FOLIA 414

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 14(2) (2024)

ISSN 2657-8549

DOI 10.24917/26578549.14.2.7

Andrzej Czop

Uniwersytet WSB MERITO w Poznaniu, Filia w Chorzowie

ORCID 0000-0002-9621-5879

Tomasz Malinowski

Krakowskie Centrum Bezpieczeństwa

ORCID 0009-0004-2375-2966

Znaczenie śladów cyfrowych w zapewnianiu bezpieczeństwa systemów logistycznych

The Role of Digital Footprints in Securing Logistics Systems

Abstrakt

Artykuł jest efektem przeprowadzonych badań ukierunkowanych na ustalenie roli i znaczenia śladów pozostawianych przez sprawców zamachów w procesie zapewniania bezpieczeństwa systemom logistycznym. Autorzy scharakteryzowali systemy logistyczne, wskazując na ich złożony charakter oraz istotne znaczenie w funkcjonowaniu gospodarki państwa. Wskazali, że muszą one podlegać szczególnej ochronie poprzez stosowanie nowoczesnych zabezpieczeń technicznych[1] tworzonych w oparciu na najnowszych technologiach, zintegrowanych na platformach cyfrowych. Przedstawili kluczową rolę śladów zabezpieczanych na miejscu zamachu, które dostarczają wielu istotnych informacji pozwalających na rekonstrukcję działania sprawcy, ustalenie jego *modus operandi*, a nawet identyfikację[2]. Autorzy wiele uwagi poświęcili znaczeniu śladów cyfrowych, wskazując, że w przypadku systemów informatycznych w logach systemowych pozostają widoczne zmiany w zapisach logowań, w plikach, a także te pozwalające na określenie aktywności sprawcy w aplikacjach i sieci. W artykule podkreślono znaczenie prawidłowego zabezpieczenia logów, materiałów wideo i audio, które są źródłem ważnych dowodów w postępowaniu karnym. Pozostawione przez sprawcę ślady umożliwiają zarówno efektywny proces wykrywczy, jak i zapobieganie podobnym sytuacjom w przyszłości. Zdaniem autorów stwarzają także bazę do wypracowania optymalnych rozwiązań projektowych w zakresie zabezpieczania technicznego

[1] A. Czop (2021). *Rola Specjalistycznych Uzbrojonych Formacji Ochronnych w przeciwdziałaniu zagrożeniom terrorystycznym w Polsce*. Kraków, s. 125–126.

[2] E. Miturska (2015). *Mechanizmy psychologiczne motywacji człowieka. Przegląd koncepcji teoretycznych*. „Świat Problemów", nr 4(267), s. 5.

systemów logistycznych. Przedstawione w artykule ustalenia są przyczynkiem do dalszych badań, ukierunkowanych na podniesienie bezpieczeństwa tych systemów.

Słowa kluczowe bezpieczeństwo, logistyka, ślady, cyberbezpieczeństwo

Abstract

The article presents research aimed at determining the role and importance of digital traces left by perpetrators in the process of enhancing the security of logistics systems. The author characterized logistics systems, pointing out their complex nature and significant importance in the functioning of the state's economy. He emphasized the need for special protection of these systems through the use of modern technical security measures, based on the latest technologies and integrated into digital platforms. The key role of traces secured at the scene of the attack is presented, as they provide important information enabling the reconstruction of the perpetrator's actions, determination of their *modus operandi*, and even identification. Significant attention is given to the importance of digital traces, pointing out that in the case of IT systems, system logs record changes in login data and files, as well as activity within applications and the network, enabling the identification of the perpetrator. The article emphasizes the importance of properly securing logs, video, and audio materials, which serve as important evidence in criminal proceedings. Traces left by perpetrators enable both effective detection process and the prevention of similar incidents in the future. According to the author, they also create a basis for developing optimal design solutions in the area of technical security of logistics systems. The findings presented in the article serve as a contribution to further research aimed at enhancing the security of such systems.

Keywords: security, logistics, traces, cybersecurity

Wprowadzenie – metodologia badań

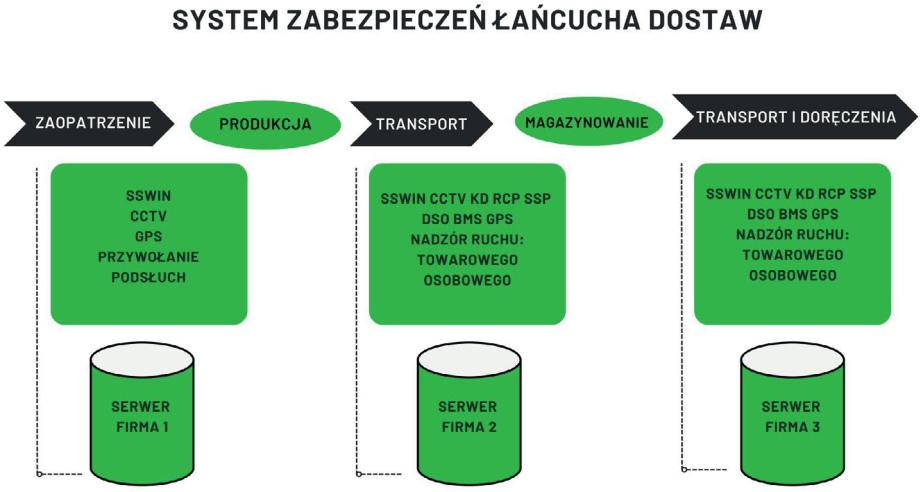
Szybki rozwój systemów ochrony technicznej przyczynia się do zwiększenia różnorodności zasobów informacji magazynowanych w pamięciach wewnętrznych urządzeń oraz na serwerach. Równocześnie uległy zwiększeniu zasoby dostępnych informacji. Stosowanie serwerów czasu oraz synchronizowanych z nimi wewnętrznych zegarów pozwala na ich równoległe wykorzystanie za pomocą dostępnych narzędzi informatycznych. Systemy ochrony technicznej znajdują zastosowanie w bardzo wielu dziedzinach, w różnych formach i technologiach[3]. Szczególne znaczenie mają systemy zaimplementowane w systemach logistycznych. Dzięki nim następuje przeprowadzenie w sposób bezpieczny procesów logistycznych. Tworzenie systemu bezpieczeństwa równolegle z budową systemu logistycznego prowadzi do zwiększenia efektywności przyjętych rozwiązań w sferze techniczno-organizacyjnej.

Zarządzanie systemem bezpieczeństwa w logistyce wspomaga i optymalizuje podejmowane procesy decyzyjne. Najbardziej niepożądanym elementem, który może wystąpić w procesie logistycznym, jest naruszenie lub przerwanie łańcucha

[3] A. Czop (2014). *Udział firm ochrony osób i mienia w zapewnianiu bezpieczeństwa publicznego w Polsce.* Katowice, s. 144.

bezpieczeństwa[4]. Stąd już na etapie jego projektowania, konieczne jest ustalanie najbardziej niekorzystnego scenariusza.

