telefonicznego przy użyciu psa ciągnącego wózek z bębnem. Pokaz wyszkolenia psów Towarzystwa Miłośników Psa Służbowego.
Źródło: „Mój Pies" 1937, nr 12, s. 14., https://jbc.bj.uj.edu.pl/dlibra/publication/352302/edition/336445/content [dostęp: 4.05.2024 r.].

Problematyka związana z nazewnictwem zwierząt służbowych pojawiła się już w czasie I wojny światowej[10]. Wykorzystywanie dużej liczby zwierząt: koni, psów i gołębi[11] oraz pozyskiwanie ich dla armii poszczególnych państw wymagało stosowania różnych rozwiązań umożliwiających policzalność zwierząt, a także przyszły zwrot ich właścicielom[12]. W przypadku psów powszechnie stosowano obroże z wygrawerowanym numerem rejestracyjnym[13]. W armii angielskiej imię psa służbowego było utrzymywane w tajemnicy i znane tylko jego opiekunowi[14]. Chodziło o to, by nikt nie był w stanie psa zawołać po imieniu[15]. Ze względu na to, że psy w tym czasie traktowane były jak środek łączności i przenosiły na swoim grzbiecie juki z meldunkami i rozkazami, rozwiązanie to miało swoje uzasadnienie. W Wojsku Polskim, w Centrum Wyszkolenia Piechoty, próby wprowadzenia specjalnych oznaczeń na obroży dla psów zaproponowano dopiero w 1935 r.[16]

Protoplaści kynologii policyjnej w II Rzeczypospolitej[17] także stanęli przed dylematem nazewnictwa psów służbowych. Początkowo nadawanie imion psom służbowym odbywało się na zasadzie dowolności[18]. Możliwe, że to nawet sam przewodnik nadawał imię lub używano po prostu nazwy cywilnej psa nadanej wcześniej przez właściciela. Sposób ten jednak wobec rosnącego dość szybko pogłowia okazał się niewystarczający. Dlatego w 1924 r. rozkazem Komendanta Głównego Policji Państwowej[19] wprowadzono urzędowe nazewnictwo pogłowia psów służbowych. Psy policyjne miały zatem mieć nadawane nazwy od kolejnych liter alfabetu w każdym kolejnym roku kalendarzowym, począwszy od litery A w 1924 r.[20] Rozwiązanie to zlikwidowało dowolność w podejściu do nazewnictwa zwierząt służbowych. Psy nazwane przed wejściem w życie rozkazu miały zatrzymać swoją nazwę, ale dodano do niej przydomek na stosowną literę rocznika[21]. Postanowienia te potwierdzone zostały w *Instrukcji o psach policyjnych*[22]. Każdy pies przysyłany na kurs tresury musiał mieć nazwę i numer ewidencyjny. Nadany numer miał być obligatoryjnie używany w dokumentacji razem z imieniem psa[23]. Nadawanie imion stało się wyłączną prerogatywą kolejnych ośrodków szkoleniowych do wybuchu II wojny światowej.

W kontekście nazewnictwa psów nie sposób nie wspomnieć o pierwszych próbach ewidencji psów służbowych w Policji Państwowej. Próby te podjęto bardzo wcześnie, bo już w 1920 r., gdy w zasadzie psów policyjnych było jeszcze w kraju dość mało[24]. Rozkaz nr 45 KG PP z 18 marca 1920 r.[25] wprowadził obowiązek prowadzenia wykazu na formularzu zawierającym ogólne umiejscowienie psa w danej jednostce: nazwę okręgu, nazwę powiatu oraz zbiór innych informacji identyfikujących zwierzę.

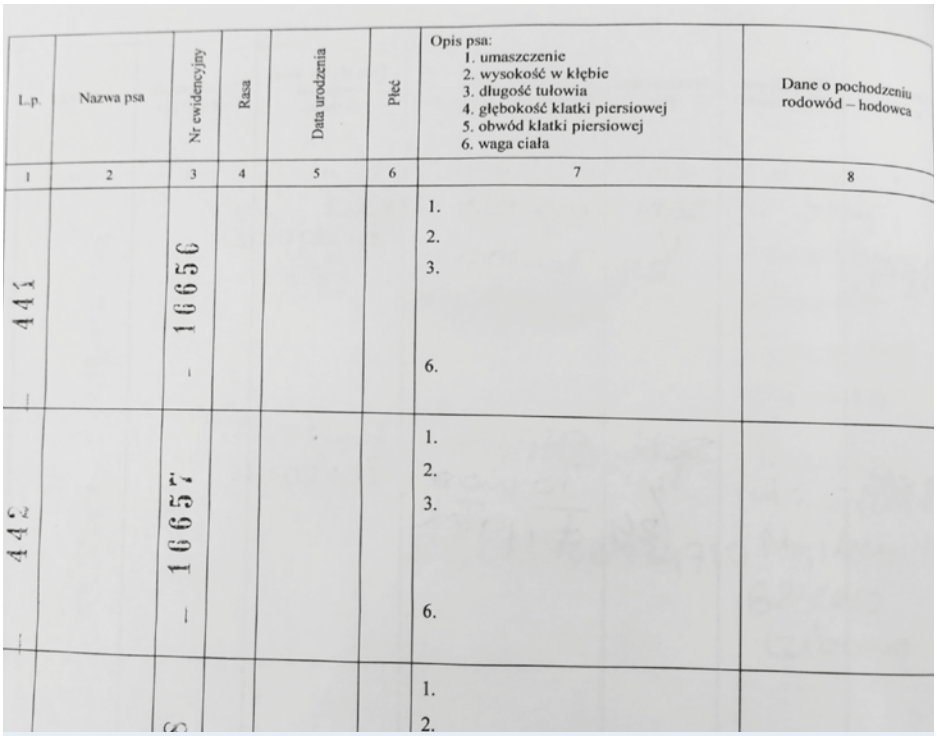
Mówimy zatem o pierwszych próbach uporządkowania nazewnictwa psów policyjnych i wprowadzenia pierwszej formy nadzoru Komendy Głównej Policji Państwowej nad posiadanymi zwierzętami służbowymi. Można zastanowić się nad praktycznymi przesłankami wprowadzenia tego typu rozwiązania. Powodami tymi mogły być przede wszystkim posiadanie na stanie wielu psów, które należało rozróżnić, a także przydzielanie konkretnych

Schemat 1. Dane pierwszej ewidencji psów w Policji Państwowej – informacje identyfikujące zwierzę na podstawie rozkazu nr 45 KG PP z dnia 18 marca 1920 r.
Źródło: opracowanie własne na podstawie rozkazu nr 45 KG PP z dnia 18 marca 1920 r., https://www.szukajwarchiwach.gov.pl/skan/-/skan/0e02255db01a5a886fb39dd9a5211953b-64166c1799279ae2941c76d9de3d1d0 [dostęp: 4.05.2024 r.].

Fot. 4. Fragment książki ewidencji Zakładu Tresury Psów MO z 1946 r. Źródło: ekspozycja materiałów w Izbie Tradycji Zakładu Kynologii Policyjnej.

zwierząt wyznaczonym policjantom. Wszystkie ewidencje psów policyjnych, jakie zachowały się w zasobach Archiwum Akt Nowych w Warszawie, nie zawierają danych dotyczących samych psów, ale odnoszą się zawsze do duetu: człowiek i pies. Sposób takiego nazewnictwa psów przetrwał do roku 1939, czyli do wybuchu II wojny światowej. Podkreślenia wymaga, że zachowane w Izbie Tradycji[26] zapisy wskazują, że po odtworzeniu kolejnych ośrodków szkolenia psów po II wojnie światowej kontynuowano właśnie ten przedwojenny sposób nazewnictwa pogłowia psów policyjnych.

W czasach współczesnych każdy pies zakwalifikowany do szkolenia w ramach procedury centralnego doboru psów do użycia w Policji otrzymuje nazwę, numer ewidencyjny oraz numer w systemie elektronicznej identyfikacji. Wynika



Fot. 5. Fragment Książki ewidencji psów służbowych Policji. Źródło: Gabinet Weterynaryjny Zakładu Kynologii Policyjnej Centrum Szkolenia w Legionowie. Zdj. P. Mrozowski.

(pieczęć jednostki organizacyjnej Policji)

KSIĄŻKA

PSA SŁUŻBOWEGO

POLICJI

(nazwa psa)

(nr identyfikacyjny)

(nr ewidencyjny)

(kategoria)

Cena zakupu psa ……..…… PLN

Wartość psa po szkoleniu ……..……..…… PLN w ……..……roku

Wzór drugiej strony Książki psa służbowego. Źródło: zarządzenie nr 91 KGP z 2022 r., zał. nr 4.

to z zapisów zarządzenia nr 91 Komendanta Głównego Policji z dnia 4 października 2022 r. w sprawie metod i form wykonywania zadań z użyciem psów służbowych w Policji[27].

