FOLIA 414

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 14(2) (2024)

ISSN 2657-8549

DOI 10.24917/26578549.14.2.6

Małgorzata Bereźnicka

Uniwersytet Komisji Edukacji Narodowej w Krakowie

ORCID 0000-0002-1525-9184

Justyna Rokitowska

Uniwersytet Komisji Edukacji Narodowej w Krakowie

ORCID 0000-0002-3046-8929

Internetowa kontrola rodzicielska czasu i treści a zaangażowanie młodzieży w seksting oraz potrzeba edukacji w tym zakresie

Internet Parental Control of Time and Content, Youth Involvement in Sexting, and the Need for Education on These Issues

Abstrakt

Internet jako ogromne narzędzie o zasięgu ogólnoświatowym może stanowić źródło informacji, wiedzy, rozrywki, jednakże korzystanie z niego w nadmiarze oraz wykorzystywanie nieodpowiednich treści może być również źródłem wielu niebezpieczeństw, grożących młodym użytkownikom w codziennym życiu. W związku z dynamicznymi zmianami, jakie następują wraz z rozwojem technologicznym, pojawiają się również coraz to nowsze kategorie zagrożeń dla bezpieczeństwa we współczesnym świecie. Wraz z szybkim i gwałtownym upowszechnieniem się mediów społecznościowych, dających nowe możliwości dla użytkowników, w coraz większym stopniu rozwijają się kolejne niebezpieczne zjawiska, jak np. seksting, oraz ryzykowne sytuacje z tym związane dla dzieci, młodzieży i dorosłych.

W artykule zaprezentowano wyniki badań, które przeprowadzono wśród 318 maturzystów z województwa małopolskiego, z trzech liceów ogólnokształcących i dwóch techników. Młodzież wypełniała anonimowe ankiety w warunkach lekcyjnych, a badanie składało się z trzech części związanych z wiedzą, doświadczeniami i opiniami na temat zjawiska sekstingu. W tekście zestawiono ze sobą kontrolę rodzicielską czasu online i treści internetowych z aktywnym uczestnictwem młodzieży w sekstingu. Celem było sprawdzenie, czy te zmienne mogły różnicować doświadczenia badanych związane z sekstingiem, a także edukację dotyczącą zagrożeń wynikających z tego zjawiska.

Słowa kluczowe: Internet, seksting, młodzież, kontrola rodzicielska, edukacja, edukacja dla bezpieczeństwa

Abstract

The Internet, as a huge global tool, can be a source of information, knowledge, and entertainment, but excessive use and exposure to inappropriate content can also pose significant dangers for young users in their daily lives. Due to the dynamic changes that come with technological development, new categories of security threats continue to emerge in the modern world. With the rapid and exponential growth of social media, which offers new opportunities for users, dangerous phenomena such as sexting, along with the associated risks for children, adolescents, and adults, are becoming increasingly prevalent. The article presents the results of research that was conducted among 318 secondary school graduates from the Małopolska Voivodeship, representing three general secondary schools and two technical secondary schools. The young people completed anonymous questionnaires in classroom settings. The study consisted of three parts related to their knowledge, experiences, and opinions on the phenomenon of sexting. The text juxtaposes parental control over online time and content with young people's active participation in sexting. The aim was to explore if these variables could differentiate respondents' experiences of sexting, as well as their education about the dangers associated with it.

Key words: Internet, sexting, youth, parental control, education, safety education

Internet jest narzędziem, które oferuje wiele możliwości ułatwiających edukację i rozwój[1], jednak w nadmiarze korzystanie z niego może być ryzykowne, m.in. ze względu na potencjalnie szkodliwe treści i wiele niebezpieczeństw, grożących przede wszystkim młodym i niedoświadczonym (życiowo) użytkownikom. Dlatego powstaje coraz więcej aplikacji, dzięki którym można ograniczyć dostęp do stron internetowych z niepożądanymi treściami. Prowadzi się również wiele akcji uświadamiających społeczeństwo, w tym dzieci i rodziców, o zagrożeniach w sieci.

Internet a kontrola rodzicielska

W naszym kraju obserwuje się w ostatnich latach stały wzrost liczby godzin spędzonych przez młodych użytkowników na korzystaniu z internetu. Obecnie u nastolatków jest to średnio blisko 5 godzin dziennie, a w dni wolne od zajęć ponad 6 godzin, przy czym 1/10 przeznacza na aktywność w sieci powyżej 8 godzin dziennie, w tym spora część w godzinach nocnych. Aż co trzeci nastolatek wykazuje się wysokim natężeniem wskaźników problematycznego użytkowania internetu (PUI)[2]. Dane te pochodzą z kolejnej edycji badania „Nastolatki 3.0", przeprowadzonego w 2020 roku, w którym wzięło udział 1773 uczniów z klas VII szkoły podstawowej i z klas II szkoły ponadpodstawowej z 61 placówek we wszystkich województwach oraz 893 rodziców i opiekunów prawnych[3].

Eksperci przestrzegają zwłaszcza przed nadmiernym korzystaniem z portali internetowych, które mogą sprzyjać dysfunkcjom i problemom psychospołecznym, takim jak lęki i depresje, wycofanie, objawy somatyczne, zaburzenia myśli i uwagi,

[1] J. Gajda (2009). *Poznawanie dziecka w aspekcie współczesnej pedagogiki kultury*. W: J. Izdebska, J. Szymanowska (red.). *Dziecko w zmieniającej się przestrzeni życia. Obrazy dzieciństwa*. Białystok, s. 22–23.

[2] R. Lange, NASK (red.). (2011). *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów*. NASK – Państwowy Instytut Badawczy. Warszawa, s. 6.

[3] *Ibidem*.

zachowania niedostosowane czy agresywne[4]. Wydaje się, że brak ograniczeń czasowych w dostępie dzieci i młodzieży do sieci jest znaczącym problemem, ale sprawę dodatkowo komplikuje fakt tego, co w niej robią. A zatem oprócz czasu online, należy przyjrzeć się także kwestii nie zawsze pozytywnych, z punktu widzenia wychowania i rozwoju, materiałów.

W badaniach Agencji Gemius, przeprowadzonych wspólnie z Fundacją Dzieci Niczyje (obecnie Fundacja Dajemy Dzieciom Siłę), wśród młodzieży w wieku 12–17 lat blisko 3/4 przyznało, iż w ostatnim roku trafiło na materiały o charakterze erotycznym lub pornograficznym. Ponad połowa natrafiła na brutalne sceny przemocy, a blisko 1/3 zetknęła się z materiałami nawołującymi do przemocy lub nietolerancji wobec ludzi innej rasy, narodowości lub wyznania[5].

Oprócz zagrożeń związanych z niepożądanymi treściami, sieć zwiększa także ryzyko niebezpiecznych kontaktów, np. z oszustami, pedofilami czy przestępcami. Dzieci często nie zdają sobie sprawy z tego, że „po drugiej stronie" może być ktoś zupełnie inny niż osoba, za którą się podaje (np. dorosły, a nie rówieśnik). Z kolei młodzież wydaje się bardziej świadoma w tym zakresie, a mimo to wykazuje skłonność do podejmowania ryzyka. Według raportu z 2014 roku „Nastolatki wobec Internetu", blisko co trzecia badana osoba udająca się na spotkanie ze znajomym poznanym w mediach społecznościowych, nie powiadomiła o tym fakcie nikogo ze swojego otoczenia (pozostali najczęściej informują kolegów/koleżanki), równocześnie prawie 4/5 ankietowanych zdaje sobie sprawę, że takie spotkania mogą być niebezpieczne[6].