Tabela 1. System zabezpieczenia łańcucha dostaw



Źródło: opracowanie własne.

Artykuł jest efektem przeprowadzonych badań ukierunkowanych na ustalenie roli i znaczenia śladów pozostawianych przez sprawców zamachów w procesie zapewniania bezpieczeństwa systemom logistycznym.

Sformułowano główny problem badawczy wyrażony w pytaniu: jaka jest możliwość wykorzystania śladów zamachu w podwyższaniu poziomu bezpieczeństwa systemów logistycznych? Aby odpowiedzieć na to zasadnicze pytanie, postawiono następujące problemy szczegółowe:

1. Czym są systemy logistyczne i jakimi środkami technicznymi mogą być chronione?
2. Jaka jest istota śladów kryminalistycznych i kiedy mają wartość dowodową?
3. Jakie jest znaczenie i możliwość wykorzystania śladów pozostawionych w cyberprzestrzeni?
4. Jakie działania podejmują sprawcy zamachów celem zacierania śladów?

W prowadzonych badaniach wykorzystano metodę krytycznej analizy dostępnej literatury przedmiotu oraz studium przypadku. Badaniu poddano sprawy dotyczące zamachów na systemy logistyczne. Dwie to sprawy karne realizowane przez jednego z autorów, w trakcie jego służby w pionie kryminalnym Policji. Kolejna sprawa była przedmiotem działań obu autorów w ich działalności komercyjnej związanej z zapewnianiem bezpieczeństwa przedsiębiorcom prowadzącym działalność gospodarczą.

[4] K. Ficoń (2021). *Łańcuch bezpieczeństwa. Zagrożenia, ryzyko, kryzysy*. Warszawa, s. 261–270.

Systemy logistyczne

W literaturze występuje wiele definicji systemu logistycznego. W badaniach przyjęto definicję wskazującą, iż system ten składa się z kilku elementów, z których każdy podlega ochronie.

W tym ujęciu system logistyczny przedsiębiorstwa określony jest jako zbiór następujących elementów:

- zakład produkcyjny wraz z zasobami ludzkimi i zachodzącymi między nimi relacjami;
- środki transportu wraz z zasobami ludzkimi i zachodzącymi między nimi relacjami;
- magazyny z zasobami ludzkimi i zachodzącymi między nimi relacjami;
- odbiorca – zakład lub osoba wykorzystuje gotowy, dostarczony produkt[5].

Głównymi elementami systemu logistycznego są:

- fizyczne przepływy surowców, materiałów, towarów i usług;
- strumienie informacyjno-decyzyjne sterujące tym przepływem;
- zapasy materiałów rzeczowych;
- infrastruktura oraz koszty logistyczne[6].

Na etapie definiowania procesu zabezpieczenia technicznego systemu logistycznego należy wskazać elementy, które muszą podlegać ochronie. Ich zdefiniowanie następuje po oględzinach, audycie, analizach i przeprowadzeniu procesu wnioskowania.

Ważnym elementem jest środek transportu, najtrudniejszy do skutecznego zabezpieczenia z uwagi na jego ciągłe przemieszczanie się w terenie, przy zmieniających się warunkach otoczenia. Środek transportu, w zależności od jego przeznaczenia, może zostać wyposażony w: system alarmowy, system telewizji przemysłowej i system monitorowania GPS (*Global Positioning System*). Obecnie środki transportowe już w wyposażeniu fabrycznym posiadają szereg funkcji zapewniających bezpieczeństwo osobie nadzorującej pojazd (wraz z towarem), co powoduje, że w przypadku wystąpienia sytuacji krytycznej nastąpi wykrycie niebezpieczeństwa i skuteczne powiadomienie o takiej niepożądanej sytuacji[7]. Dostępność magistral (np. CAN – sieć *Controller Area Network*) w środku transportowym wspomaga procesy: analiz, zbierania komunikatów alarmowych i przesyłania danych.

Typowym przykładem takiego ostrzegawczego działania może być:

- nadmierna prędkość,
- zatrzymanie pojazdu,
- tankowanie,
- niebezpieczne przechyły,
- zmęczenie kierującego,

---

[5] A. Sadowski (2006). *System logistyczny w przedsiębiorstwie – ujęcie teoretyczne.* „Przegląd Organizacji", nr 3(794), s. 43–44.

[6] *Ibidem*.

[7] S. Panecki (2013). *Interfejs komunikacyjny CAN: podstawy.* https://mikrokontroler.pl/2013/06/10/interfejs-komunikacyjny-can-podstawy/ [dostęp: 11.09.2024].

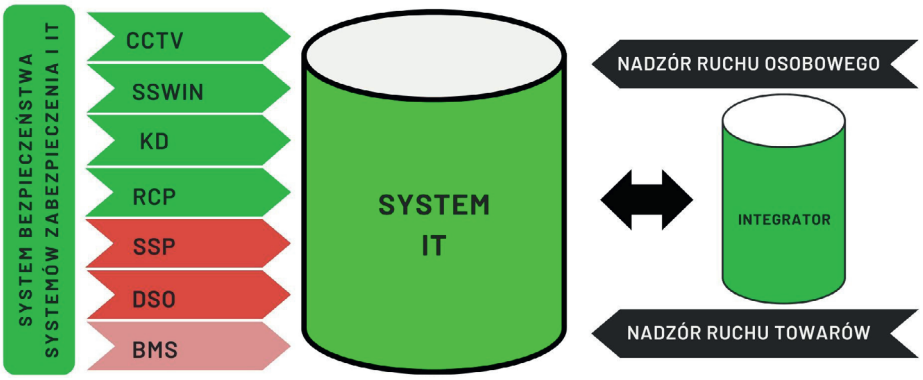
– zjazd z określonej trasy przejazdu[8].

Tworzone w obecnych technologiach systemy zabezpieczenia technicznego systemów logistycznych są integrowane na platformach cyfrowych. Zapewniają one szybki i wygodny dostęp do urządzeń oraz mechanizmów zarządzania. Takie rozwiązania wymagają jednak sporych nakładów finansowych potrzebnych do opracowania oraz wdrożenia zabezpieczeń tożsamych z zabezpieczeniami funkcjonującymi w systemach informatycznych.

System zabezpieczenia technicznego to: *zespół połączonych ze sobą środków technicznych i organizacyjnych tworzących rozwiązania wspomagające w ochronie osób i mienia w systemach logistycznych*[9].

Tabela 2. System zabezpieczenia technicznego

System zabezpieczenia technicznego – Zespół połączonych ze sobą środków technicznych i organizacyjnych tworzących rozwiązania wspomagające w ochronie osób i mienia w systemach logistycznych.



Źródło: opracowanie własne.

Lista systemów zabezpieczeń technicznych stosowanych w logistyce nie jest zamknięta i jest uzależniona od konkretnej struktury logistycznej, która podlega ochronie, a zastosowanie odpowiednich narzędzi powinno być efektem szczegółowej analizy związanej z jej specyfiką i wrażliwością na ewentualny zamach.