Według stanu na dzień 31 sierpnia 2023 r. pogłowie psów policyjnych wynosiło 850 psów różnych kategorii[28]. Trudno zatem, by obecne psy policyjne nie miały nazw służbowych i kolejnych numerów ewidencyjnych.

Zakupywany pies przeznaczony do szkolenia na kursie specjalistycznym dla przewodników psów w Zakładzie Kynologii Policyjnej Centrum Szkolenia Policji w Legionowie otrzymuje zatem imię służbowe i numer ewidencyjny.

Imię zaczyna się na literę alfabetu przypadającą na dany rok kalendarzowy. Imiona te nadawane są wszystkim zakupionym do szkolenia zwierzętom. W praktyce psy policyjne mają nadane im nazwy służbowe (oficjalne) oraz nazwy własne (tzw. prywatne), do których są przywiązane. Pamiętajmy, że psy do użycia w Policji zakupywane są w wieku od roku do dwóch lat[29]. Są to zwierzęta w pewnym stadium rozwoju osobniczego – nazwane i reagujące na swoje imię. Trudno by było odzwyczajać je od imienia, na które reagują od urodzenia i do którego przyzwyczaił je wcześniejszy właściciel.

Nadana nazwa służbowa wpisywana jest również do Książki psa służbowego Policji – odpowiednika dokumentu weterynaryjnego, cywilnej książeczki zdrowia psa. Określona zostaje również kategoria wyszkolenia i cena psa. Dokument ten prowadzony jest przez całe życie psa i stanowi potwierdzenie odbytych szczepień, zabiegów, przebytych chorób itp. Szczegółowy wzór określony jest w załączniku nr 4 do zarządzenia nr 91 KGP.

Każdy pies policyjny posiadający nazwę i numer jest przydzielany komisyjnie, za protokołem, wytypowanemu policjantowi.

Mowa o powierzeniu policjantowi psa służbowego, którego zakup i przygotowanie do realizacji zadań służbowych generuje znaczne koszty. Zwierzę to jest utrzymywane przez wiele lat przez jednostkę organizacyjną Policji. Dodatkowo objęte jest stałą opieką weterynaryjną oraz żywione z budżetu jednostki[30].

Obecnie także prowadzona jest szczegółowa ewidencja psów policyjnych. Choć nosi ona nazwę: Wykaz opiekunów i psów służbowych Policji[31], to w zasadzie zbiera zbliżone dane do tej pierwotnej ewidencji zastosowanej w 1920 r.

Przyjęte rozwiązania z zakresu nazewnictwa i ewidencji psów służbowych przetrwały 100 lat od ich wprowadzenia w czasach Policji Państwowej. Pomimo upływu wieku nadal są funkcjonalne i sprawdzają się w przypadku utrzymywania i ewidencji dużego pogłowia psów. Na zakończenie warto zaznaczyć, że współczesne nadawanie imion psom policyjnym to wyłączne uprawnienie Zakładu Kynologii Policyjnej Centrum Szkolenia Policji w Legionowie. Podobne prerogatywy posiadały kolejne ośrodki szkoleniowe psów służbowych od roku 1924[32].

WZÓR

ZATWIERDZAM

.....

.....
(miejscowość, data)

PROTOKÓŁ

PRZYDZIELENIA PSA/KONIA* SŁUŻBOWEGO

W dniu ..... r., zgodnie z decyzją: ..... nr ..... z dnia ..... r.,
(nazwa i numer dokumentu)

komisja w składzie:

przewodniczący: .....,

członkowie: .....

.....

.....

przydzieliła psa/konia* służbowego o nazwie: ....., nr ewidencyjny* .....,

kod transpondera*....., rasy: ..... maści*: .....,

kategorii* ..... nr identyfikacyjny / UELN: .....,

opiekunowi .....,
(stopień, imię i nazwisko, ID kadrowy, jednostka organizacyjna Policji, inne dane)*

od opiekuna* .....,
(stopień, imię i nazwisko, ID kadrowy, jednostka organizacyjna Policji, inne dane)*

1. Uzasadnienie: .....

.....

.....

2. Uwagi dotyczące stanu zdrowia, higieny i utrzymania psa/konia* służbowego: .....

.....

.....

3. Przekazany sprzęt i dokumentacja psa/konia* służbowego: .....

.....

.....

....
(podpis opiekuna przekazującego)* (podpis opiekuna)

Podpisy komisji:

Członkowie: Przewodniczący:

…… ....……

……

……..……

Wykonano w ……. egz.
Rozesłano wg rozdzielnika
* Niewłaściwe skreślić.

Wzór protokołu przydzielenia psa. Źródło: rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 grudnia 2021 r. w sprawie psów służbowych i koni służbowych w Policji (Dz. U. poz. 2467), zał. nr 1.

„Wzór”

Wykaz opiekunów i psów służbowych Policji – stan na dzień …….. r.

L.p.	Dane opiekuna						Dane psa										Uwagi
	Stopień**)	Imię	Nazwisko	Identyfikator**)	Jednostka/komórka organizacyjna Policji	Przeszkolenie*)	Nazwa psa	Nr ewidencyjny	Nr identyfikacyjny Chip	Kategoria	Rasa	Data urodzenia	Data rozpoczęcia szkolenia	Nr atestu	Data ważności atestu	KGP/BOA/KWP/KSP	

*) Rodzaje ukończonych kursów dla przewodnika psa służbowego i rok ich ukończenia
**) Niewłaściwe skreślić

Wzór wykazu opiekunów i psów służbowych Policji. Źródło: zarządzenie nr 91 KGP, zał. nr 21.

[1] Zgodnie z § 3 zarządzenia nr 91 Komendanta Głównego Policji z dnia 4 października 2022 r. w sprawie metod i form wykonywania zadań z użyciem psów służbowych w Policji (Dz. Urz. KGP poz. 225) jest to podstawowa forma doboru psów do realizacji zadań w Policji.
[2] Zarządzenie nr 91 KGP, § 3 ust. 4 pkt 1–4.
[3] Tamże, § 3 ust. 4 pkt 5.
[4] S. Tomaszewska, *Nazwać swoje zwierzę – czyli o wielkomiejskiej zoonimii*, „Acta Universitatis Lodziensis. Folia Linguistica” 1998, nr 37, s. 169.
[5] Tamże.
[6] Tamże.
[7] Tamże, s. 171.
[8] Wikipedia, *Zoonim*, https://pl.wikipedia.org/wiki/Zoonim [dostęp: 4.05.2024 r.].
[9] Tamże.
[10] Problematyka ta jest szeroko opisywana w: E. Braratay, *Zwierzęta w okopach. Zapomniane historie*, Wydawnictwo w Podwórku, Gdańsk 2013, s. 35–36.
[11] Do oznaczania przynależności gołębi służyły zakładane na lewe nogi obrączki rodowe zawierające oznaczenia w postaci godła państwowego, litery Wojska Polskiego, liczby ewidencyjne oraz ostatnie cyfry lęgu gołębia, M. Leszczyński, *Wielki Leksykon Uzbrojenia. Wrzesień 1939. Psy i gołębie*, wyd. Edipresse Polska S.A., 2019, s. 23.
[12] Zwierzęta te były zależnie od kraju zakupywane lub rekwirowane, E. Braratay, *Zwierzęta w okopach*. *Zapomniane historie*, s. 29–30, 33–34.
[13] Numer ten pozwalał na odnalezienie właściciela psa w rejestrach mobilizacyjnych, tamże, s. 36.
[14] Tamże, s. 109.
[15] Niejednokrotnie zwierzęta te, przenosząc rozkazy i wiadomości, były celowo zwabiane na stronę przeciwną w celu przejęcia cennych informacji.
[16] M. Leszczyński, *Wielki Leksykon Uzbrojenia. Wrzesień 1939. Psy i gołębie,* s. 42–44.
[17] P. Mrozowski, *Wiktor Ludwikowski. Zapomniany protoplasta kynologii policyjnej*, „Kwartalnik Policyjny” 2023, nr 3–4, https://kwartalnik.csp.edu.pl/kp/aktualne-wydanie/5581,Wiktor-Ludwikowski-Zapomniany-protoplasta-kynologii-policyjnej.html [dostęp: 7.04.2024 r.].
[18] Głównie z braku regulacji policyjnych w tej sprawie.
[19] Rozkaz nr 269 KG PP z dnia 3 października 1924 r., AAN, sygn. 2/349/2/2.4/561/71, https://www.szukajwarchiwach.gov.pl/skan/-/skan/d0c15b595eb568247c0b2fcd0a1fa9ae95fde-0d5af861ffca3109f4615fd86b5 [dostęp: 10.07.2024 r.].
[20] Tamże.
[21] Tamże.
[22] Rozkaz nr 322 KG PP z dnia 27 kwietnia 1926 r., AAN, sygn. 2/349/1/1.1/8/14, https://www.szukajwarchiwach.gov.pl/skan/-/skan/c2133a21cbe225517ac916be4f0004de28b57f62d2a888-345274ceb83e6b7103 [dostęp: 10.04.2024 r.].
[23] Tamże, § 18.
[24] Rozkaz nr 214 KG PP z dnia 1 czerwca 1923 r., AAN, sygn. 2/349/2/2.4/561/78,https://www.szukajwarchiwach.gov.pl/skan/-/skan-/8df2bfae97e58154017183ce27cb497d9fd36744ef9dbb56abf-7c66243de2d5a [dostęp: 10.07.2024 r.].
[25] Rozkaz nr 45 KG PP z dnia 18 marca 1920 r. w sprawie hodowli i tresury psów policyjnych, https://www.szukajwarchiwach.gov.pl/skan/-/skan/0e02255db01a5a886fb39dd9a5211953b-64166c1799279ae2941c76d9de3d1d0 [dostęp: 4.05.2024 r.].
[26] K. Wójcikowska, *Nadzór nad realizacją zadań z zakresu kynologii policyjnej*, „Kwartalnik Policyjny” 2023, nr 3–4, https://kwartalnik.csp.edu.pl/kp/aktualne-wydanie/5533,Nadzor-nad-realizacja-zadan-z-zakresu-kynologii-policyjnej.html [dostęp: 10.04.2024 r.].
[27] Zarządzenie nr 91 KGP, § 19 ust. 1.
[28] K. Wójcikowska, *Nadzór nad realizacją zadań z zakresu kynologii policyjnej*.
[29] Zarządzenie nr 91 KGP, § 7 ust. 1.
[30] Rozporządzenie MSWiA z dnia 22 grudnia 2021 r. w sprawie psów służbowych i koni służbowych w Policji, § 12–21.
[31] Prowadzenie tej ewidencji wynika z § 53 zarządzenia nr 91 KGP.
[32] Rozkaz nr 359 KG PP z dnia 13 kwietnia 1927 r. w sprawie uzupełnienia instrukcji o psach policyjnych, AAN, sygn. 2/349/2/2.1/372/39, https://www.szukajwarchiwach.gov.pl/skan/-/skan-/0e02255db01a5a886fb39dd9a5211953b64166c1799279a-e2941c76d9de3d1d0 [dostęp: 10.07.2024 r.].