Do ryzykownych treści i kontaktów należy dodać jeszcze ryzykowne zachowania. Można tu wymienić m.in. stalking (nękanie), zastraszanie, dręczenie, dostarczanie destrukcyjnych porad czy niepożądanych materiałów, hazard, hakerstwo, ale chyba najpowszechniejsze są różne formy cyberprzemocy. Kluczowe znaczenie ma fakt, że im więcej czasu dzieci spędzają online, tym bardziej prawdopodobne, że będą cyberofiarami[7] lub sprawcami przemocy w sieci[8].

Według badań „Nastolatki 3.0" co piąty nastolatek miał doświadczenia związane z przemocą internetową (najczęściej wyzywaniem, ośmieszaniem, poniżaniem).

---

[4] K. Makaruk (2013). *Korzystanie z portali społecznościowych przez młodzież. Wyniki badania EU NET ADB*. W: Fundacja Dzieci Niczyje. *Dziecko krzywdzone. Teoria, badania, praktyka*, t. 12, nr 1, 76–77.

[5] Ł. Wojtasik. *Kontakt dzieci z niebezpiecznymi treściami w Internecie*. Raport z badań Gemius/Fundacja Dajemy Dzieciom Siłę. https://bibe.ibe.edu.pl/475-kontakt-dzieci-z-niebezpiecznymi-tresciami-w-internecie.html [dostęp: 17.09.2024].

[6] R. Lange, J. Osiecki (2014). *Nastolatki wobec Internetu*. NASK, Rzecznik Praw Dziecka oraz Wyższa Szkoła Nauk Społecznych PEDAGOGIUM. Warszawa. https://www.nask.pl/pl/raporty/raporty/3473,Raport-z-badan-quotNastolatki-wobec-internetuquot-2014.html [dostęp: 10.09.2024].

[7] P.K. Smith, J. Mahdavi, M. Carvalho, S. Fisher, S. Russell, N. Tippett (2008). *Cyberbullying, its forms and impact in secondary school pupils*. "Journal of Child Psychology and Psychiatry", 49, 376–385.

[8] F. Mishna, M. Khoury-Kassabri, T. Gadalla, J. Daciuka, (2012). *Risk factors for involvement in cyber bullying: Victims, bullies and bully–victims*. "Children and Youth Services Review", 34, 63–70.

Rodzice najczęściej nie są tego świadomi i tylko 1/10 z nich potwierdza, że wiedzą o takich doświadczeniach swoich dzieci[9].

Z raportu wynika, że co trzeci badany nie tylko nie zgłasza nigdzie cyberprzemocy, ale nawet nie podejmuje rozmowy na ten temat z bliskimi czy innymi osobami mogącymi pomóc. Większość rodziców (69%) uważa, że wiodącym sposobem radzenia sobie z takimi problemami w sieci jest szukanie wsparcia u rodziców/opiekunów, podczas gdy w rzeczywistości takie postępowanie dotyczy jedynie co czwartego nastolatka (nieco częściej po pomoc zgłaszają się do przyjaciół i znajomych lub administratorów serwisu)[10].

Ponad 1/4 (27%) rodziców deklaruje, że w domu stosują technologie zabezpieczające przed niebezpiecznymi treściami w internecie. Tych deklaracji nie potwierdzają ich nastoletnie dzieci, wśród których mniej niż 1/10 (9%) uważa, że rodzice stosują w ich domach systemy kontroli. Jednakże już negatywne odpowiedzi w obu grupach (brak zainstalowanego filtru rodzinnego ani innej technologii ograniczającej dostęp do ryzykownych treści w sieci) mają zbliżone proporcje (kolejno 67% i 69%). Zatem można założyć, iż być może dzieci nie zawsze są świadome działań podejmowanych przez rodziców[11].

Zapytani o zasady korzystania z internetu, nastolatki deklarowały najczęściej, że w ich domach nie wprowadza się zasad ograniczających czas online czy reguł dotyczących selekcji treści (40%). Jedynie 17% przyznało, że rodzice rozmawiają z nimi zawsze, gdy zgłoszą problem, oraz kiedy podejrzewają, że ich dziecko tego potrzebuje (8%). Młodzież przyznała również, że jeszcze rzadziej mają ustalony czas online (7%), przekazuje im się materiały na temat zagrożeń w sieci (5%), a nieliczni badani wymieniali sprawdzanie faktycznej aktywności w internecie (3%), ustalanie zasad dostępu do internetowych zasobów oraz wgląd rodziców w ich konta (po 2%), a także korzystanie ze sprzętów umożliwiających im surfowanie w sieci jedynie w określonych godzinach (niespełna 2%) albo tylko w obecności opiekunów (niecały 1%)[12].

Z kolei tylko 31% rodziców przyznało, że nie stosuje w domu żadnych regulacji w omawianym zakresie. Ponad połowa odpowiedziała, że prowadzą z dziećmi profilaktyczne rozmowy, aby zapobiegać zagrożeniom (59%), rozmawiają też z nimi zawsze, gdy te zgłaszają im problem (57%) lub gdy podejrzewają, iż jest taka potrzeba (rzadziej – 42%), a ponadto ustalają maksymalny czas online (34%), sprawdzają, co dzieci robią w internecie (33%), dzielą się materiałami dotyczącymi zagrożeń w sieci (16%), ustalają zasady dotyczące dostępu do konkretnych treści (15%), mają wgląd w konta dzieci (12%), udostępniają im sprzęty do korzystania z internetu tylko w określonych godzinach (3%) lub tylko w swojej obecności (0,2%)[13].

Rozbieżności w odpowiedziach dzieci i rodziców na temat stosowania zasad dotyczących czasu spędzonego przez nie w sieci oraz selekcji treści, do jakich mają dostęp,

[9] R. Lange, NASK (red.). (2011). *Nastolatki 3.0. Raport z… Op. cit.*, s. 90.

[10] *Ibidem*.

[11] *Ibidem*, s. 103.

[12] *Ibidem*, s. 105.

[13] *Ibidem*, s. 104.

musi niepokoić. Pozostaje pytanie, czy to działania opiekunów nie są wystarczająco wyraźne, czy też nastolatki – co nie byłoby też niczym nietypowym – czasami wybiórczo słuchają tego, co dorośli mają im do powiedzenia? Ale nawet wtedy odpowiedzi rodziców wydają się mało satysfakcjonujące i z pewnością jest to obszar badawczy wymagający większej troski i uwagi.

Seksting – zachowanie ryzykowne w sieci

Jak wspomniano wcześniej, użytkowanie internetu daje wiele korzyści, lecz równocześnie może być źródłem różnorakich zagrożeń. Część z nich pojawiła się w zasadzie od momentu, kiedy rozpowszechniono to medium (np. oszustwa), inne miały związek z rozwojem form komunikacji online (np. nękanie na portalach społecznościowych). Jedno z nowszych zjawisk, związanych m.in. z użytkowaniem nowych mediów i wiążące się z największym ryzykiem, gdy ma miejsce w internecie, stanowi seksting.