Zabezpieczanie śladów i dowodów w postępowaniu karnym

Zabezpieczanie śladów zdarzenia jest bardzo istotnym elementem działań podejmowanych przez służby odpowiedzialne za porządek i bezpieczeństwo. Najczęściej prowadzane jest podczas tzw. czynności procesowych, a w szczególności w trakcie

[8] *Ibidem*.

[9] Zob. P. Pajorski (2015). *Systemy zabezpieczenia technicznego w służbie ochrony osób*. „Security, Economy & Law" Nr 4 (IX), s. 135–137.

oględzin[10]. Ich przeprowadzenie jest czynnością procesową, najczęściej wykonywaną po złożeniu zawiadomienia o zdarzeniu przestępczym[11].

Ślady występują w wyniku działania sprawców i są nierozłącznym elementem czynności przestępczych[12]. Każde działanie pozostawia ślady fizyczne w świecie realnym i cyfrowe w świecie wirtualnym. Te ostatnie stwarzają iluzję, że znikają w wyniku kasowania plików lub gdy użytkownik opuszcza przeglądarkę internetową. Faktycznie jednak zapisane na serwerach dane pozostają na nich bardzo długo i stanowią często podstawę efektywności działań w procesie śledczym[13]. Wiedza o zabezpieczaniu śladów jest niezbędna w procesach:

- analizy ryzyka,
- projektowych,
- wykrywania ryzyka,
- szkoleniowych.

Jeżeli posiadamy wiedzę o śladach, znamy również sposoby ich nanoszenia przez potencjalnego sprawcę. Z kolei znając te sposoby, można podjąć działania eliminujące lub ograniczające przedostanie się sprawcy na teren lub do obiektu bez pozostawienia śladów. Jeżeli sprawca pozostawił określone ślady, to na ich podstawie można przeprowadzić zarówno proces wykrywczy, jak i przygotować odpowiednie działania o charakterze profilaktycznym. Wiedza o śladach poprawia jakość audytu bezpieczeństwa obiektów, obszarów i urządzeń pod kątem stosowanych rozwiązań technicznych i fizycznych. Znajomość tej problematyki pozwala na wypracowanie lepszych jakościowo rozwiązań projektowych, co implikuje także realne oszczędności, pozwalając uniknąć tzw. przewymiarowania systemu lub wyeliminować kosztowną ochronę fizyczną. Wiedza ta jest ściśle związana ze znajomością sposobów działania sprawców, co pozwala także na trafne przewidywanie skutków przestępczych działań. Ponadto, im więcej śladów jesteśmy w stanie rozpoznać i zabezpieczyć, tym lepiej poznajemy metodykę działania sprawców – ich *modus operandi*[14]. To z kolei pozwala na przygotowanie adekwatnych rozwiązań zabezpieczających, które nie mogą być szablonowe, wymagają stałego testowania i ciągłej weryfikacji.

Nie każdy jednak ślad zabezpieczony w toku postępowania jest dowodem. Dowodem jest ślad, który nie pozwala na zanegowanie jego wartości. Zatem niektóre ślady są bezużyteczne lub jedynie poszlakowe[15] i muszą zostać wsparte innymi. Przykładem może tu być odcisk palca, który pozwala na odnalezienie – najlepiej 14 – cech wspólnych

[10] Ustawa z dnia 6 czerwca 1997 r. Kodeks Postępowania Karnego, Dz. U. 1997 Nr 89 poz. 555, art. 207.

[11] *Ibidem*, art. 304.

[12] M. Goc, J. Moszczyński (2017). *Ślady kryminalistyczne Ujawnianie, zabezpieczanie, wykorzystanie*. Warszawa, s. 17.

[13] Więcej: W.A. Kasprzak (2015). *Ślady cyfrowe. Studium prawno-kryminalistyczne*. Warszawa, s. 246.

[14] M. Sąsiada. *Modus operandi jako środek identyfikacji sprawcy przestępstwa*, s. 204–222. https://repozytorium.uni.wroc.pl/en/dlibra/publication/22385/edition/29211/modus-operandi-jako-srodek-identyfikacji-sprawcy-przestepstwa-sasiada-monika [dostęp: 20.09.2024].

[15] P. Kruszyński (2004). *Wykład Prawa Karnego Procesowego*. Białystok, s. 254.

z materiałem pobranym[16]. Wprawdzie ślad niespełniający takich warunków można byłoby odrzucić, ale poszlakowo należy go uwzględnić i dążyć do uzupełnienia go kolejnym. W przypadku śladu cyfrowego[17] można przywołać wizerunek osoby (z systemu monitoringu), która przemieszczała się w miejscu wystąpienia zamachu, godzinę przed jego przeprowadzeniem. To także tylko poszlaka, ale uzupełniona kolejnym śladem może mieć już wartość dowodową.

Umiejętność zebrania i zabezpieczenia dowodów jest warunkiem szybkiego i skutecznego postępowania przygotowawczego[18].

Jeżeli jesteśmy w stanie ujawnić ślady oraz prawidłowo je zabezpieczyć na miejscu zdarzenia lub w innym miejscu (np. podczas przesłuchania czy przeszukania), mamy możliwość ich procesowego wykorzystania. Prawidłowe zabezpieczenie śladów polega na odnalezieniu cech szczególnych określonej materii, jednoznacznie wskazujących ich powiązania z faktami będącymi przedmiotem postępowania[19].

Studium przypadku

Pierwsza poddana analizie sprawa dotyczyła kradzieży z włamaniem do przedsiębiorstwa zajmującego się dystrybucją płynów technologicznych. Firma ta zlokalizowana była w dużym obiekcie, w centrum Krakowa. Obiekt był ogrodzony, ale nie posiadał odpowiedniego oświetlenia. Wzdłuż ogrodzenia przebiegała droga szutrowa umożliwiająca poruszanie się po niej lekkich samochodów ciężarowych. Pomiędzy drogą i ogrodzeniem był pas ziemi o szerokości około 1,5 m. Obiekt nie posiadał ochrony fizycznej sprawowanej przez firmę ochrony osób i mienia. Był wyposażony w analogowy system monitoringu wizyjnego oraz system alarmowy. W dziale technicznym przedsiębiorstwa nie było dokumentacji technicznej dotyczącej obiektu. Na obszarze wewnętrznym zakładu zlokalizowane były bocznice kolejowe, na które wjeżdżały cysterny z płynem koniecznym do procesów technologicznych. Cysterny te przed ich opróżnieniem były ważone oraz sprawdzane pod kątem objętości, a następnie oczekiwały na rozładunek – od 2 do 3 dni. Cechą charakterystyczną przewożonych płynów była ich rozszerzalność pod wpływem temperatury. Sprawcy włamywali się na teren obiektu, a potem do cystern. Dokonywali kradzieży płynu, a następnie wodą uzupełniali jego niedobór. Jakość płynu ulegała degradacji i niemożliwe było wykorzystanie go do procesów technologicznych. Tym samym nastąpiło przerwanie łańcucha produkcji spożywczej i branży medycznej[20].