Summary

From the pages of the history of police K9. Nomenclature and records of service dogs

The article is the part of one of the chapters of publication being prepared by the Police Canine Unit of the Police Training Centre in Legionowo and concerning the formation of police K9 in the years 1919–1939. It describes attempts to name the population of service dogs in times of the State Police as well as contemporarily applied solutions in this area. It also raises the issue of police dogs records and the allocation of animals to police officers.

Tłumaczenie: Katarzyna Olbryś

Pierwsze Ogólnokrajowe Zawody Sportowe Policji Państwowej

Fot. 1. Start biegu na 3 km. Źródło: *Przebieg zawodów sportowych policji*, „Gazeta Administracji i Policji Państwowej" 1926, nr 43, s. 693(15), https://jbc.bj.uj.edu.pl/dlibra/publication/242416/edition/230752/content? [dostęp: 24 czerwca 2024 r.].

kom. Dominik Jędryka

Zakład Kynologii Policyjnej CSP

Podnoszenie sprawności fizycznej i możliwość sprawdzenia się w ramach organizowanych przez Policję imprez sportowych mają ogromną wartość dla służby. Uczestnictwo w turniejach sportowych wpływa zapewne na zwiększenie ogólnej aktywności fizycznej wśród policjantów i pracowników Policji, ale również przekładać się może na zwiększenie efektywności w realizacji zadań służbowych oraz wzmacnia pozytywny wizerunek formacji.

Sportowa rywalizacja policjantów w ramach organizowanych zawodów do dziś cieszy się dużym zainteresowaniem wśród funkcjonariuszy. Dobrym przykładem pozytywnych wartości, jakie niesie organizacja sportu w Policji, jest coroczna edycja Turnieju Służb Mundurowych w Piłce Nożnej Halowej im. podkom. Andrzeja Struja. Do tegorocznej rywalizacji podczas XIV edycji stanęły 92 drużyny z Polski i zza granicy. W skład drużyn wchodzili funkcjonariusze i pracownicy Policji reprezentujący komendy wojewódzkie Policji oraz szkoły i uczelnie policyjne z całego kraju, a także drużyny z Czech, Rumunii, Słowacji i Ukrainy. Piłkarskie zawody były hołdem oddanym policjantowi, który poniósł śmierć w wyniku podjętej interwencji. Turniej miał rangę międzynarodową i był objęty patronatem Komendanta Głównego Policji[1].

Idea zmagań sportowych również znajdowała duże uznanie wśród policjantów, ich rodzin oraz członków kół sportowych okresu międzywojennego. Niniejszy artykuł może stać się inspiracją do reaktywowania idei Ogólnokrajowych Zawodów Sportowych Policji w przypadającą na rok 2026 setną rocznicę pierwszych zawodów w Warszawie. Powrót do wartości przyświecających rozgrywaniu tak dużej imprezy sportowej miałby istotny wpływ na kreowanie pozytywnego wizerunku współczesnej Policji oraz etosu służby.

Ówczesne wydarzenia sportowe, do których się odnoszę, jak wskazują czasopisma policyjne, często wymiennie nazywane były zawodami „ogólnopolicyjnymi" lub „ogólnokrajowymi", co mogło nadawać rangę najważniejszej imprezy sportowej dla ówczesnej służby na miarę mistrzostw Polski. Istnieją mało znane informacje dotyczące rozgrywanych konkurencji sportowych, m.in. technicznych aspektów przebiegu konkurencji, oraz informacje dotyczące do dziś istniejących miejsc rozgrywania zawodów, które niewątpliwie związane są z rozwojem sportu nie tylko policyjnego, ale i ogólnopolskiego. Na uwagę zasługują ciekawostki opisywane w prasie policyjnej tamtego okresu, a dotyczące niekiedy przeszkód i niedociągnięć w organizacji zawodów sportowych.

Policja Państwowa była organem wykonawczym władz państwowych i samorządowych i miała za zadanie ochronę bezpieczeństwa, spokoju i porządku publicznego. Na podstawie ustawy z dnia 24 lipca 1919 r. powołującej Policję Państwową[2] określono warunki, jakie powinni spełniać kandydaci do służby tak, aby mogli służyć i spełniać postawione przed nimi zadania służbowe. Nie bez

powodu w tak ważnym dla tworzenia i działania Policji Państwowej dokumencie określono, jako warunek przyjęcia kandydata na policjanta, posiadanie przez niego dobrego stanu zdrowia fizycznego. Dotyczyło to przyjęć zarówno na szeregowych policjantów, jak i na stanowiska oficerskie ze struktur wojskowych.

Analizując szereg archiwalnych dokumentów, publikacji oraz informacji prasowych dotyczących funkcjonowania Policji Państwowej od początku jej utworzenia do wybuchu II wojny światowej, można zauważyć ogromne zainteresowanie władz Policji Państwowej sprawami związanymi z rozwojem fizycznym, krzewieniem kultury fizycznej i sportu w środowisku policyjnym. Powodem tego zainteresowania z pewnością były walory uprawiania dyscyplin sportowych, które mogły być przydatne w służbie. Komendant Główny Policji Państwowej gen. Kordian Zamorski podkreślał znaczenie wychowania fizycznego i uprawianych dyscyplin sportowych dla potrzeb wykonywania zadań służbowych przez policjantów. W wydanym w 1938 r. rozkazie[3] zwracał uwagę na wiele zaniedbań w realizacji zajęć wychowania fizycznego dla policjantów oraz podkreślał doniosłe znaczenia wychowania fizycznego dla służby. Wskazywał, iż „wyrobienie policjanta i jego sprężystość" mają niebagatelny wpływ na wykonywanie zadań służbowych, gdy ma „za przeciwnika przestępcę przeważnie zwinnego i sportowo wyrobionego". Rozkazem tym zostało zalecone m.in. wyrabianie umiejętności pokonywania naturalnych torów przeszkód oraz ćwiczenia skoków w dal i wzwyż, pełzania, wspinania się i przechodzenia przez przeszkody.