Termin ten powstał z połączenia słów *sex* oraz *texting* (z ang. seks i SMS-owanie) i oznacza przesyłanie między użytkownikami sieci wiadomości tekstowych i innych rodzajów materiałów o charakterze seksualnym[14]. W szerszym znaczeniu odnosi się do tworzenia, wysyłania, odbierania, udostępniania, przekazywania wiadomości, zdjęć lub filmików o seksualnym zabarwieniu, głównie za pośrednictwem telefonu komórkowego, jak również poczty e-mail, czatów i portali społecznościowych. W dobie coraz bardziej jaskrawego dzielenia się swoją prywatnością, a nawet intymnością w sieci, zwłaszcza wśród ludzi młodych (ale także np. celebrytów, stanowiących dla nich nierzadko wzór), część młodych ludzi omawianą aktywność traktuje jako kolejną formę komunikacji, poprzez którą mogą wyrazić lub potwierdzić swoje zainteresowanie odbiorcami takich wiadomości, a zatem w tym rozumieniu seksting bywa częścią flirtu[15].

Skala tego zjawiska wśród młodzieży jest niełatwa do oszacowania. Według różnych badań liczby wahają się od 15% do 40% w zależności od metodologii, definicji i innych składowych[16]. Podobnie jak inne zagrożenia internetowe, dotykające przede wszystkim dzieci i młodzież, seksting w ostatnich latach stał się przedmiotem zainteresowania i obaw specjalistów, co zaowocowało powstawaniem i publikowaniem coraz większej liczby opracowań na ten temat na całym świecie[17].

---

[14] J.R. Temple, A.P. Jonathan, P. Van Den Berg, V.D. Le, A. McElhany, B.W. Temple (2012). *Teen Sexting and Its Association With Sexual Behaviors.* "Archives of Pediatrics and Adolescent Medicine", 166(9), 828–833.

[15] S.E. Baumgartner, P.M. Valkenburg, J. Peter (2010). *Assessing causality in the relationship between adolescents' risky sexual online behavior and their perceptions of this behavior.* "Journal of Youth & Adolescence", 39, 1226–1239.

[16] J. Ringrose, R. Gill, S. Livingstone, L. Harvey. *A Qualitative study of children, young people and 'sexting'. A report prepared for the NSPCC*, s. 12. https://eprints.lse.ac.uk/44216/1/__Libfile_repository_Content_Livingstone%2C%20S_A%20qualitative%20study%20of%20children%2C%20young%20people%20and%20%27sexting%27%20%28LSE%20RO%29.pdf [dostęp: 15.09.2024].

[17] A. Phippen (2011). *Sharing Personal Images and Videos Among Young People*. University of Plymouth. https://childnetsic.s3.amazonaws.com/downloads/Research_Highlights/

Na świecie prowadzono badania na ten temat m.in. w Stanach Zjednoczonych[18], Australii[19] czy RPA[20], a w Europie badania podjęto np. w ramach EU Kids Online – międzynarodowej sieci badawczej mającej na celu zwiększenie wiedzy na temat możliwości, ryzyka i bezpieczeństwa dzieci w internecie[21]. Edycja z 2018 roku objęła swym zasięgiem piętnaście krajów Unii Europejskiej, w których uczestniczyły osoby w wieku 9–17 lat. W Polsce objęły one 1 433 uczniów z 90 szkół oraz po jednym z ich rodziców (jednak z zagadnień dotyczących sekstingu wyłączono dwa najmłodsze roczniki uczniów). Wykazano, że wraz z wiekiem wzrasta prawdopodobieństwo narażenia na odbiór materiałów o charakterze seksualnym w różnych formach przekazów medialnych, jednak najczęściej dzieje się tak poprzez smartfon (24% – minimum raz w tygodniu lub częściej), reklamy w sieci (16%) oraz telewizję (14%). Skala sekstingu inicjowanego przez młodzież okazała się niewielka, bo wysyłanie lub umieszczanie w sieci takich materiałów dotyczyło niespełna 4% badanych. W większości odbywało się to sporadycznie, ale wraz z wiekiem częstotliwość rosła: od 0,9% w najmłodszej grupie 11–12 lat do 5,3% wśród najstarszych – w wieku 15–17 lat[22].

Nieco inaczej wyglądały wyniki badań polskiej Fundacji Dajemy Dzieciom Siłę z 2014 roku, w których spośród pół tysiąca młodzieży w wieku 15–19 lat ponad połowa (55%) zaprzeczyła, jakoby ktokolwiek z ich przyjaciół miał wysyłać takie materiały, jednak pozostali przyznali, że w ich otoczeniu to się zdarza. Treści takie przynajmniej raz w życiu otrzymało 34%. Nadawcami były głównie osoby znajome, odbiorcami głównie respondenci płci męskiej, aczkolwiek omawiane materiały wysyłały również zupełnie obce osoby. Najpowszechniejszym motywem była chęć „poderwania" lub przyciągnięcia uwagi. Wysłanie zdjęcia/filmu z podtekstem erotycznym dotyczyło 1/9 nastolatków, najczęściej dziewcząt, które przesyłały je głównie w ramach flirtu do osób będących z nimi w związku. Z kolei dane badań fundacji przeprowadzonych trzy lata później pośród dwóch tysięcy nastolatków w wieku 15–18 lat wykazały, że ponad 2/5 ankietowanych dostało od innej osoby jej nagie zdjęcie/film, a niespełna 1/8 wysłała swoje nagie zdjęcie/film. Najczęściej działo się to w związku i miało na celu sprawienie przyjemności odbiorcom (65%), było spowodowane ich prośbą (36%),

---

UKCCIS_RH_10_Sexting.pdf [dostęp: 23.09.2024]; C. Badenhorst (2011). *Legal responses to cyber bullying and sexting in South Africa*. "Centre for Justice and Crime Prevention, CJCP Issue Paper" 10. South Africa; K.J. Mitchell, D. Finkelhor, L.M. Jones, J. Wolak (2012). *Prevalence and Characteristics of Youth Sexting: A National Study*. "Crimes against Children Research Center". University of New Hampshire, Durham; K. Albury, K. Crawford, P. Byron, B. Mathews (2013). *Young People and Sexting in Australia: ethics, representation and the law*. "ARC Centre for Creative Industries and Innovation Journalism and Media Research Centre". The University of New South Wales, Australia.

[18] K. J. Mitchell, D. Finkelhor, L.M. Jones, J. Wolak (2012). *Prevalence and Characteristics… Op. cit.*

[19] K. Albury, K. Crawford, P. Byron, B. Mathews (2013). *Young People and Sexting in Australia… Op. cit.*

[20] C. Badenhorst (2011). *Legal responses to cyber bullying… Op. cit.*

[21] EU Kids Online. www.eukidsonline.net [dostęp: 10.08.2024].

[22] J. Pyżalski, A. Zdrodowska, Ł. Tomczyk, K. Abramczuk (2019). *Polskie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski*. Wydawnictwo Naukowe UAM, Poznań.

chęcią podjęcia flirtu lub żartem (29%), a także chęcią dokuczenia (12%). Interesujące były wyniki wskazujące na zależność sekstingu z pornografią, okazało się bowiem, że osoby mające z nią kontakt, były częściej skłonne do angażowania się w seksting; trzy razy częściej jako odbiorcy i pięć razy częściej jako nadawcy[23].