---

[16] I. Bogusz. M. Bogusz. *Ślady kryminalistyczne dla słuchaczy szkolenia zawodowego podstawowego*. Legionowo, s. 15–20.

[17] H. Gaweł. *Analiza śladów cyfrowych z perspektywy informatologii i cyberbezpieczeństwa*, s. 65–81. https://ruj.uj.edu.pl/server/api/core/bitstreams/f7024af4-fbce-446e-bb95-e459e668182a/content [dostęp: 28.09.2024].

[18] J. Gąsiorowski (2016). *Nowoczesne technologie w Kryminalistyce*. „Kultura Bezpieczeństwa Nauka – Praktyka – Refleksje" Nr 21, s. 73–114.

[19] L. Biliński, W. Miś (2009). *Kryminalistyczno-procesowe zabezpieczanie śladów na miejscu zdarzenia*. Piła, s. 7–19.

[20] Sprawa dochodzeniowa prowadzona przez T. Malinowskiego w trakcie jego służby w krakowskiej Policji.

Podczas czynności dochodzeniowo-śledczych na miejscu zdarzenia odnaleziono: ślady opon, obuwia i zwierzęcia. Wszystkie nadawały się do identyfikacji. Zabezpieczono je technicznie przed zniszczeniem. Już na miejscu zdarzenia, na podstawie tych śladów, śledczy przyjął założenie, że: sprawca przyjechał samochodem, wysiadł lewymi przednimi drzwiami, a tylnymi lewymi drzwiami wypuścił z samochodu psa. Po sposobie poruszania się sprawcy, ichnogramie (pozostawionych śladach obuwia), policjant wywnioskował, że sprawca utykał na prawą nogę, był otyły i miał około 180 cm wzrostu. Funkcjonariusz ustalił drogę pokonaną przez sprawcę i odnalazł ukryte przez niego przedmioty służące do popełnienia przestępstwa. Ujawnił na nich ślady linii papilarnych. W toku postępowania wykrywczego zastosowano pułapki kryminalistyczne. Dalsze ekspertyzy śladów i zebrany w trakcie przesłuchań materiał doprowadziły do wytypowania, identyfikacji, a finalnie zatrzymania sprawców kradzieży.

W analizowanym przypadku śledczy na miejscu zdarzenia zabezpieczyli dodatkowo materiał cyfrowy pochodzący z systemów zabezpieczenia technicznego. Były to:

- nagranie z dysku rejestratora;
- lista zdarzeń z systemu alarmowego;
- lista zdarzeń z integratora (platforma zarządzania systemami bezpieczeństwa).

Analiza całościowa zebranego cyfrowego materiału dowodowego doprowadziła do utrwalenia dowodów i potwierdzenia sposobu działania sprawcy. W wyniku tych działań otrzymano wiele informacji, a w szczególności:

- historię działania sprawcy,
- precyzyjną lokalizację momentów kluczowych,
- sposób i metodę działania sprawcy,
- wskazanie przedmiotów podlegających szczególnemu zainteresowaniu sprawcy,
- wskazanie osób odpowiedzialnych,
- zachowanie sprawcy i osób z nim powiązanych z wnętrza organizacji,
- dane niezbędne do rekonstrukcji zdarzenia.

Prawidłowo zabezpieczone logi, materiał wideo oraz audio to niepodważalne elementy w procesie, który jest oparty na łańcuchu dowodowym. Ustalono, że kradzieże płynów były możliwe dzięki powiązaniom przestępczym pracowników zakładu z grupą paserów, ich znajomością procesów technologicznych oraz sposobów zabezpieczenia mienia na terenie firmy (rozmieszczenie kamer, obchody stróża). W dalszej odsprzedaży płynów uczestniczył paser zatrudniający firmę transportową.

W opisywanym przypadku siły i środki łańcucha bezpieczeństwa zastosowane do ochrony łańcucha dostaw okazały się niewystarczające. Nie pozwalały również na jednoznaczną identyfikację sprawcy i stanowiły jedynie poszlakę w postępowaniu przygotowawczym, co znacznie spowolniło proces wykrywczy. Podobne rozwiązania analogowe są niestety nadal stosowane z uwagi na ograniczanie kosztów ochrony przez przedsiębiorców.

Analizowana sprawa wykazała, iż podwyższenie poziomu technologicznego ochrony wiąże się z koniecznością zastosowania zaawansowanych systemów informatycznych.

Druga poddana analizie sprawa[21] także dotyczyła zamachu na system logistyczny. Była to kradzież z włamaniem do sklepu z luksusową odzieżą (nastąpiło tu przerwanie łańcucha dostaw do odbiorcy końcowego). W wyniku tego przestępstwa sklep oraz magazyny zlokalizowane w obiekcie, zaopatrujące inne placówki handlowe, nie mogły działać przez 8 godzin, co spowodowało duże straty finansowe. Sklep zlokalizowany był w centrum miasta, w obiekcie wolnostojącym. Ochrona obiektu została wykonana zgodnie z najlepszą wiedzą techniczną. Systemy IT zainstalowane wewnątrz były platformą integracji elementów systemu ochrony (kamery IP, rejestrator IP, system sygnalizacji włamania i napadu z interfejsem IP). Sprawca przed atakiem dokonał rozpoznania przestępczego, ustalając możliwe drogi wejścia do obiektu oraz rozmieszczenie i sposób funkcjonowania urządzeń chroniących obiekt. Między innymi ustalił ruch personelu oraz kilkukrotnie wzbudził system alarmowy. Pozyskał również zaufanie jednego z pracowników, który przekazał mu istotne informacje o funkcjonowaniu obiektu. Niestety przyczyny wzbudzania systemu alarmowego nie zostały przeanalizowane przez dział techniczny. Pracownik serwisu wyłączył system na jedną noc, a informacja ta dotarła do sprawcy. W dniu braku reakcji serwisowej sprawca przyszedł do sklepu, przedostał się do magazynu i pozostał w nim na noc. Dokonał kradzieży zegarków i odzieży o dużej wartości i opuścił obiekt. Jego wizerunek został zarejestrowany przez system kamer.

W opisywanym przypadku siły i środki łańcucha bezpieczeństwa zastosowane do ochrony łańcucha dostaw okazały się wystarczające w zakresie organizacyjno-technicznym. Wystąpiły tu następujące fazy przygotowania systemu ochrony:

- analiza bezpieczeństwa;
- analiza ryzyka;
- opracowanie koncepcji zabezpieczenia;
- sprawdzenie koncepcji;
- wykonanie projektu systemu;
- realizacja systemu;
- nadzór nad procesem realizacji;
- testowanie systemu;
- nadzór nad testowaniem;
- wdrożenie systemu;
- nadzór nad wdrożeniem;
- test końcowy;
- przekazanie systemu użytkownikowi;
- użytkowanie.