Sprawy wychowania fizycznego wśród ogółu społeczeństwa również wzbudzały duże zainteresowanie władz państwowych. 10 listopada 1926 r., w przededniu wielkiej rocznicy dla Polaków, Marszałek Józef Piłsudski jako minister spraw wojskowych, profesor Kazimierz Bartel – ówczesny minister wyznań religijnych i oświecenia publicznego, oraz generał Sławoj Felicjan Składkowski jako minister spraw wewnętrznych ogłosili uchwałę uznającą wychowanie fizyczne za sprawę pierwszorzędnej wagi dla państwa. Zapowiedzieli tym samym wniesienie do sejmu projektu ustawy o powszechnym wychowaniu fizycznym[4].

Niska sprawność fizyczna policjantów pełniących służbę w formie patrolu musiała stanowić problem dla Komendy Głównej Policji Państwowej. Z rozkazów Komendanta Głównego PP oraz okólników służbowych wynika, że konieczność trenowania pokonywania naturalnych torów przeszkód przez policjantów była wymagana. Przepisy te wskazywały nawet w jakiej formie, w jakich okolicznościach i z jaką częstotliwością ćwiczenia tego typu miałyby się odbywać[5].

O wielkiej roli sportu dla policjantów świadczyły chociażby liczne artykuły poświęcone tematyce sportu w cyklicznym wydawnictwie „Na Posterunku". W rubryce „Wychowanie fizyczne – sport" można było znaleźć informacje nie tylko o przebiegu zawodów policyjnych, ogólnodostępnych wydarzeń sportowych, meczów piłkarskich, ale także informacje o najpopularniejszych w tamtym okresie dyscyplinach sportowych. Na łamach periodyku podkreślano walory utylitarne dyscyplin sportowych wykazujących przydatność dla właściwej realizacji zadań służbowych przez policjantów[6]. Dzięki zamieszczonym informacjom czytelnik mógł się dowiedzieć, co trenować, jak trenować oraz w jakim ubraniu. Często z przyczyn ekonomicznych do najpopularniejszych należały dyscypliny lekkoatletyczne, ale nie brakowało też dyscyplin wymagających większych nakładów sprzętowych, takich jak: wioślarstwo, tenis ziemny, szermierka, hokej, kolarstwo czy jazda konna. Dużym zainteresowaniem wśród społeczeństwa, policjantów i innych zawodów mundurowych cieszyło się strzelectwo.

W wydawanej równolegle „Gazecie Policji Państwowej" podinspektor Julian Juni słusznie zauważa znaczenie sportu, wzorując się na przykładach wybitnych sportowców, m.in. z Europy, Stanów Zjednoczonych, którzy zasilali szeregi formacji policyjnych tych krajów, będąc reprezentantami dyscyplin lekkoatletycznych, boksu oraz piłki nożnej[7]. Tym samym dostrzega potrzebę rozwoju wychowania fizycznego i sportu na potrzeby Policji Państwowej w Polsce. Możliwe, że stanowisko autora artykułu miało duży wpływ na powstawanie zrzeszeń i organizacji policyjnych zajmujących się sportem. Tak w 1924 r. w Katowicach powstał pierwszy PKS – Policyjny Klub Sportowy[8], a w ślad za nim w 1926 r. na terenie II Rzeczypospolitej zostało utworzonych 14 klubów[9]. Do dzisiaj trwa spór o faktyczną liczbę powstałych PKS-ów z uwagi na dużą dynamikę tworzenia policyjnych sportowych organizacji, a zarazem ich likwidacji. W 1929 r. funkcjonowało 105 PKS-ów zrzeszających 10 000 członków (policjantów, osoby cywilne)[10]. Zauważalny wzrost liczby PKS-ów i napływu członków nastąpił po I Ogólnokrajowych Zawodach Sportowych. Miało to związek z wydanym przez Komendanta Głównego PP Mariana Borzęckiego rozkazem nr 338 z dnia 30 października 1926 r.[11] Niniejszym rozkazem polecał zakładanie PKS-ów w powiatach, tworzenie wyselekcjonowanych drużyn mogących stanowić reprezentację na przyszłoroczne wydarzenie sportowe Policji Państwowej. Jak wynika z rozkazu, M. Borzęcki już na początkowym etapie dostrzegał wielkie możliwości promocji wizerunku Policji Państwowej w prasie i wśród społeczeństwa poprzez organizację i udział środowiska policyjnego w sporcie. Dzięki wielkiemu poparciu Komendanta Głównego PP równolegle do tworzących się PKS-ów powstawały ogniska sportowe PP oraz koła sportowe przy stowarzyszeniu „Rodzina Policyjna"[12]. Jak wskazują wyniki inauguracyjnych zawodów, wielu sportowców policjantów przynależało do kół sportowych.

Wymieniając dyscypliny sportowe uprawiane na potrzeby służby policyjnej, nie można zapomnieć o popularnym boksie, a wśród policjantów – walce wręcz opartej w tamtym okresie na technikach ju-jitsu, nazywanej na potrzeby szkoleń policyjnych „gimnastyką policyjną"[13]. Zajęcia z gimnastyki policyjnej w ramach szkoleń policyjnych były związane z nauką obezwładniania osób, a w odniesieniu do teraźniejszych czasów – z niczym innym jak technikami interwencyjnymi. Warto wspomnieć o bardzo popularnej w środowiskach militarnych w tamtym okresie dyscyplinie, jaką była walka na bagnety[14], polegająca na zadawaniu pchnięć i uderzeń przeciwnikowi przy wykorzystaniu specjalnie skonstruowanych karabinów (Mosin) sprężynowych (sprężyna pełniąca funkcję bezinwazyjnego bagnetu) i strojów ochronnych z maskami na twarz. Dodatkowo, na potrzeby walk na polu bitwy wojskowej, trenowano dyscyplinę rzutu granatem opartą na przepisach instrukcji grenadierskiej[15].

IDEA SPORTOWYCH ZAWODÓW POLICYJNYCH

Jak już wspomniano wcześniej, Komendant Główny PP Marian Borzęcki do spraw popularyzacji sportu w Policji Państwowej podchodził dość wizjonersko. W organizacji sportu dla funkcjonariuszy policyjnych upatrywał dużą szanse promocji PP jako formacji zdrowej, silnej i wysportowanej. Należy jednak pamiętać, iż Policja Państwowa na początkowym etapie tworzenia borykała się z wieloma problemami zarówno natury finansowej, jak i szkoleniowej. Baza treningowa była dość skromna. Początkowe lata to nie był dobry czas na tworzenie masowych struktur sportowych i rozpowszechnianie wychowania fizycznego wśród często jeszcze nieprzeszkolonych w podstawowym zakresie niższych funkcjonariuszy.
Komendant Główny PP dostrzegał potrzebę wzmacniania fizycznego policjantów, którym zdrowie i sprawność były niezbędne do realizacji podstawowych zadań służbowych. Niedoskonałości fizyczne oraz niski poziom sprawności fizycznej ówczesnych policjantów zapewne dostrzegali przestępcy, którzy uzyskiwali przewagę w konfrontacji ze słabym fizycznie policjantem.

I ZAWODY KORPUSU POLICJI PAŃSTWOWEJ

Fot. 2. Prezydent Rzeczypospolitej wręcza nagrodę jednemu ze zwycięzców. Źródło: *Pierwsze Zawody Sportowe Korpusu Policji Państwowej*, „Gazeta Administracji i Policji Państwowej" 1926, nr 43, s. 679(1), https://jbc.bj.uj.edu.pl/dlibra/publication/242416/edition/230752/content? [dostęp: 10 czerwca 2024 r.].