W wynikach scharakteryzowanych w dalszej części badań własnych, przeprowadzonych pośród 318 maturzystów, skala sekstingu obejmowała różne przedziały liczbowe, w zależności od formy czy wieku respondentów. Przykładowo, według badanych przesyłanie zdjęć o charakterze seksualnym w ich szkołach podstawowych prawie nie miało miejsca, a na dalszych etapach edukacyjnych występowało u mniej niż połowy. Sami uczniowie częściej doświadczali sekstingu jako odbiorcy niż nadawcy, w obu grupach z przewagą chłopców. Ponad 2/5 badanych otrzymało erotyczne zdjęcie od osoby będącej z nimi w związku, w tym ponad 1/3 kilka razy lub wielokrotnie. Rzadziej otrzymywali takie zdjęcia od koleżanek czy kolegów (od niespełna 1/3 do 1/5), a tylko pojedyncze osoby od nieznajomych. Nadawcami materiałów erotycznych najczęściej byli w stosunku do osoby będącej z nimi w związku – zadeklarował to co trzeci respondent (z czego 1/4 robiła to kilka razy lub wielokrotnie), a blisko 1/5 przesyłała takie materiały do koleżanki i 1/10 do kolegi. Zdaniem ankietowanych powodem zarówno otrzymania takich materiałów, jak i ich wysyłania, była głównie chęć flirtu, przyciągnięcia uwagi lub żart[24].

Problematyka zagrożeń związanych z sekstingiem to temat ważny i aktualny, dlatego warto prowadzić na ten temat badania. Potrzebne są też oparte na nich projekty, aby przeciwdziałać zjawisku, które może mieć bardzo poważne, a niekiedy wręcz dramatyczne konsekwencje, nierzadko rzutujące na całe życie zaangażowanej w tę aktywność młodej osoby.

Kontrola rodzicielska a seksting – badania własne

Wspomniane badania autorskie przeprowadzono wśród 318 małopolskich maturzystów z trzech liceów ogólnokształcących i dwóch techników, którzy wypełnili anonimowe kwestionariusze ankiety w warunkach lekcyjnych. Składało się z trzech części związanych z wiedzą, doświadczeniami i opiniami młodzieży na temat zjawiska sekstingu[25]. W niniejszym artykule skupiono się na kwestiach niezbadanych wcześniej, zestawiając ze sobą kontrolę rodzicielską czasu online i treści internetowych z aktywnym uczestnictwem ankietowanych w seksting. Główny cel stanowiło sprawdzenie, czy te zmienne mogły różnicować doświadczenia respondentów związane z sekstingiem, a także edukację dotyczącą wypływających z niego zagrożeń.

Analizowana grupa badawcza składała się ze 109 chłopców (34%) i 209 dziewcząt (66%). Maturzyści zamieszkiwali zarówno wsie – 176 osób (55%), jak

[23] K. Makaruk, J. Włodarczyk, P. Michalski (2017). *Kontakt dzieci i młodzieży z pornografią. Raport z badań.* Fundacja Dajemy Dzieciom Siłę. https://www.saferinternet.pl/pliki/Raport-kontakt_dzieci_i_mlodziezy_z_pornografia.pdf [dostęp: 26.09.2024].

[24] M. Bereźnicka, J. Rokitowska (2021). *Seksting – wiedza, doświadczenia i opinie młodzieży.* Wydawnictwo Libron.

[25] *Ibidem*.

i miasta – 142 osoby (45%, w tym 8% z dużych aglomeracji, powyżej 50 tys. mieszkańców). Większość badanych posiadała pełną rodzinę (236 osoby; 74%), u pozostałych małżeństwo rodziców się rozpadło (54 osoby; 17%), jeden rodzic nie żyje (20 osób; 6%), dwie osoby wskazały, że są sierotami, jedna – że utrzymuje kontakt z rodzicem mieszkającym poza granicami kraju, również jeden ankietowany wybrał odpowiedź „inne" bez doprecyzowania, a czterech uczniów w ogóle nie udzieliło odpowiedzi na to pytanie.

Aby naświetlić tło dla dalszych analiz, należy przedstawić dane dotyczące tego, jak dużo czasu respondenci poświęcają na surfowanie w sieci. Oddzielono tu sytuacje, w których badani są online w związku ze swoimi zainteresowaniami oraz bez związku z nimi, zakładając ostrożnie, że w tym pierwszym przypadku ten czas z reguły ma większą wartość z punktu widzenia samorozwoju, zaś w drugim tak być nie musi. Ponadto, realizowanie pasji przez młodzież należy do czynników chroniących przed zachowaniami ryzykownymi[26], podczas gdy dużą liczbę godzin spędzanych przed komputerem dla przyjemności uwzględnia się jako jeden z czynników ryzyka[27]. Dla pełnego obrazu dodajmy, że aż co piąty respondent nie posiadał żadnych zainteresowań (21%), wśród wskazań reszty dominował sport (40%), słuchanie muzyki (30%), pasje artystyczne (17%), literatura (13%), filmy i seriale (9%), zainteresowania komputerowe (7%), turystyka (5%) oraz pozostałe odpowiedzi (30%), wśród których wymieniano pojedyncze wybory dotyczące m.in. zainteresowań technicznych (np. mechatronika, mechanika), biologiczno-chemicznych (biologia, chemia, weterynaria), humanistycznych (języki obce, psychologia, kultura innych krajów itp.). Dodatkowo warto wspomnieć, że realizacja zainteresowań poza siecią, w każdym z podanych niżej przedziałów czasowych, wynosiła o kilka procent mniej niż uskutecznianie tego w internecie (co jest niepokojącą tendencją).

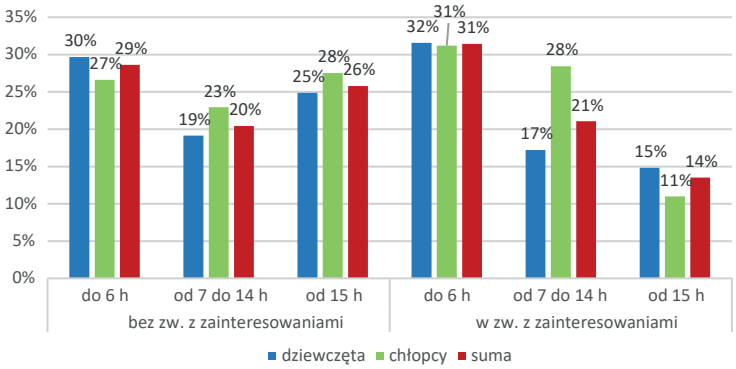
Dane odnoszące się do liczby godzin spędzanych online w związku z tymi zainteresowaniami oraz bez związku z nimi, z uwzględnieniem płci i zbiorowości, przedstawiono na poniższym wykresie (Wykres 1). Ze względu na ograniczenia objętości tekstu pominięto dane liczbowe, koncentrując się na procentowych, a przez wzgląd na czytelność danych, zarówno tu, jak i w kolejnych diagramach, zrezygnowano z zamieszczenia informacji o braku odpowiedzi. W tym przypadku jednak jest to szczegół warty podkreślenia, ponieważ dotyczy aż 25% ogółu.

Blisko 1/3 badanych spędza w sieci do 6 godzin tygodniowo, zarówno w związku ze swoimi zainteresowaniami, jak i bez nich. Więcej – bo od 7 do 14 godzin– to odpowiedź wskazana przez około 1/5 w obu tych grupach. Wyraźna różnica pojawia się dopiero w najwyższym przedziale czasowym – od 15 godzin – co nie zaskakuje, biorąc

[26] J. Mazur i in. (2008). *Czynniki chroniące młodzież 15-letnią przed podejmowaniem zachowań ryzykownych*. Raport z badań HBSC 2006. Instytut Matki i Dziecka. Zakład Ochrony i Promocji Zdrowia Dzieci i Młodzieży, Warszawa, 32 i 37; M. Łoś i in. *Mapa czynników ryzyka i chroniących młodzież przed zachowaniami ryzykownymi. Raport I z badań NPZ.XI_17.2017*. Instytut Profilaktyki Zintegrowanej, s. 61 i 66. https://ore.edu.pl/wp-content/uploads/2018/10/raport-i-mapa-czynnikow-ryzyka-i-chroniacych-mlodziez-przed-zachowaniami-ryzykownymi.pdf [dostęp: 1.10.2024].