Na podstawie wyników testów ustalono, że gromadzony przez urządzenia elektroniczne materiał cyfrowy i logi posiadają walory użytkowe i nie będą powodowały zniekształceń podczas prowadzonych czynności dochodzeniowo-śledczych.

W analizowanej sprawie śledczy na miejscu zdarzenia zabezpieczyli materiał dowodowy w postaci wielu śladów oraz dodatkowo materiał cyfrowy pochodzący z systemów zabezpieczenia technicznego oraz systemu IT. Zainstalowany sprzęt ochrony

[21] Sprawa dochodzeniowa prowadzona przez T. Malinowskiego w trakcie jego służby w krakowskiej Policji.

technicznej oraz fizycznej spełniał oczekiwania policjantów i można było, bez żadnych wątpliwości, rozpoznać sprawcę przestępstwa. Zabezpieczonymi w toku postępowania materiałami były:

- nagranie z dysku rejestratora;
- logi rejestratora;
- logi z systemu alarmowego;
- lista zdarzeń z systemu alarmowego;
- logi z systemu IT.

Analiza całościowa zebranego cyfrowego materiału dowodowego doprowadziła do utrwalenia dowodów i potwierdzenia sposobu działania sprawcy. W wyniku tych działań otrzymano wiele informacji, a w szczególności:

- historię działania sprawcy;
- precyzyjną lokalizację momentów kluczowych;
- sposób i metodę działania sprawcy;
- wskazanie przedmiotów podlegających szczególnemu zainteresowaniu sprawcy;
- dane pomocne do rekonstrukcji zdarzenia.

Trzecia poddana badaniu sprawa[22] dotyczyła fazy wstępnej tworzenia systemu logistycznego przez jedną z krakowskich firm. Właściciel miał przedstawić swoim partnerom biznesowym prezentację, z której wynikało, iż biznesplan jest zasadny, a inwestycja będzie podlegała szybkiemu zwrotowi. Zarządzanie systemem logistycznym miało być oparte w całości na systemie IT, bez konieczności udziału czynnika ludzkiego. W firmie znajdował się już system IT w pełni monitorowany przez aplikację oraz urządzenia i oprogramowanie gromadzące logi.

W tym przypadku działania przestępcze polegały na dążeniu do „skompromitowania" przez sprawcę jego współpracownika z działu bezpieczeństwa IT, z którym wspólnie mieli przygotować prezentację nowo budowanego systemu. Gdy prezentacja była już na ukończeniu, sprawca zapisał ostateczną wersję na dysku swojego komputera. Równocześnie poprosił współpracownika o wykonanie jeszcze jednego slajdu do prezentacji. W tym celu przesłał mu plik zawierający wirus. Sprawca ze swojego komputera usunął ślady działania przestępczego i nakłonił współpracownika do usunięcia plików z poczty elektronicznej.

Pracownik w dobrej wierze wykonał dodatkowy slajd do prezentacji, nie wiedząc, że w trakcie tej pracy otwiera plik z wirusem. W wyniku zainfekowania komputera ofiary nastąpiło zniszczenie wykonanej pracy oraz degradacja systemu operacyjnego i plików komputera. Sprawca za pomocą dostępnych narzędzi IT sprawdził stan komputera ofiary i prezentacji, by upewnić się, że nie ma już plików z wykonaną pracą. Przesłał będące w jego posiadaniu pliki do przełożonego z komentarzem, iż współpracownik nie potrafił wykonać zamówionej przez niego prezentacji. Ofiara po uzyskaniu informacji o szczegółach zamachu[23] dokonała zgłoszenia o popełnieniu przestępstwa.

---

[22] Sprawa prowadzona przez autorów w ramach konsultacji zleconej przez pracownika (ofiarę) działu bezpieczeństwa IT jednej z krakowskich firm.

[23] *Ibidem*.

Na miejscu opisanego zdarzenia zabezpieczono:
- logi z serwerów;
- logi z komputerów;
- logi z urządzeń sieciowych;
- logi z systemu monitorującego ruch sieciowy;
- konwersację na platformie wymiany informacji;
- plik z wirusem do analizy;
- dokumentację techniczną systemów informatycznych;
- dokumentację wytworzoną przez firmę, która wykonała między innymi politykę bezpieczeństwa oraz regulaminy;
- uzyskano inne informacje za pomocą dostępnych narzędzi IT.

Analiza całościowa zebranego cyfrowego materiału dowodowego doprowadziła do utrwalenia dowodów i potwierdzenia sposobu działania sprawcy. W wyniku tych działań otrzymano wiele informacji, a w szczególności:
- historię działania sprawcy;
- precyzyjną lokalizację momentów kluczowych;
- sposób i metodę działania sprawcy;
- wskazanie przedmiotów podlegających szczególnemu zainteresowaniu sprawcy;
- dane do rekonstrukcji zdarzenia.

Czyn został udowodniony, a jego sprawca został zwolniony z firmy i poniósł konsekwencje prawno-karne.

Badanie wybranych spraw pozwoliło na stwierdzenie, iż prawidłowo zabezpieczone logi z systemów oraz materiał wideo i audio to niepodważalne elementy w procesie, na którym oparty jest łańcuch dowodowy.

Przeprowadzona w ramach studium przypadku analiza zdarzeń zaistniałych w świecie realnym i zdarzenia w cyberprzestrzeni wykazała istnienie wyraźnych podobieństw pomiędzy zamachami przeprowadzonymi w tych dwóch, różnych środowiskach.

Poniżej wskazano wybrane działania i efekty pracy dochodzeniowo-wykrywczej[24], które odnoszą się do zdarzeń zaistniałych w świecie rzeczywistym i cyfrowym (wirtualnym).

W środowisku realnym, po zawiadomieniu o zamachu na system logistyczny, dokonuje się:
- zabezpieczenia miejsca zdarzenia;
- oględzin miejsca zdarzenia;
- zabezpiecza się ślady;
- zeznaniami świadków ustala się i dokumentuje fakty i inne elementy;
- zabezpiecza się inne materiały jako dowody w sprawie (mogą to być: dokumentacje, materiał wideo i audio, wyciągi z historii działania systemu alarmowego, kontroli dostępu, systemu informującego o pożarze, systemu automatyki budynkowej).

[24] Wytyczne nr 3 Komendanta Głównego Policji z dnia 30 sierpnia 2017 r. w sprawie wykonywania niektórych czynności dochodzeniowo-śledczych przez policjantów, Dz.Urz.KGP.2017.59.

W oparciu o zebrane w toku postępowania materiały możliwe jest ustalenie:
- historii działania sprawcy;
- precyzyjnej lokalizacji momentów kluczowych;
- sposobu i metod działania sprawcy;
- przedmiotów podlegających szczególnemu zainteresowaniu sprawcy;
- drogi ucieczki sprawcy.