Przełomem w sprawie organizacji imprezy sportowej był okólnik nr 1363 Komendanta Głównego PP z 23 lipca 1926 r., który spowodował podjęcie działań organizacyjnych I Zawodów Korpusu Policji Państwowej (formalna nazwa pierwszych zawodów)[16]. Określono rodzaj konkurencji, jakie będą przeprowadzone w ramach zawodów, w tym 5 konkurencji w dyscyplinach lekkoatletycznych, tj. bieg na 100 m, bieg przełajowy na 3 km, chód na 5 km, skok w dal, skok wzwyż, rozgrywane na podstawie obowiązujących przepisów Polskiego Związku Lekkiej Atletyki – PZLA, oraz rzut granatem. Określono obowiązujący zawodników strój lekkoatletyczny oraz pantofle, z wyjątkiem konkurencji realizowanych w umundurowaniu z obciążeniem (chód na 5 km). Na początkowym etapie organizacyjnym założono możliwość rozegrania innych konkurencji, w tym rzut dyskiem, rzut oszczepem itp., pod warunkiem zgłoszenia się minimum 10 uczestników. Przewidziano także rozegranie meczu piłkarskiego, prosząc o zgłaszanie się drużyn wyrażających chęć na rozegranie potyczki piłkarskiej i wskazując za przeciwnika drużynę koła sportowego Inspekcji PP m.st. Warszawy[17]. Ponadto został odnotowany fakt, iż zawody strzeleckie zostaną zrealizowane w następnym roku[18]. Termin odbywania się zawodów został określony w przybliżeniu na połowę października. Nadmieniono, iż Komenda Główna PP w ramach organizacji zawodów zapewni zakwaterowanie, natomiast koszty podróży i wyżywienia poniosą sami uczestnicy. Mogło mieć to potem znaczący wpływ na zmniejszoną liczbę uczestników, którzy nie stawili się do zawodów pomimo wcześniejszych zgłoszeń.
W dniach 16–18 października 1926 r., jak opisano na łamach „Gazety Administracji i Policji Państwowej", odbyło się święto sportu policyjnego, które miało „doniosłe znaczenie moralne dla władz policji jako też dla wszystkich sportowców w policji"[19]. Zawody miały wysoką rangę z uwagi na obecność m.in. Prezydenta Rzeczypospolitej Ignacego Mościckiego, Ministra Spraw Wewnętrznych Felicjana Sławoja Składkowskiego, Komisarza Rządu na m.st. Warszawę Władysława Jaroszewicza, II Wiceministra Spraw Wojskowych generała Kazimierza Fabrycego, Zastępcę Dowódcy Korpusu generała Wincentego Kaczyńskiego, Szefa Sztabu Korpusu pułkownika Erwina Więckowskiego oraz Komendanta Głównego Policji Państwowej Mariana Borzęckiego, jako gospodarza zawodów, wraz z wyższymi oficerami PP: Zastępcą Komendanta Głównego PP nadinspektorem Henrykiem Wardęskim, inspektorami Czyniewskim, Foresterem, Kaufmanem, Koralem, Tomanowskim, Wróblewskim, podinspektorami Charlemagne, Liliesztern, Płotnickim oraz inspektorem Władysławem Sobolewskim[20], który brał udział w licznych turniejach szermierczych, m.in. bronił barw polskich na Olimpiadzie w 1924 r. w Paryżu[21]. Rola insp. Sobolewskiego w sprawach organizacyjnych dotyczących zawodów sportowych wydaje się istotna w tamtym czasie, gdyż pełnił on funkcję Kierownika Działu Wyszkolenia Komendy Głównej PP.
W zawodach wzięli udział policjanci i urzędnicy policyjni zrzeszeni w organizacjach sportowych niemal ze wszystkich komend wojewódzkich: warszawskiej, łódzkiej, kieleckiej, białostockiej, m.st. Warszawy, lwowskiej, tarnopolskiej, stanisławowskiej, wołyńskiej, wileńskiej oraz sportowcy Komendy Głównej Policji Województwa Śląskiego. Swoją gotowość do udziału w zawodach zgłosiło 247 zawodników, natomiast w samych zawodach wzięło

udział 132 zawodników[22]. Na niższą liczbę zawodników biorących udział mogły mieć wpływ sprawy organizacyjne, w tym m.in. zapewnienie jedynie zakwaterowania zawodnikom bez zwrotu kosztów podróży.

Co prawda, do pierwszych zawodów ogólnokrajowych nie były prowadzone oficjalne eliminacje, ale można przypuszczać, iż w poszczególnych województwach odbywała się selekcja zawodników podczas obowiązkowych ćwiczeń fizycznych. Do tworzenia reprezentacji na zawody ogólnokrajowe komendanci wojewódzcy PP zostali zobowiązani okólnikami nr 1335 i 1363 KG PP z 1926 r.[23] Główny Komendant Policji Województwa Śląskiego inspektor Leon Wróblewski, mając na uwadze zaplanowane ogólnokrajowe zawody, w okólniku nr 109/1926 zarządził, by każdy oddział policyjny w czasie przeznaczonym na ćwiczenia musztry uprawiał również ćwiczenia lekkoatletyczne, jak bieg krótko- i długodystansowy, skoki wszelkiego rodzaju, rzut kulą, oszczepem, dyskiem, granatem, pływanie itp.[24] Działanie to miało na celu wyselekcjonowanie kadry reprezentantów Województwa Śląskiego na ogólnokrajowe zawody policyjne.

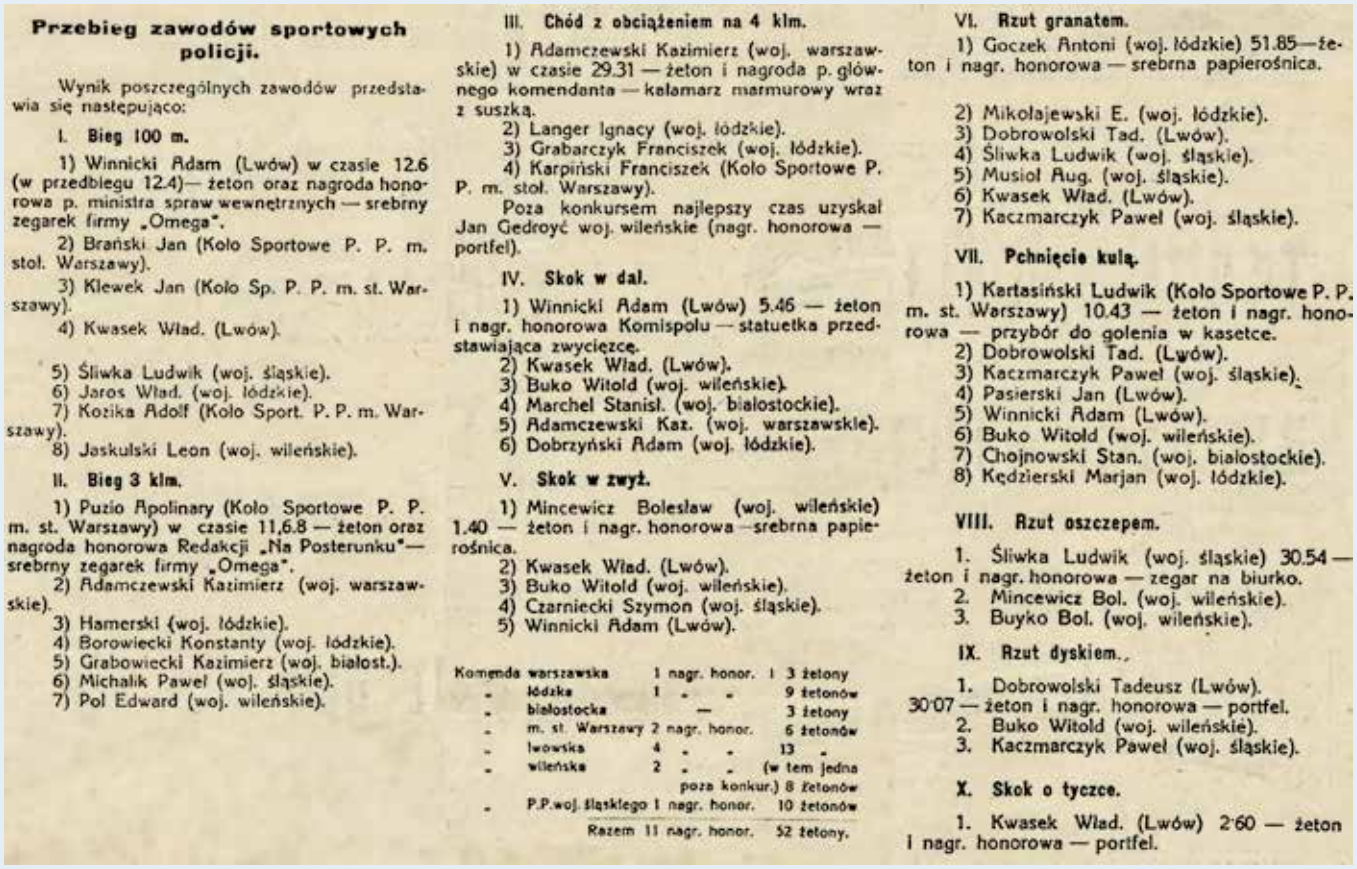
Przod. Karasiński Ludwik (Koło Sport. P. P. m. st. Warszawy), zwycięzca w pchnięciu kulą.