[27] *Ibidem*, s. 36 i 71–72.

Wykres 1. Liczba godzin spędzana w Internecie tygodniowo

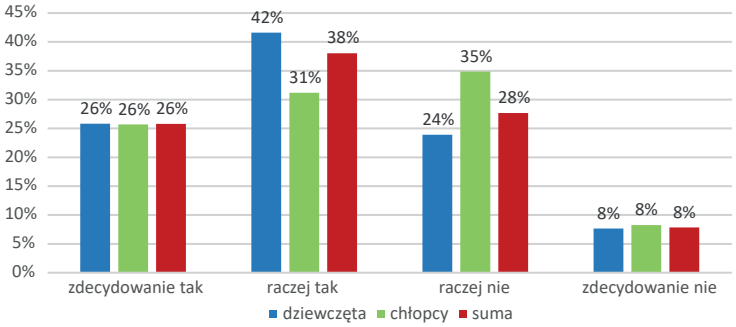


Źródło: opracowanie własne.

pod uwagę dużą grupę badanych nieposiadających żadnych pasji; w grupie, która swój czas online łączy z zainteresowaniami było to 14%, podczas gdy u reszty – prawie 1/3. Proporcje wskazań uwzględniających płeć były bardzo zbliżone w grupie spędzającej czas bez związku z zainteresowaniami, natomiast u ankietowanych łączących te dwie sfery, w średnim przedziale czasowym było znacznie więcej odpowiedzi od respondentów płci męskiej niż żeńskiej (kolejno 28% i 17%), a w najwyższym przedziale widać niewielką przewagę dziewcząt nad chłopcami (odpowiednio 15% i 11%).

Zmierzając do przedstawienia danych dotyczących kontroli rodzicielskiej czasu spędzanego przez badanych online, zasadnym wydaje się przybliżenie opinii ich samych dotyczącej tego, czy spędzają zbyt dużo czasu w sieci. Dane te ilustruje wykres 2.

Wykres 2. Opinia badanych dotycząca zbyt długiego przebywania online



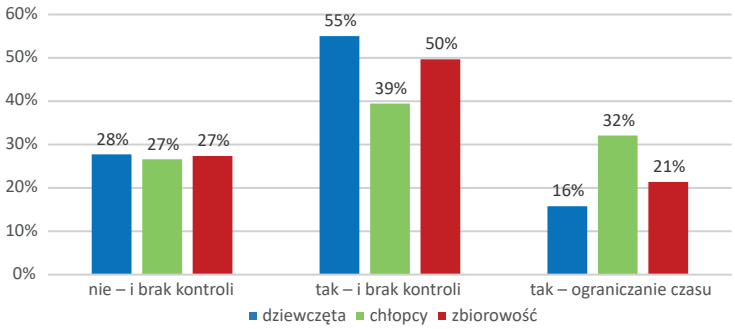
Źródło: opracowanie własne.

Mimo iż są to tylko deklaracje i można zakładać, że młodzi ludzie często bagatelizują aspekty dotyczące marnotrawienia czasu czy nie zawsze wartościowego spędzania

go, to jednak ponad 1/4 zdecydowanie potwierdziła, że zbyt długo przebywa online, a blisko 2/5 – że raczej tak jest. Tylko nieco więcej niż 1/4 respondentów uznała, że w ich przypadku ten czas raczej nie jest zbyt długi, a mniej niż 1/10 – że zdecydowanie tak nie jest. Różnice uwzględniające płeć widać jedynie w odpowiedziach „raczej tak" (przewaga dziewcząt) oraz „raczej nie" (przewaga chłopców).

Interesujące jest zestawienie wcześniejszych wyników z danymi dotyczącymi oceny tego aspektu werbalizowanej przez rodziców ankietowanych. Ich przekonania co do tej kwestii wraz z odpowiedziami odnoszącymi się do rodzicielskiej kontroli czasu online ich dzieci, kiedykolwiek, począwszy od szkoły podstawowej, zostały przedstawione poniżej (poza brakiem odpowiedzi, dotyczącym 5% ogółu).

Wykres 3. Ocena rodziców dotycząca zbyt długiego przebywania badanych online i kontrolowanie tego czasu



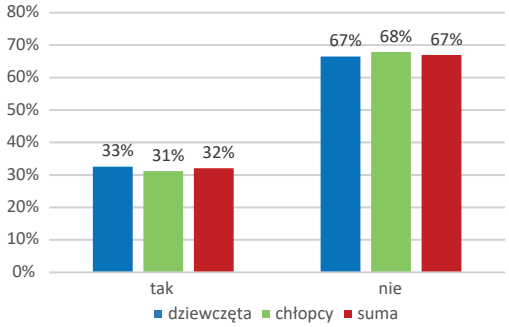
Źródło: opracowanie własne.

Okazuje się, że znacznie więcej rodziców niż ich dzieci uważało, że te ostatnie spędzają zbyt dużo czasu w sieci. Takie przekonanie wyraziło aż 71% badanych. Jedynie nieco ponad 1/4 odpowiedziała tu przecząco. Mimo tego, tylko w co piątym przypadku miały miejsce próby ograniczania przez rodziców czasu spędzanego w internecie przez ich dzieci (co ciekawe – znacznie częściej u chłopców), zaś nie wystąpiło to u blisko 4/5 badanych. Przy czym aż u połowy respondentów pojawił się rozdźwięk między poczuciem, że rodzice uważali, iż przebywają oni zbyt dużo online, a przekonaniem, że mimo to nie podejmowali żadnych działań, by to zmienić.

Zbyt długi czas spędzany online przez dzieci i młodzież to jeden problem. Innym są treści, często szkodliwe bądź niewłaściwe dla młodych użytkowników. Ankietowanych zapytano o to, czy kiedykolwiek, począwszy od szkoły podstawowej, rodzice kontrolowali zawartość odwiedzanych przez nich stron i miejsc w sieci. Wyniki zilustrowano na poniższym wykresie.

Dane prezentują się nieco lepiej niż w przypadku czasu. Treści internetowe, według deklaracji badanych, były kontrolowane w domach co trzeciego z nich (32%), czyli o 11% więcej niż we wcześniejszych wynikach. Natomiast ponownie nie zanotowano wyraźnej różnicy między przedstawicielami obu płci. Jako dodatkową informację

Wykres 4. Kontrola rodzicielska treści internetowych



Źródło: opracowanie własne.

doprecyzujemy, że w okresie, gdy uczęszczali oni do szkoły podstawowej, miało to miejsce ponad trzykrotnie częściej, niż kiedy byli w gimnazjum (odpowiednio 29% i 9%), zaś w szkole średniej zjawisko to prawie nie miało miejsca (3%).

Ankietowanych zapytano o sytuację, w której mieli być nadawcami w sekstingu. Na pytanie o to, czy i jak często wysyłali własne erotyczne zdjęcia, nie udzieliło odpowiedzi od 8 do 14%. Uzyskane wyniki z uwzględnieniem kontroli rodzicielskiej czasu online oraz treści internetowych przedstawiają dwie kolejne tabele.