W środowisku wirtualnym po zawiadomieniu o zamachu na system logistyczny dokonuje się:
- zabezpieczenia miejsca zdarzenia;
- oględzin miejsca zdarzenia;
- zabezpieczenia śladów;
- przesłuchań świadków celem ustalenia i udokumentowania faktów;
- zabezpieczenia innych materiałów jako dowodów w sprawie (mogą to być: dokumentacje, materiały wideo i audio, wyciągi z historii działania systemu alarmowego, kontroli dostępu, systemu informującego o pożarze, systemu automatyki budynkowej);
- zabezpieczenia logów z systemów IT;
- zabezpieczenia dokumentacji związanej z bezpieczeństwem systemów IT.

W oparciu na zebranych w toku postępowania materiałach możliwe są do ustalenia:
- historia działania sprawcy;
- precyzyjna lokalizacja momentów kluczowych;
- sposób i metoda działania sprawcy;
- wskazanie przedmiotów podlegających szczególnemu zainteresowaniu sprawcy;
- poznanie drogi ucieczki sprawcy.

Porównanie zdarzeń przestępczych zaistniałych w świecie fizycznym (realnym) i wirtualnym wskazuje na bardzo duże podobieństwo w obszarze sposobów i motywów działania sprawców. W obu sytuacjach najczęstszymi motywami działania są:
- chęć osiągnięcia zysku majątkowego. Zysk może mieć różny charakter np. zdobycie środków finansowych lub pozbawienie kogoś majątku. Ten rodzaj zysku zawiera duży ładunek emocjonalny sprawcy lub osoby zlecającej realizację czynu przestępczego;
- chęć osiągnięcia zysku emocjonalnego, który może mieć różny charakter np. zaspokojenie emocji własnych lub osoby zlecającej realizację czynu przestępczego. Przestępstwa te mają bardzo często powiązanie z elementami motywów działań na tle społecznym, seksualnym, ideologicznym, politycznym.

Do grupy przestępstw związanych z osiąganiem zysku emocjonalnego można też zaliczyć przestępstwa wynikające z uzależnień, takich jak narkomania czy alkoholizm. Zakres motywów działania sprawców jest bardzo szeroki, stąd trudno wyszczególnić wszystkie jego elementy. Zakres ten nigdy nie jest jednoznaczny i łączy w sobie wiele czynników ulegających zmianie podczas cyklu przestępczego, czyli od zamiaru, poprzez realizację i osiągniecie (lub nie) zamierzonego celu[25].

[25] K. Daszkiewicz (1961). *Motyw przestępstwa.* „Palestra" 5/9(45), s. 62–64

Przeprowadzona w ramach studium przypadku analiza trzech spraw kryminalnych pozwoliła na wskazanie nie tylko podobieństw, ale też wyraźnej różnicy pomiędzy śladami przestępstw pozostawianymi w środowisku fizycznym i wirtualnym. Nie można bowiem zostawić śladu traseologicznego[26] lub osmologicznego[27] na dysku twardym komputera podczas włamania do systemu informatycznego (IT), jak również nie można zostawić adresu charakterystycznego dla urządzenia pracującego w systemie informatycznym (IP) w miejscu włamania do obiektu. Model działania sprawców w tych różnych środowiskach jest inny, pomimo możliwej zbieżności interesów oraz podobnych stanów emocjonalnych wykazywanych przez przestępców[28].

Analiza OSINT

Gdy zawiodą podstawowe techniki śledcze, może nastąpić zatrzymanie procesu wykrywczego i konieczne jest odniesienie się do przeszłości, czyli stanu sprzed dokonania zamachu lub do przebiegu bieżących zdarzeń. W pracy dochodzeniowej trzeba mieć na uwadze, iż nie ma całkowitej anonimowości sprawcy tak w świecie rzeczywistym, jak i cyfrowym. Efektywną metodą jest na tym etapie dochodzenia przeprowadzanie wywiadów w świecie rzeczywistym i cyfrowym. W tym pierwszym są to rozmowy z ludźmi (rozpytanie, przesłuchanie), które zawsze mogą być obciążone błędem percepcji oraz ułomnością pamięci ludzkiej.

Z badań wynika, iż ograniczenia te nie występują w świecie cyfrowym. Zapisane na serwerach informacje nie są bowiem obarczone subiektywnym postrzeganiem rzeczywistości. Często dostęp do nich jest ograniczony. Szukanie informacji wstecznych to tzw. OSINT[29]. To metoda polegająca na używaniu dostępnych, „otwartych" narzędzi i szukaniu informacji w otwartych bazach danych. Ta forma działania potocznie bywa określana jako „biały wywiad".

Analiza OSINT przeprowadzona przez służby może doprowadzić do ukierunkowania na sprawcę zamachu. Należy jednak pamiętać, że służby nie opierają się wyłącznie na „białym wywiadzie". Prowadzą także wywiad „szary" i „czarny", charakteryzujące się niekiedy głęboką ingerencją w życie obywateli. W tej fazie istotnym elementem związanym z procesem wykrywczym jest analiza materiałów archiwalnych. Typowymi przykładami materiałów archiwalnych cyfrowych są:

- materiał z monitoringów wizyjnych i audio – zapisane pliki oraz logi systemowe;
- materiał z systemów alarmowych – zapisane pliki z logami oraz pliki konfiguracyjne;
- pliki z serwerów zawierające monitoring ruchu sieciowego;
- pliki z serwerów zawierające logi logowań;

[26] K. Kozdrój-Miler, J. Jędraszek, K. Klemczak (2022). *Ujawnianie śladów traseologicznych*. „Problemy Kryminalistyki" 315(1), s. 34–47.

[27] R. Bączyk (2011). *Ślady osmologiczne*. Słupsk, s. 9.

[28] J. Gołębiowski (2021). *Umysł przestępcy. Tajniki kryminalnego profilowania psychologicznego*. Kraków, s. 37–44.

[29] B. Saramak (2015). *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*. Warszawa, s. 19–22.

- pliki z serwerów zawierające inne logi aplikacji;
- pliki z serwerów zawierające logi zarządzania sieciami;
- pliki z serwerów bazodanowych zawierające logi;
- pliki z serwerów systemów ochrony systemu IT zawierające logi;
- pliki z serwerów BMS – sterowanie budynkiem;
- pliki z serwerów KD – kontrola dostępu.

W fazie planowania ataku przestępczego następuje pozostawianie przez sprawców wielu śladów związanych z przygotowaniem przestępczego działania. Na tym etapie sprawca pozostaje jeszcze anonimowy, a potencjalne ofiary często odczytują jego zachowania jako działanie w dobrej wierze (wykorzystywanie socjotechnik). Sprawcy stosują różne socjotechniki. Typowy przykład to zaangażowanie sprawców w rzekome niesienie pomocy swoim ofiarom: *Pomogę Ci posprzątać sklep, zostaw mi hasło do alarmu. Podaj hasło to pomogę Ci opracować materiały na konferencję, przecież nie masz na to czasu*.

Bardziej wyrafinowane metody to zastosowanie socjotechniki w stosunku do pracowników mających dostęp do obiektu i kluczy lub też socjotechniki realizowane w systemach „IT" zmierzające do wyłudzenia haseł (ataki na konta wrażliwe).