Fot. 3. Zwycięzca w pchnięciu kulą przod. Ludwik Karasiński. Źródło: *Przebieg zawodów sportowych policji*, „Gazeta Administracji i Policji Państwowej" 1926, nr 43, s. 693(15), https://jbc.bj.uj.edu.pl/dlibra/publication/242416/edition/230752/content? [dostęp: 10 czerwca 2024 r.].

Pierwszy dzień zawodów został przeznaczony na rozegranie meczów piłki nożnej. W przedmeczu o godzinie 13.30 do pojedynku stanęły drużyny Policyjnego Koła Sportowego m.st. Warszawy i drużyna klasy B harcerskiego Klubu „Varsovia", która pokonała rywala wynikiem 7:1. Kolejnym meczem rozegranym w tym samym dniu był bój PKS Katowice z drużyną klasy A klubu „Varsovia". Wynik 5:4 na korzyść stołecznego klubu wskazywał na zaciętą walkę[25]. Mecz ten, prowadzony przez sędziego Panza ze Lwowa, nie należał do łatwych z uwagi na warunki, w jakich przyszło toczyć pojedynek drużynom. Śliska murawa pokryta „licznemi jeziorkami"[26] i padający deszcz stanowiły znaczne utrudnienie dla graczy. Mimo to wynik do przerwy wynosił 4 bramki na koncie drużyny z Katowic. Gdy już wszystko wydawało się przesądzone, piłkarze stołecznego kluby podźwignęli się, zdobywając 5 bramek i ostatecznie kończąc mecz na swoją korzyść[27].

W kolejnych dniach zawodów rozegrano wcześniej zaplanowane konkurencje lekkoatletyczne z kilkoma zmianami polegającymi m.in. na skróceniu dystansu chodu na 5 km do 4 km z obciążeniem oraz wprowadzeniu wcześniej warunkowo planowanych konkurencji, tj. rzutu oszczepem, rzutu dyskiem i skoku o tyczce. Za przebieg konkurencji lekkoatletycznych odpowiedzialny został instruktor wychowania fizycznego st. przodownik F. Rokicki[28]. Duży podziw budzi fakt uczestnictwa i zajmowania czołowych lokat przez tych samych zawodników w nawet kilku konkurencjach rozgrywanych tego samego dnia. Chociażby uznanie dla Adama Winnickiego – reprezentanta Województwa Lwowskiego, który wykazywał swoją wszechstronność fizyczną w biegu na 100 m z czasem 12,6 sek. (pierwsze miejsce), skoku w dal z wynikiem 5,46 m (pierwsze miejsce), skoku wzwyż (piąte miejsce), pchnięcie kulą (szóste miejsce). Innym zawodnikiem, który stanął na wysokości sportowego zadania, był Władysław Kwasek z Województwa Lwowskiego, który swoją wszechstronność wykazał w 5 w konkurencjach, uzyskując m.in. w skoku o tyczce najlepszy wynik 2,60 m[29]. Odnośnie do informacji prasowej zamieszczonej w „Gazecie Administracji i Policji Państwowej" dotyczącej rozegranych zawodów na uwagę zasługuje fakt przyznania zwycięzcom konkurencji oraz jednemu uczestnikowi poza konkursem, Janowi Giedroyciowi (chód z obciążeniem 4 km), żetonów pamiątkowych oraz nagród rzeczowych, m.in. srebrnego zegarka firmy „Omega", kałamarza marmurowego wraz z suszką, statuetki, srebrnej papierośnicy, przyborów do golenia w kasetce, zegara na biurko czy portfela. Fundatorami nagród rzeczowych byli minister spraw wewnętrznych, komendant główny policji oraz redakcja „Na Posterunku". Wartość nagród za zwycięstwo była dość znaczna w stosunku do uzyskiwanych w tym czasie uposażeń. Zarobki policjantów kształtowały się na poziomie od 150 zł (posterunkowy) i 270 zł (podkomisarz) do 1000 zł (komendant główny PP)[30].

Dodatkowo na łamach „Gazety Administracji i Policji Państwowej" w kilku zdaniach podziękowano za przygotowanie meczów piłkarskich gronu organizacyjnemu i sędziom, „którzy z prawdziwem poświęceniem wytrwali na



Przebieg zawodów sportowych policji.

Wynik poszczególnych zawodów przedstawia się następująco:

I. Bieg 100 m.

1) Winnicki Adam (Lwów) w czasie 12.6 (w przedbiegu 12.4)— żeton oraz nagroda honorowa p. ministra spraw wewnętrznych — srebrny zegarek firmy „Omega".
2) Brański Jan (Koło Sportowe P. P. m. stol. Warszawy).
3) Klewek Jan (Koło Sp. P. P. m. st. Warszawy).
4) Kwasek Wład. (Lwów).
5) Śliwka Ludwik (woj. śląskie).
6) Jaros Wład. (woj. łódzkie).
7) Kozika Adolf (Koło Sport. P. P. m. Warszawy).
8) Jaskulski Leon (woj. wileńskie).

II. Bieg 3 klm.

1) Puzio Apolinary (Koło Sportowe P. P. m. st. Warszawy) w czasie 11,6.8 — żeton oraz nagroda honorowa Redakcji „Na Posterunku"— srebrny zegarek firmy „Omega".
2) Adamczewski Kazimierz (woj. warszawskie).
3) Hamerski (woj. łódzkie).
4) Borowiecki Konstanty (woj. łódzkie).
5) Grabowiecki Kazimierz (woj. białost.).
6) Michalik Paweł (woj. śląskie).
7) Pol Edward (woj. wileńskie).

III. Chód z obciążeniem na 4 klm.

1) Adamczewski Kazimierz (woj. warszawskie) w czasie 29.31 — żeton i nagroda p. głównego komendanta — kałamarz marmurowy wraz z suszką.
2) Langer Ignacy (woj. łódzkie).
3) Grabarczyk Franciszek (woj. łódzkie).
4) Karpiński Franciszek (Koło Sportowe P. P. m. stol. Warszawy).

Poza konkursem najlepszy czas uzyskał Jan Gedroyć woj. wileńskie (nagr. honorowa — portfel).

IV. Skok w dal.

1) Winnicki Adam (Lwów) 5.46 — żeton i nagr. honorowa Komispolu — statuetka przedstawiająca zwycięzcę.
2) Kwasek Wład. (Lwów).
3) Buko Witold (woj. wileńskie).
4) Marchel Stanisł. (woj. białostockie).
5) Adamczewski Kaz. (woj. warszawskie).
6) Dobrzyński Adam (woj. łódzkie).

V. Skok w zwyż.

1) Mincewicz Bolesław (woj. wileńskie) 1.40 — żeton i nagr. honorowa —srebrna papierośnica.
2) Kwasek Wład. (Lwów).
3) Buko Witold (woj. wileńskie).
4) Czarniecki Szymon (woj. śląskie).
5) Winnicki Adam (Lwów).

Komenda warszawska	1 nagr. honor.	i	3 żetony
„ łódzka	1 „ „		9 żetonów
„ białostocka	—		3 żetony
„ m. st. Warszawy	2 nagr. honor.		6 żetonów
„ lwowska	4 „ „		13 „
„ wileńska	2 „ „	(w tem jedna poza konkur.)	8 żetonów
„ P.P.woj. śląskiego	1 nagr. honor.		10 żetonów
	Razem 11 nagr. honor.		52 żetony.

VI. Rzut granatem.

1) Goczek Antoni (woj. łódzkie) 51.85—żeton i nagr. honorowa — srebrna papierośnica.
2) Mikołajewski E. (woj. łódzkie).
3) Dobrowolski Tad. (Lwów).
4) Śliwka Ludwik (woj. śląskie).
5) Musioł Aug. (woj. śląskie).
6) Kwasek Wład. (Lwów).
7) Kaczmarczyk Paweł (woj. śląskie).

VII. Pchnięcie kulą.

1) Kartasiński Ludwik (Koło Sportowe P. P. m. st. Warszawy) 10.43 — żeton i nagr. honorowa — przybór do golenia w kasetce.
2) Dobrowolski Tad. (Lwów).
3) Kaczmarczyk Paweł (woj. śląskie).
4) Pasierski Jan (Lwów).
5) Winnicki Adam (Lwów).
6) Buko Witold (woj. wileńskie).
7) Chojnowski Stan. (woj. białostockie).
8) Kędzierski Marjan (woj. łódzkie).

VIII. Rzut oszczepem.

1. Śliwka Ludwik (woj. śląskie) 30.54 — żeton i nagr. honorowa — zegar na biurko.
2. Mincewicz Bol. (woj. wileńskie).
3. Buyko Bol. (woj. wileńskie).

IX. Rzut dyskiem.

1. Dobrowolski Tadeusz (Lwów). 30.07 — żeton i nagr. honorowa — portfel.
2. Buko Witold (woj. wileńskie).
3. Kaczmarczyk Paweł (woj. śląskie).