Tabela 1. Angażowanie się badanych w seksting a kontrola rodzicielska czasu online

		Nigdy	Raz	Kilka razy	Wielokrotnie	Brak odpowiedzi
Do chłopaka/ dziewczyny	Kontrola	56%	6%	16%	12%	10%
	Brak kontroli	61%	7%	14%	10%	8%
Do koleżanki	Kontrola	67%	9%	5%	4%	14%
	Brak kontroli	71%	8%	5%	5%	11%
Do kolegi	Kontrola	76%	4%	5%	1%	14%
	Brak kontroli	76%	7%	5%	2%	10%

Źródło: opracowanie własne.

Najbardziej pożądaną odpowiedź „nigdy" wybierało od 56% do 76% respondentów w zależności od odbiorcy, wśród których najrzadziej wskazywano osoby będące z ankietowanymi w związku, nieco częściej koleżanki oraz najczęściej koledzy. Również pozostałe wyniki, odnoszące się do częstotliwości czynnego angażowania się w seksting, potwierdzają, że taka aktywność miała miejsce głównie w bliskich relacjach (z dziewczyną/chłopakiem) – jedynie tu pojawiły się liczby dwucyfrowe. Odpowiedź „raz" wybierało 4–7% badanych, kilka razy – 5–16%, a wielokrotnie – 1–12%. Natomiast trudno dopatrzeć się większych zależności między tymi odpowiedziami, a czynnikiem ograniczania czasu spędzanego online przez rodziców – różnice w obu grupach są niewielkie i nie układają się w żaden regularny wzór.

Podobne wnioski można wyciągnąć z analizy kolejnej tabeli, ukazującej zależności między kontrolowaniem przez rodziców badanych treści internetowych, do których mają oni dostęp. Zarówno sam fakt wysyłania swoich zdjęć o charakterze seksualnym do osób, z którymi ankietowani byli w związku, jak i częstotliwość sekstingu, zdarzały się częściej niż w przypadku, kiedy odbiorcami były osoby niepozostające z nimi w relacji romantycznej, tj. koleżanki i koledzy. I ponownie różnice w odpowiedziach respondentów, u których wystąpiła kontrola rodzicielska treści internetowych oraz u pozostałych, były niewielkie, zatem nie można mówić o żadnej istotnej tendencji.

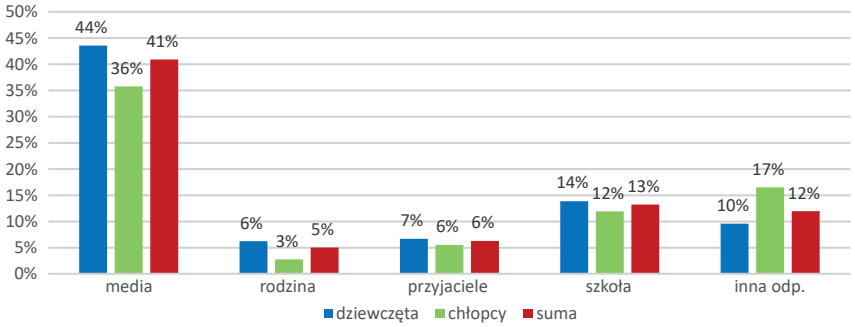
Tabela 2. Angażowanie się badanych w seksting a kontrola rodzicielska treści internetowych

		Nigdy	Raz	Kilka razy	Wielokrotnie	Brak odpowiedzi
Do chłopaka/ dziewczyny	Kontrola	62%	4%	13%	12%	10%
	Brak kontroli	56%	7%	17%	11%	9%
Do koleżanki	Kontrola	70%	10%	5%	3%	13%
	Brak kontroli	69%	8%	5%	5%	14%
Do kolegi	Kontrola	77%	4%	6%	1%	12%
	Brak kontroli	76%	5%	5%	1%	14%

Źródło: opracowanie własne.

O braku istotnego wpływu na aktywność młodzieży dotyczącą sekstingu świadczą niestety również deklarowane przez nich źródła wiedzy o zagrożeniach związanych z tym zjawiskiem, choć należy zaznaczyć, że aż 30% badanych nie udzieliło odpowiedzi na to pytanie. Pozostałe dane ilustruje poniższy wykres.

Wykres 5. Źródła wiedzy badanych o sekstingu



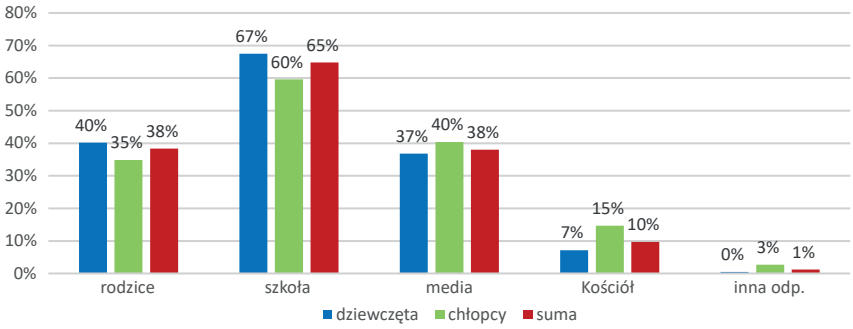
Źródło: opracowanie własne.

Najczęściej jako źródło wiedzy o sekstingu ankietowani wymieniali media (41%, z 8%-ową przewagą dziewcząt), przy czym ponad połowa z nich podała konkretnie

internet. Reszta wskazań miała miejsce znacznie rzadziej i obejmowała szkołę (13%), przyjaciół (6%) i dopiero na czwartym miejscu rodzinę (5%). Wśród innych źródeł (12%, z 7%-ową przewagą chłopców) przeważały odpowiedzi o ich braku oraz pojedyncze ogólnikowe słowa odnoszące się do życia, doświadczenia, świata, środowiska, własnych przemyśleń etc. Można zatem zauważyć, że nie rozczarowuje nie tylko niska liczba wskazań dotyczących rodziców, ale i całokształt powyższych odpowiedzi.

W świetle powyższych danych, kluczowe wydawało się dowiedzenie się, kto zdaniem respondentów, powinien edukować ich na temat sekstingu. Ważną informacją jest to, że jedynie 4% respondentów uznało, iż nie ma potrzeby edukowania o zagrożeniach związanych z tym zjawiskiem. Pozostałe wyniki dotyczące tej kwestii przedstawiono poniżej.

Wykres 6. Preferowane źródła wiedzy badanych o sekstingu



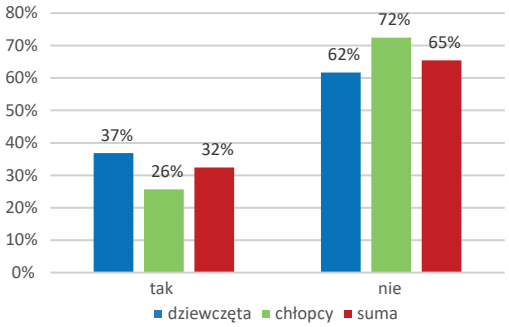
Źródło: opracowanie własne.

Uzyskane wyniki są interesujące i prowokują do przemyśleń, ponieważ można dostrzec duży rozdźwięk między faktycznymi, a preferowanymi źródłami wiedzy młodzieży o sekstingu. Wśród tych ostatnich dominuje szkoła, którą wskazało 65%, sporo wskazań mają również rodzice i media (po 38%), przy czym warto zauważyć, że o ile środki masowego przekazu wskazywano w poprzednim pytaniu dość często, tak rodziców prawie nie wymieniano. Czwarte miejsce pod względem liczby wskazań zajął Kościół (10%), który częściej wskazywali chłopcy (podobnie jak media, natomiast więcej dziewcząt podawało tu szkołę i rodziców). Pozostałe, pojedyncze odpowiedzi zawierały propozycje warsztatów, kampanii czy nieokreślone bliżej edukowanie przez ekspertów.