Podejmowane są też metodyczne działania w zakresie skanowania sieci komputerowych w celu realizacji kolejnych, bardziej odległych działań. Typowym przykładem jest tu tzw. wpuszczenie kreta, czyli osoby, która rozpracowuje działanie obiektu fizycznego w sytuacjach rzeczywistych (np. pracownik ochrony zatrudnia się do montażu systemów alarmowych) lub sieci IT w działaniach wirtualnych (np. pracownik działu IT). W wyniku takich aktywności sprawców następuje przełamanie zabezpieczeń technicznych lub cyfrowych. W takim przypadku[30] najczęściej uszkodzeniu ulegają elementy mechaniczne takie jak: zamki, skrzydła drzwiowe, szyby, okna itd.

W przypadku przełamania zabezpieczeń fizycznych (w systemach cyfrowych) brak jest widocznych uszkodzeń fizycznych, natomiast występują np. zmiany w cechach plików. Bardzo ważne są tu logi systemowe[31]. Trzeba podnieść walor ustawień czasowych i zgodności logów z serwerami czasu. Przy założeniu, że pracownik IT dokonuje synchronizacji czasu za pomocą serwerów, rola logów wzrasta do dowodu wyznaczającego czas poruszania się sprawcy w środowisku poszkodowanego. W przypadku ustalenia, że logi systemowe generują się bez serwera czasu, ich rola jako materiału dowodowego będzie jednak wątpliwa[32]. Zatem w pierwszej kolejności sprawdzeniu i zabezpieczeniu muszą podlegać logi systemowe, konfiguracyjne, na podstawie których następuje ustalenie, czy kolejne logi mogą zostać określone jako dowód w sprawie.

Innym bardzo istotnym elementem w świecie wirtualnym jest monitoring systemów informatycznych, który obejmuje kompleksowo system zabezpieczenia systemu

[30] M. Szustakowski, W. Ciurapiński. *Techniczne systemy zabezpieczenia mienia i infrastruktury krytycznej*. https://certus.edu.pl/rzeszow/wp-content/uploads/2020/11/30_techniczne_systemy_zabezpieczenia_mienia_i_infrastruktury_krytycznej-1.pdf, s. 2–4 [dostęp: 30.10.2024].

[31] H. Gaweł. *Analiza śladów cyfrowych z perspektywy informatologii i cyberbezpieczeństwa*. https://ruj.uj.edu.pl/server/api/core/bitstreams/f7024af4-fbce-446e-bb95-e459e668182a/content, s. 66–81 [dostęp: 02.11.2024].

[32] J. Widacki (2002, wyd. 2). *Kryminalistyka*. Warszawa, s. 192.

logistycznego. Za pomocą systemu monitorowania „sieci" następuje śledzenie ruchu, a zatem generowanie kolejnych logów, które zawierają dowody działania sprawcy.

W przypadku systemów informatycznych ważne ślady pozostające w logach systemowych to:

- zapisy logowań;
- zmiany w plikach;
- aktywność w aplikacjach;
- aktywność sieciowa[33].

Sprawcy przestępstw podejmują także próby obniżenia wartości dowodowej śladów pozostawianych przez siebie śladów. Są to działania ukierunkowane na niszczenie śladów na miejscu zdarzenia.

Jednym z podstawowych sposobów działania sprawców jest ukrywanie tożsamości poprzez maskowanie. W świecie realnym sprawcy używają masek do zakrywania twarzy, farb do niszczenia kamer, ubrań strażackich do oszukania czujników lub innych elementów odzieży celem wprowadzenia w błąd urządzeń analityki AI. Bardzo często stosują na miejscach zdarzeń środki niszczące ślady i uniemożliwiające skuteczne użycie np. psa tropiącego. W systemach cyfrowych sprawcy ukrywają swoją tożsamość poprzez stosowanie VPN, proxy czy szyfrowania. Coraz częściej do ukrycia tożsamości używane są narzędzia AI, które odpowiednio zastosowane, zmieniają wygląd oraz głos sprawcy. Wybór metody maskowania jest uzależniony od wyposażenia obiektu lub sieci komputerowej w systemy bezpieczeństwa. W obiektach handlowych są to: zamki, alarmy, kamery. W systemach informatycznych są to: firewalle, systemy detekcji włamań (IDS), oprogramowanie antywirusowe. W obiektach handlowych może być także stosowana fizyczna kontrola dostępu (strażnicy, karty systemu kontroli dostępu), a w systemach informatycznych mechanizmy uwierzytelniania i autoryzacji (hasła, tokeny, certyfikaty).

Wnioski

Przeprowadzony proces badawczy pozwolił na uzyskanie odpowiedzi na postawione problemy szczegółowe. Ustalono, że system logistyczny ma charakter złożony, a jego głównymi elementami są: fizyczne przepływy surowców, materiałów, towarów i usług, strumienie informacyjno-decyzyjne nim sterujące, zapasy materiałów rzeczowych oraz infrastruktura logistyczna wraz z kosztami. Wskazano, że współczesne systemy logistyczne ze względu na swoje znaczenie muszą podlegać dostosowanym do ich specyfiki systemom zabezpieczeń technicznych tworzonym w oparciu na najnowszych technologiach pozwalających na ich pełną integrację na platformach cyfrowych zapewniających szybki i wygodny dostęp do wszystkich urządzeń oraz mechanizmów zarządzania[34].

W toku badań ustalono także, iż każdy zamach, jako działanie człowieka, pozostawia ślady fizyczne zarówno w świecie realnym, jak i cyfrowym. Wykazano, że wartość dowodową ma jedynie taki ślad, który w procesie jego weryfikacji nie pozwala na

[33] H. Gaweł. *Analiza śladów cyfrowych… Op. cit.* [dostęp: 02.11.2024].

[34] A. Bujak, J. Kłosowski (2014). *System logistyczny przedsiębiorstwa i jego parametry*. „Logistyka" nr 3/2014, s. 882–890.

zanegowanie jego wartości procesowej. Zauważono, iż nawet ślady z pozoru bezużyteczne czy o charakterze poszlakowym mogą mieć istotne znaczenie, jeśli zostaną uzupełnione innymi środkami dowodowymi.

Z badań wynika, że w przypadku systemów informatycznych w logach systemowych pozostają ważne ślady widoczne w zapisach logowań, zmiany w plikach, aktywność w aplikacjach i sieci. To z kolei pozwala, w przypadku stwierdzonego zamachu na system logistyczny, otrzymać wiele kluczowych informacji pozwalających na rekonstrukcję działania sprawcy, precyzyjną lokalizację istotnych momentów zdarzeń, określenie *modus operandi* sprawcy, wskazanie przedmiotów będących w jego zainteresowaniu, analizę zachowań sprawcy i ewentualnie osób z nim powiązanych, a nawet identyfikację sprawcy[35].