X. Skok o tyczce.

1. Kwasek Wład. (Lwów) 2.60 — żeton i nagr. honorowa — portfel.

Fot. 4. Tabela wyników policyjnych zawodów sportowych. Źródło: *Przebieg zawodów sportowych policji*, „Gazeta Administracji i Policji Państwowej" 1926, nr 43, s. 693(15).

trudnem stanowisku"[31]. Jako organizatora meczów piłkarskich wymieniono nadkom. W. Dąbrowskiego z Komendy PP m.st. Warszawy, jako organizatora dyscyplin lekkoatletycznych wskazano st. przod. F. Rokickiego – instruktora wychowania fizycznego ze Szkoły Głównej PP (zwycięzcę w konkurencji skoku wzwyż II Ogólnokrajowych Zawodów Sportowych PP). W skład grona sędziowskiego wchodzili nadkom. Schuch, nadkom. Zieliński, asp. Grzeszkiewicz, Paruszewski, Weyrauch, Szejnach, gospodarz obiektów Ledziński oraz Grabicka[32].

Fot. 5. Awers żetonu wręczanego uczestnikom Ogólnokrajowych Zawodów Sportowych Policji Państwowej (projekt S.R. Koźbielewskiego wykonany z brązu, średnica 34 mm). Zdj. D. Jędryka.

Komendant Główny PP M. Borzęcki niedługo po zakończeniu pierwszych zawodów PP, doceniając znaczenie sportowego wyrobienia funkcjonariuszy i nosząc się z zamiarem organizacji zawodów na szerszą skalę w następnych latach, rozkazem nr 338 z dnia 30 października 1926 r. polecił komendantom wojewódzkim PP organizację zawodów wojewódzkich będących eliminacjami do zawodów ogólnokrajowych oraz nakazał objęcie szerszym zainteresowaniem obszaru krzewienia kultury fizycznej w środowiskach policyjnych poprzez tworzenie policyjnych klubów sportowych i wyłanianie reprezentacji poszczególnych dyscyplin[33]. Była to najprawdopodobniej jedna z ostatnich decyzji Mariana Borzęckiego na stanowisku Komendanta Głównego PP, gdyż 31 października 1926 r. płk Janusz Zygmunt Jagrym-Maleszewski został przeniesiony do dyspozycji celem objęcia stanowiska komendanta głównego PP, co faktycznie nastąpiło 5 listopada tegoż roku.

W wyniku analizy dokumentów i publikacji prasowych tamtego okresu można zauważyć pewne rozbieżności co do podawanej liczby uczestników pierwszych zawodów policyjnych. Na łamach „Gazety Administracji i Policji Państwowej" opublikowano informację o 132 zawodnikach, natomiast w rozkazie KG PP będącym podsumowa-

niem osiągniętych wyników wskazano 62 zawodników stających w szranki sportowych konkurencji, przy czym 52 zawodników zostało sklasyfikowanych na listach wyników, które pokryły się z informacjami zamieszczonymi w prasie i w rozkazie Komendy Głównej Policji Państwowej. Na łamach gazety „Na Posterunku" nr 39 z 1927 r. wskazano, iż liczba uczestników pierwszej edycji ogólnokrajowych zawodów wynosiła 150[34]. Można przypuszczać, że zaistniałe rozbieżności liczbowe były efektem zaokrąglania danych dotyczących zawodów.

Kierownik Wydziału Wyszkolenia Komendy Głównej PP inspektor Władysław Sobolewski na łamach prasy resortowej stwierdził, iż pierwsze zawody muszą wywołać echo, które odezwie się donośnie nawet w najdalej wysuniętych placówkach policyjnych i zachęci do sportu nie tylko pojedyncze jednostki, lecz również ogół braci policyjnej, która w tamtych czasach niestety dość obojętnie odnosiła się do spraw sportu[35]. Zwracał także uwagę na konieczność tworzenia kół i organizacji sportowych oraz zachęty do uprawiania sportu przez policjantów.

Pierwsza tak pomyślna próba zawodów sportowych może napawać serce wszystkich policjantów-sportowców otuchą, że nie pójdzie na marne, lecz owszem – doda bodźca do usilnej i wytrwałej pracy na polu sportu wszystkim tym, którzy chcą widzieć w policjancie polskim ideał zachodniego obywatela – podsumował zawody inspektor Władysław Sobolewski[36].

1 P. Ostaszewski, *Turniej Struja 2024*, „Gazeta Policyjna" 2024, nr 3, s. 9.
2 Ustawa z dnia 24 lipca 1919 r. o policji państwowej (Dz.Pr.P.P. Nr 61, poz. 363), art. 2, art. 26 pkt 4.
3 Rozkaz nr 743 KG PP z dnia 12 marca 1938 r., pkt 1, AAN, sygn. 567, k. 102.
4 W. Osmólski, *Wychowanie fizyczne i sport według Władysława Osmólskiego*, Warszawa 1920, s. 90.
5 Rozkaz nr 715 KG PP z dnia 24 lutego 1937 r., pkt 6, AAN, sygn. 567, k. 5.
6 Komenda Główna Policji, *Sport w Policji Państwowej,* https://hit.policja.gov.pl/hit/aktualnosci/194845,SPORT-W-POLICJI-PANSTWOWEJ.html [dostęp: 14.06.2024 r.].
7 J. Juni, *Dookoła spraw policyjnych,* „Gazeta Administracji i Policji Państwowej" 1921, nr 52, s. 811, https://jbc.bj.uj.edu.pl/dlibra/publication/241067/edition/229424/content [dostęp: 14.06.2024 r.].
8 J. Jeziorski, *Dziesięciolecie Policyjnego Klubu Sportowego*, „Kalendarzyk Policji Województwa Śląskiego" 1934, s. 293, https://www.sbc.org.pl/dlibra/publication/270480/edition/255865 [dostęp: 10 czerwca 2024 r.].
9 *Sprawy policji*, „Na Posterunku" 1929, nr 19, s. 292, https://polona.pl/item-view/1d033fc0-342a-45ee-bb54-9087889e3c68?page=10 [dostęp: 10 czerwca 2024 r.].
10 *Mistrzostwa Policji*, „Stadion" 1929, nr 36, s. 2, https://jbc.bj.uj.edu.pl/dlibra/publication/931610/edition/895444/content [dostęp: 14.06.2024 r.].
11 Rozkaz nr 338 KG PP z dnia 30 października 1926 r., AAN, sygn. 372, k. 87.
12 J. Paciorkowski, *I Zawody Sportowe Policji Państwowej*, „Policja 997" 2016, wydanie specjalne nr 7, s. 6.
13 S. Szczepkowski, *Gimnastyka Policyjna,* Warszawa 1917, s. 4.
14 W. Dańczuk, *Walka wręcz. Boks. Szermierka*, Okręgowa Szkoła Policji Państwowej, Łódź 1924, s. 61.
15 Komenda Główna Policji Państwowej, *Instrukcja władania granatem ręcznym*, drukiem „Gazety Administracji i Policji Państwowej", Warszawa 1931, s. 44.
16 *Z życia policji*, „Gazeta Administracji i Policji Państwowej" 1926, nr 30, s. 493, https://jbc.bj.uj.edu.pl/dlibra/publication/242403/edition/230739/content? [dostęp: 10 czerwca 2024 r.].
17 Tamże.
18 Tamże.
19 *Pierwsze Zawody Sportowe Korpusu Policji Państwowej*, „Gazeta Administracji i Policji Państwowej" 1926, nr 43, s. 679(1), https://jbc.bj.uj.edu.pl/dlibra/publication/242416/edition/230752/content? [dostęp: 10 czerwca 2024 r.].
20 Tamże.
21 *Ś.P. dr Władysław Marian Sobolewski, inspektor P.P.*, „Przegląd Policyjny" 1937, nr 6, s. 404, https://jbc.bj.uj.edu.pl/dlibra/publication/337282/edition/322253/content [dostęp: 10 czerwca 2024 r.].
22 Tamże.
23 J. Jaroszewski, *Ruch sportowy w Policji Państwowej w województwie łódzkim w latach 1919–1939. Zarys problematyki*, „Sport i Turystyka. Środkowoeuropejskie Czasopismo Naukowe" 2022, t. 5, nr 1, s. 23.
24 *Wychowanie fizyczne. Sport,* „Na Posterunku" 1926, nr 31, s. 601, https://polona.pl/item-view/7275b985-8a67-45be-b898-ad769f8-ebc2d?page=16 [dostęp: 14.06.2024 r.].
25 *Pierwsze Zawody Sportowe Korpusu Policji Państwowej*, „Gazeta Administracji i Policji Państwowej" 1926, nr 43, s. 679(1).
26 W. Sobolewski, *Pierwsze Zawody Sportowe Korpusu Policji Państwowej*, „Na Posterunku" 1926, nr 42, s. 752, https://polona.pl/item-view/d1e93595-6cfb-448f-8c99-88006cff4fe6?page=3 [dostęp: 14.06.2024 r.].
27 Tamże.
28 W. Sobolewski, *Pierwsze Zawody Sportowe Korpusu Policji Państwowej*, s. 753.
29 *Przebieg zawodów sportowych policji,* „Gazeta Administracji i Policji Państwowej" 1926, nr 43, s. 693, https://jbc.bj.uj.edu.pl/dlibra/publication/242416/edition/230752/content [dostęp: 14.06.2024 r.].
30 M. Berch, *Uposażenie Policji Państwowej w świetle nowych przepisów*, „Na Posterunku" 1934, nr 7, s. 101, https://polona.pl/item-view/44e068f4-0f43-47e2-a141-95a4129613e8?page=4 [dostęp: 14.06.2024 r.].
31 *Przebieg zawodów sportowych policji*, „Gazeta Administracji i Policji Państwowej" 1926, nr 43, s. 693.
32 M. Berch, *Uposażenie Policji Państwowej w świetle nowych przepisów*, s. 101.
33 Rozkaz nr 338 KG PP z dnia 30 października 1926 r., pkt 6, AAN, sygn. 372, k. 89.
34 A. Librach, *II Ogólnopolicyjne Zawody Sportowe,* „Na Posterunku" 1927, nr 39, s. 609–610, https://academica.edu.pl/reading/readSingle?page=3&uid=22097100 [dostęp: 14.06.2024 r.].
35 W. Sobolewski, *Pierwsze Zawody Sportowe Korpusu Policji Państwowej*, s. 751.
36 Tamże, s. 753.