Nierzadko odpowiedzi młodzieży wydają się nie do końca spójne i tak też było w przypadku zapytania ich o to, czy w ich domu edukowało się o sekstingu. Na to pytanie nie udzieliło odpowiedzi jedynie 2% badanych, pozostałe wyniki przedstawia poniższy wykres.

Mimo minimalnej obecności rodziny we wskazaniach dotyczących źródła wiedzy o sekstingu, w tym pytaniu blisko 1/3 młodzieży (częściej dziewczęta) przyznała, że w ich domu edukowało się na ten temat. Być może tę rozbieżność można tłumaczyć

Wykres 7. Edukowanie o sekstingu w domu

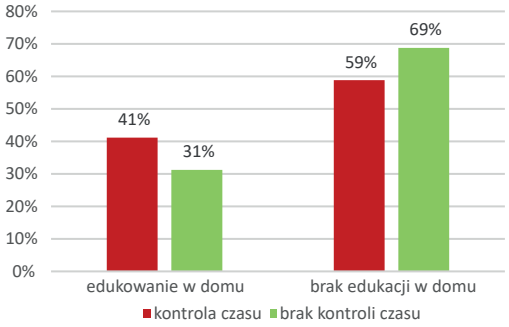


Źródło: opracowanie własne.

niewystarczająco częstymi lub niezbyt efektywnymi działaniami w tym zakresie. Niezależnie od tego, niepokojące jest to, że takich prób nie podejmowano wcale aż u 65% respondentów (z przewagą chłopców).

W dalszej kolejności zamierzano sprawdzić, czy fakt zaistnienia lub braku kontroli rodzicielskiej czasu online oraz treści internetowych w jakiś sposób różnicował kwestię edukowania na temat zagrożeń wynikających z sekstingu. W tym celu podzielono respondentów na dwie grupy. Poniższy wykres ukazuje wyniki odnoszące się do omawianego zagadnienia u respondentów, których rodzice ograniczali ilość spędzanego przez nich czasu w sieci, oraz u których takie sytuacje w ogóle nie miały miejsca.

Wykres 8. Edukowanie o sekstingu w domu a kontrola czasu online

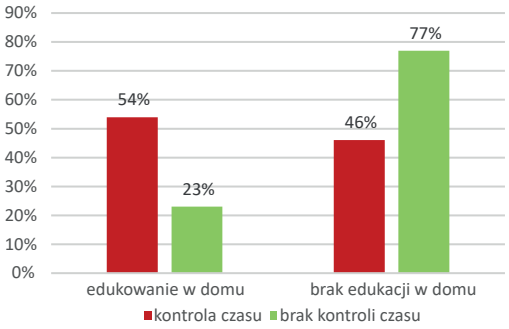


Źródło: opracowanie własne.

Z uzyskanych danych wynika, że nieco częściej edukacja o sekstingu miała miejsce w grupie, w której rodzice przywiązywali również uwagę do tego, by ich dzieci nie przebywały zbyt długo online, aczkolwiek różnice nie są tu bardzo duże, bo 10-procentowe (odpowiednio 41% i 31%). I w obu grupach u ponad połowy wspomniana edukacja nie miała miejsca, jednak przeważały odpowiedzi respondentów, których rodzice nie ograniczali im czasu spędzanego w sieci (69% w stosunku do 59%).

W kolejnych danych, gdzie przekazywanie wiadomości na temat ryzyka związanego z sekstingiem powiązano tym razem z kontrolą treści (poniższy wykres), te różnice są już dużo większe, bo 21-procentowe. U ponad połowy ankietowanych, których rodzice wykazywali troskę dotyczącą treści internetowych dostępnych dla ich dzieci, w domu uświadamiano ich także o zagrożeniach wynikających z omawianej aktywności. Natomiast w grupie, gdzie nie miała miejsca kontrola tych treści, aż 3/4 nie było również edukowane w tym zakresie.

Wykres 9. Edukowanie o sekstingu w domu a kontrola treści internetowych



Źródło: opracowanie własne.

Podsumowanie i wnioski

Reasumując powyższe analizy, można stwierdzić, iż wśród badanych, którzy spędzają w internecie więcej czasu niż pozostali, przeważają osoby niełączące tego z żadnymi zainteresowaniami. Zaś co się tyczy płci, w grupie poszukującej w sieci treści związanych z ich hobby, dominują chłopcy, natomiast u reszty nie dostrzeżono istotnych różnic. Przeważająca część respondentów skłonna jest uznać, iż spędza zbyt dużo czasu online, znacznie mniejsza grupa raczej tak nie uważa, a jedynie nieliczni są tego pewni.

Większość rodziców ankietowanych (według deklaracji blisko 4/5), uważała, że ich dzieci spędzają zbyt dużo czasu online, a jednak poza niewielką grupą (1/5) nie próbowali w żaden sposób im tego czasu ograniczać. Wyniki dotyczące kontroli treści okazały się nieco lepsze, działania w tym zakresie podejmowano w odniesieniu do 1/3 respondentów. Oczywiście nie wiemy, w jakim okresie były podejmowane takie działania (poza tym, że częściej miały miejsce na etapie szkoły podstawowej niż na późniejszych etapach), jak długo trwały, w jakich formach i czy były regularne – są to aspekty wymagające pogłębienia badań.

Analiza aktywnej formy sekstingu (wysyłanie swoich zdjęć o charakterze erotycznym) wykazała, że odbiorców w tym procederze najczęściej stanowiły osoby tworzące bliskie relacje z badanymi (dziewczyny lub chłopcy, z którymi byli w związku). Dotyczyło to około połowy respondentów, podczas gdy w pozostałych przypadkach, tj., kiedy odbiorcami były koleżanki lub koledzy, była to ok. 1/4 i częstotliwość w tym przypadku była znacznie niższa; przeważnie był to raz lub kilka razy, podczas gdy

we wspomnianych związkach działo się to zwykle kilka razy lub wielokrotnie. Nie dostrzeżono wyraźnego związku między powyższymi odpowiedziami a interesującą nas kontrolą rodzicielską ani czasem spędzanym w sieci przez badanych, ani treściami internetowymi, do których mieli dostęp.

Ponadto, wyniki dotyczące źródeł wiedzy o sekstingu ukazały, że najczęściej są to media (taką odpowiedź zaznaczyło ponad 2/5 badanych), jednak u ponad połowy w tej grupie wskazywano konkretnie internet, a więc miejsce, w którym można znaleźć zarówno wartościowe i edukujące informacje, jak i zupełnie niesprawdzone czy niewiarygodne. Znacznie rzadziej wskazywano szkołę (ponad 1/10), a także przyjaciół i rodzinę (po kilka procent). Prawie co trzeci respondent nie podał żadnego źródła albo pisał, że takowego nie posiada lub podawał ogólnikowe, niewiele znaczące odpowiedzi. W tym kontekście wiele mówią dane dotyczące preferowanych przez młodzież źródeł w omawianym zakresie, gdzie dominowała szkoła (ponad 3/5 wskazań), ale dość często wskazywano również media (blisko 2/5) oraz rodziców (taki sam wynik, jak media, przy czym warto zaznaczyć, że w poprzednim pytaniu niemal nie „istnieli"), a dodatkowo 1/10 respondentów uznała, że funkcję tę powinien pełnić także Kościół. Znaczące jest, że zaledwie garstka respondentów (4%) uznała, iż nie ma potrzeby edukowania o zagrożeniach związanych z sekstingiem, co oznacza, że młodzież dostrzega potrzebę podejmowania takich działań. Dla wzmocnienia tego przekazu można dodać, iż większość uczniów (77%, w tym 81% dziewcząt i 68% chłopców) uznała, że seksting nie jest bezpieczną aktywnością, a jedynie 8% temu zaprzeczyło (odpowiednio 6% i 13%), zaś 12% podało inną odpowiedź (odpowiednio 10% i 16%), pisząc zwykle, że to zależy od sytuacji albo że nie mają zdania na ten temat.