Badania pozwoliły na zidentyfikowanie działań sprawców zamachów zmierzających do osłabiania wartości dowodowej śladów rejestrowanych w systemach cyfrowych. Sprawcy koncentrują swe działania na ukryciu swej tożsamości poprzez stosowanie VPN, proxy oraz szyfrowanie, coraz częściej wykorzystując także narzędzia AI, które umożliwiają zmianę wyglądu[36], a nawet głosu sprawcy[37].

Poczynione w procesie badawczym ustalenia pozwoliły finalnie na udzielenie odpowiedzi na główny problem badawczy, wskazując możliwości wykorzystania śladów zamachu w podwyższaniu poziomu bezpieczeństwa systemów logistycznych.

Ustalono, że analiza zebranych śladów cyfrowych pozwala na utrwalenie dowodów i potwierdzenie sposobu działania sprawcy. Prawidłowo zabezpieczone logi, materiał wideo czy audio to niepodważalne elementy w procesie karnym opartym na łańcuchu dowodowym. Pozostawione przez sprawcę ślady umożliwiają efektywny proces wykrywczy i pozwalają na podjęcie działań o charakterze profilaktycznym. Stwarzają także bazę do wypracowania optymalnych rozwiązań projektowych w zakresie zabezpieczania technicznego systemów logistycznych.

Uzyskanie odpowiedzi na główny problem badawczy pozwoliło na zrealizowanie określonego celu badań i będzie stanowiło przyczynek do dalszych badań ukierunkowanych na wskazanie propozycji działań, zmierzających do poprawy zabezpieczeń technicznych systemów logistycznych.

Bibliografia

Bączyk R. (2011). *Ślady osmologiczne.* Słupsk.

Biliński L., Miś W. (2009). *Kryminalistyczno-procesowe zabezpieczanie śladów na miejscu zdarzenia*. Piła.

Bogusz I., Bogusz M. *Ślady kryminalistyczne dla słuchaczy szkolenia zawodowego podstawowego.* Legionowo.

[35] G. Woźny. *Modus operandi sprawców przestępstw komputerowych,* https://wspia.eu/media/x2gndgut/32-wo%C5%BAny.pdf [dostęp: 03.11.2024].

[36] A. McFarlanda (2024, 23 października 2024). *10 najlepszych narzędzi AI do zamiany twarzy*. Unite AI, https://www.unite.ai/pl/best-ai-face-swap-tools/ [dostęp: 05.11.2024].

[37] D. Martin (2024, 1 października 2024). *10 najlepszych narzędzi do zmiany głosu AI*. Unite AI, https://www.unite.ai/pl/voice-changer-tools/ [dostęp: 06.11.2024].

Bujak A., Kłosowski J. (2014). *System logistyczny przedsiębiorstwa i jego parametry.* „Logistyka" nr 3/2014.

Czop A. (2014). *Udział firm ochrony osób i mienia w zapewnianiu bezpieczeństwa publicznego w Polsce.* Katowice.

Czop A. (2021). *Rola Specjalistycznych Uzbrojonych Formacji Ochronnych w przeciwdziałaniu zagrożeniom terrorystycznym w Polsce.* Kraków.

Daszkiewicz K. (1961). *Motyw przestępstwa*. „Palestra" 5/9(45).

Ficoń K. (2021). *Łańcuch bezpieczeństwa. Zagrożenia, ryzyko, kryzysy.* Warszawa.

Gąsiorowski J. (2016). *Nowoczesne technologie w Kryminalistyce.* „Kultura Bezpieczeństwa Nauka – Praktyka – Refleksje" Nr 21.

Goc M., Moszczyński J. (2017). *Ślady kryminalistyczne Ujawnianie, zabezpieczanie, wykorzystanie*. Warszawa.

Gołębiowski J. (2021). *Umysł przestępcy. Tajniki kryminalnego profilowania psychologicznego.* Kraków.

Kasprzak W.A. (2015). *Ślady cyfrowe. Studium prawno-kryminalistyczne*. Warszawa.

Kozdrój-Miler K., Jędraszek J., Klemczak K. (2022). *Ujawnianie śladów traseologicznych*. „Problemy Kryminalistyki" 315(1).

Kruszyński P. (2004). *Wykład Prawa Karnego Procesowego*. Białystok.

Miturska E. (2015). *Mechanizmy psychologiczne motywacji człowieka. Przegląd koncepcji teoretycznych*. „Świat Problemów", nr 4(267).

Pajorski P. (2015). *Systemy zabezpieczenia technicznego w służbie ochrony osób.* „Security, Economy & Law" Nr 4 (IX).

Sadowski A. (2006). *System logistyczny w przedsiębiorstwie – ujęcie teoretyczne*. „Przegląd Organizacji" Nr 3 (794).

Saramak B. (2015). *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*. Warszawa.

Widacki J. (2002). *Kryminalistyka.* Warszawa, wyd. 2.

Źródła internetowe

Gaweł H. *Analiza śladów cyfrowych z perspektywy informatologii i cyberbezpieczeństwa*. https://ruj.uj.edu.pl/server/api/core/bitstreams/f7024af4-fbce-446e-bb95--e459e668182a/content [dostęp: 28.09.2024].

Martin D. (2024, 1 października 2024). *10 najlepszych narzędzi do zmiany głosu AI*. Unite AI. https://www.unite.ai/pl/voice-changer-tools/ [dostęp: 06.11.2024].

McFarlanda A. (2024, 23 października 2024). *10 najlepszych narzędzi AI do zamiany twarzy*. Unite AI. https://www.unite.ai/pl/best-ai-face-swap-tools/ [dostęp: 05.11.2024].

Panecki S. (2013). *Interfejs komunikacyjny CAN: podstawy.* https://mikrokontroler.pl/2013/06/10/interfejs-komunikacyjny-can-podstawy/ [dostęp: 11.09.2024].

Sąsiada M. *Modus operandi jako środek identyfikacji sprawcy przestępstwa*. https://repozytorium.uni.wroc.pl/en/dlibra/publication/22385/edition/29211/modus-operandi-jako-srodek-identyfikacji-sprawcy-przestepstwa-sasiada-monika [dostęp: 20.09.2024].

Szustakowski M., Ciurapiński W. *Techniczne systemy zabezpieczenia mienia i infrastruktury krytycznej*. https://certus.edu.pl/rzeszow/wp-content/uploads/2020/11/30_techniczne_systemy_zabezpieczenia_mienia_i_infrastruktury_krytycznej-1.pdf [dostęp: 30.10.2024].

Woźny G. *Modus operandi sprawców przestępstw komputerowych*. https://wspia.eu/media/x2gndgut/32-wo%C5%BAny.pdf [dostęp: 03.11.2024].

Źródła normatywne

Ustawa z dnia 6 czerwca 1997 r. Kodeks Postępowania Karnego, Dz. U. 1997 Nr 89 poz. 555.

Wytyczne nr 3 Komendanta Głównego Policji z dnia 30 sierpnia 2017 r. w sprawie wykonywania niektórych czynności dochodzeniowo-śledczych przez policjantów, Dz. Urz. KGP. 2017. 59.