Summary

The first Nationwide Sports Competition of the State Police

No one doubts that nowadays doing sport shapes the necessary skills of a police officer, useful in daily service. The benefits which sport brings for policemen were also recognized by the pre-war Polish Police. This is evidenced by, among other things, the organization of sports contest of the State Police in 1926, which is described in this article. The high rank of the event may be proved by, for example, the participation of the President of the Republic of Poland Ignacy Mościcki as an invited guest. As the author of the article points out, his study can be an inspiration for reactivating the idea of the National Police Sports Competition in 2026 – the 100th anniversary of the first competition held in Warsaw.

Tłumaczenie: Katarzyna Olbryś

ZASADY PUBLIKOWANIA
w „Kwartalniku Policyjnym”

Informacje dla autorów

1. Redakcja przyjmuje teksty dotąd niepublikowane o charakterze zawodowym lub naukowym, dotyczące zagadnień związanych z funkcjonowaniem Policji i z szeroko rozumianym bezpieczeństwem, a także z praktyką policyjną i współpracą formacji z innymi instytucjami ochrony porządku prawnego oraz z samorządem lokalnym.
2. Materiały do publikacji należy przesyłać pocztą elektroniczną na adres: kwartalnik@csp.edu.pl lub składać w sekretariacie Wydziału Wydawnictw i Poligrafii Centrum Szkolenia Policji w Legionowie (ul. Zegrzyńska 121, 05-119 Legionowo, tel. 47 725 58 81 lub 47 725 52 70).
3. Prace są kwalifikowane do druku przez zespół redakcyjny czasopisma. Redakcja zastrzega sobie prawo dokonywania skrótów i adiustacji tekstów oraz zmiany tytułów i śródtytułów.
4. W celu zapobiegania wszelkim przejawom nierzetelności, w tym zjawisku *ghostwriting* i *guest authorship*, redakcja wymaga ujawnienia przez autorów wkładu w powstanie publikacji.
5. Materiały mogą być weryfikowane w systemie antyplagiatowym, zgodnie z procedurą obowiązującą w Centrum Szkolenia Policji w Legionowie.
6. Materiały są publikowane w „Kwartalniku Policyjnym” nieodpłatnie, po złożeniu przez autora pisemnego oświadczenia, zgodnie z otrzymanym od redakcji wzorem.
7. Nadesłanych materiałów do publikacji redakcja nie zwraca.
8. Wersją pierwotną (referencyjną) czasopisma jest wydanie papierowe. Ponadto poszczególne numery są również dostępne w wersji elektronicznej na stronie internetowej: www.kwartalnik.csp.edu.pl.
9. Wskazówki edytorskie dotyczące przygotowania materiału przez autorów:
   - format A4, czcionka Times New Roman, wielkość 12 punktów, interlinia 1,5 wiersza, marginesy – 2,5 cm;
   - na pierwszej stronie należy podać imię i nazwisko autora materiału, stopień (lub tytuł) naukowy (tytuł zawodowy), nazwę instytucji, w której autor jest zatrudniony, nr telefonu, adres e-mailowy;
   - do tekstu należy dołączyć streszczenie oraz tytuł pracy w języku angielskim;
   - materiał ilustracyjny powinien być dostarczony w oddzielnych plikach (rysunki lub fotografie w formacie jpg, rozdzielczość 300 dpi, minimalna wielkość 1,5 MB);
   - schematy i wykresy muszą być edytowalne, tak aby można było nanieść korektę;
   - przypisy należy umieścić na dole strony lub na końcu pracy; przypisy wstawia się automatycznie i oznacza się cyframi arabskimi;
   - zgodnie z normami wydawniczymi przypis bibliograficzny powinien zawierać:
     – imię i nazwisko autora, tytuł, wydawcę, miejsce i rok wydania, numer strony:
     M. Olbrycht, J. Rutkowski, *Taktyka minersko-pirotechniczna w działaniach antyterrorystycznych*, Centrum Szkolenia Policji, Legionowo 2003, s. 35–36;
     – jeżeli dzieło jest pracą zbiorową:
     Nowy leksykon PWN, red. A. Dyczkowski, Warszawa 1998, s. 684;
     – jeżeli jest to artykuł w pracy zbiorowej:
     J. Szreniawski, *Prawo do dobrej administracji prawem podmiotowym obywatela*, w: *Dobra administracja. Teoria i praktyka*, red. J. Łukasiewicz, S. Wrzosek, Radom 2007, s. 256;
     – jeżeli jest to artykuł w czasopiśmie:
     B. Jankowska, *Odpowiedzialność karna osób prawnych*, „Państwo i Prawo” 1996, nr 7, s. 46;
     – jeżeli jest to akt prawny (należy wskazać publikator):
     Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2024 r. poz. 145);
     – jeżeli jest to tekst opublikowany w Internecie:
     J. Kowalski, *Edukacja online*, www.gazeta.pl/forum?forumedukacyjne5645 [dostęp: 12.03.2004 r.].

Zasady recenzowania artykułów

1. Artykuły o charakterze naukowym są recenzowane przez dwóch niezależnych recenzentów zewnętrznych, zgodnie z zasadami dotyczącymi tego rodzaju prac, w tym z *Dobrymi praktykami w procedurach recenzyjnych w nauce*, oprac. Zespół do Spraw Etyki w Nauce pod przewodnictwem prof. dr. hab. W. Marciszewskiego, Warszawa 2011.
2. Autorzy i recenzenci nie znają swoich tożsamości, w innych przypadkach recenzenci podpisują oświadczenie o niewystępowaniu konfliktu interesów między nimi a autorami, w tym m.in. bezpośrednich relacji osobistych, relacji podległości zawodowej, bezpośredniej współpracy.
3. Recenzja ma formę pisemną. Zawiera syntetyczną charakterystykę artykułu, część analityczną, ocenę ogólną i kończy się jednoznaczną konkluzją, tj. jest pozytywna, negatywna lub warunkowo pozytywna, jeśli recenzent wskazuje na konieczność wprowadzenia poprawek. Autorzy artykułów są zobowiązani do ustosunkowania się do uwag i uwzględnienia sugerowanych zmian.
4. Nazwiska recenzentów poszczególnych publikacji nie są ujawniane. Lista recenzentów współpracujących z czasopismem w każdym roku kalendarzowym jest publikowana w ostatnim numerze danego roku.

ZOSTAŃ POLICJANTEM

Ogólnopolska infolinia dla kandydatów do Policji:

477 210 997

Więcej informacji na stronie:
https://praca.policja.pl/pwp/rekrutacja

Zdjęcia: R. Karyś, J. Lęcznar.

CENTRUM SZKOLENIA POLICJI W LEGIONOWIE

05-119 Legionowo
ul. Zegrzyńska 121

www.csp.edu.pl