Powiązanie danych dotyczących kontroli rodzicielskiej czasu online oraz treści internetowych z edukowaniem w domu o zagrożeniach wypływających z sekstingu wykazało, że bardziej zaangażowanej postawie rodziców częściej towarzyszyło uświadamianie dzieci na temat ryzyka, jakie za sobą niesie. Przy czym różnice nie są tak wyraźne w odniesieniu do kontroli czasu, jak w odniesieniu do kontroli treści dostępnej dla młodych respondentów. Jednak uzyskane wyniki pozwalają na wysunięcie ostrożnych wniosków dotyczących związku zainteresowania rodziców tym, ile czasu ich dzieci spędzają online i co robią w sieci, z częstszym przestrzeganiem ich przed zagrożeniami związanymi z omawianym zjawiskiem.

Reasumując, wydaje się, że zaangażowanie rodziców w czas i sposoby ich aktywności online, są pożądane z wielu powodów, także w odniesieniu do ryzykownych zachowań, takich jak seksting. Badania potwierdzają, że zagrożenia napotkania negatywnych doświadczeń dzięki stosowaniu profilaktycznych zabiegów rodzicielskich spadają od 5% do 18%. Najskuteczniejsze działania to przede wszystkim: wspólne aktywności z dzieckiem w internecie (ryzyko mniejsze o 13%) oraz rozmowy na temat funkcjonowania niebezpieczeństw w sieci (ryzyko mniejsze o 10%). Sprawowanie kontroli przez opiekunów ma największe znaczenie w przypadku zamieszczania przez dzieci materiałów w sieci (ryzyko mniejsze o 18%), korzystania przez nie z komunikatorów internetowych (ryzyko mniejsze o 15%), ściągania filmów/muzyki (ryzyko mniejsze o 13%)[28]. Przy

[28] *Ibidem*, s. 34–35.

czym kontrola rodzicielska nie może polegać wyłącznie na zainstalowaniu programów blokujących szkodliwe treści, ponieważ co trzecie dziecko wie, jak obejść takie blokady[29]. Dodatkowo, z oczywistych względów, im dziecko jest starsze, tym więcej zostawia mu się swobody, również biorąc pod uwagę jego prawo do prywatności.

Jednak konieczne jest stosowanie jasnych reguł korzystania z internetu od najmłodszych lat, wymaganie respektowania tych zasad, czujność rodzicielska oraz inicjowanie rozmów uświadamiających. Niemniej ważne jest troska i dbałość o bliskie relacje, budowanie wzajemnego zaufania, a zarazem otwartość na potrzeby dzieci i renegocjowanie (zwłaszcza z młodzieżą) sposobów użytkowania sieci.

Jak dowodzi Ewa Nowicka, jednym z zadań rodziców jest „wyjaśnianie, czym są media, wprowadzanie i przestrzeganie reguł korzystania z mediów, dawanie dobrych przykładów użytkowania środków masowego przekazu, prowadzenie dyskretnej kontroli oraz rozmów na temat różnorodnych komunikatów medialnych, organizowanie spędzania wolnego czasu w sposób aktywny i interesujący. Wychowanie medialne prowadzone w rodzinie jest jednak niewystarczające. Idealnym uzupełnieniem i kontynuacją jest środowisko szkolne"[30]. Dlatego jest to kolejny podmiot, który powinien zajmować się tematyką sekstingu. Działania tej instytucji wychowawczej z jednej strony mają być komplementarne w stosunku do uczniów, a z drugiej strony wspierające wobec rodziców, którzy nie zawsze są świadomi zagrożeń, jakie niesie za sobą korzystanie z nowych technologii i czasami sami potrzebują pomocy pedagogicznej, aby móc w odpowiedni sposób i z większą skutecznością pokierować swoimi dziećmi, by były bezpieczne w cyfrowym świecie.

Bibliografia

Albury K., Crawford K., Byron P., Mathews B. (2013). *Young People and Sexting in Australia: ethics, representation and the law*. "ARC Centre for Creative Industries and Innovation. Journalism and Media Research Centre". The University of New South Wales, Australia.

Badenhorst C. (2011). *Legal responses to cyber bullying and sexting in South Africa*. "Centre for Justice and Crime Prevention, CJCP Issue Paper" 10, South Africa.

Baumgartner S.E., Valkenburg P.M., Peter J. (2010). *Assessing causality in the relationship between adolescents' risky sexual online behavior and their perceptions of this behavior.* "Journal of Youth & Adolescence", 39.

Bereźnicka M., Rokitowska J. (2021). *Seksting – wiedza, doświadczenia i opinie młodzieży.* Wydawnictwo Libron. Kraków.

EU Kids Online. www.eukidsonline.net [dostęp: 10.08.2024].

Gajda J. (2009). *Poznawanie dziecka w aspekcie współczesnej pedagogiki kultury*. W: J. Izdebska, J. Szymanowska (red.). *Dziecko w zmieniającej się przestrzeni życia. Obrazy dzieciństwa*. Białystok.

Kozak S. (2011). *Patologie komunikowania w Internecie. Zagrożenia i skutki dla dzieci i młodzieży*. Wydawnictwo Difin. Warszawa.

[29] S. Kozak (2011). *Patologie komunikowania w Internecie. Zagrożenia i skutki dla dzieci i młodzieży* (s. 205). Wydawnictwo Difin. Warszawa.

[30] E. Nowicka (2015). *Rola rodziców i nauczycieli w edukacji medialnej*. „Dyskursy Młodych Andragogów", 16, 215.

Lange R., Osiecki J. (2014). *Nastolatki wobec Internetu*. NASK, Rzecznik Praw Dziecka oraz Wyższa Szkoła Nauk Społecznych PEDAGOGIUM. Warszawa. https://www.nask.pl/pl/raporty/raporty/3473,Raport-z-badan-quotNastolatki-wobec-internetuquot-2014.html [dostęp: 10.09.2024].

Lange R., NASK (red.). (2011). *Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów*. NASK – Państwowy Instytut Badawczy. Warszawa.

Łoś M. i in. *Mapa czynników ryzyka i chroniących młodzież przed zachowaniami ryzykownymi. Raport I z badań NPZ.XI_17.2017*. Instytut Profilaktyki Zintegrowanej, 61 i 66. https://ore.edu.pl/wp-content/uploads/2018/10/raport-i-mapa-czynnikow-ryzyka-i-chroniacych-mlodziez-przed-zachowaniami-ryzykownymi.pdf [dostęp: 1.10.2024].

Makaruk K. (2013). *Korzystanie z portali społecznościowych przez młodzież. Wyniki badania EU NET ADB*. Fundacja Dzieci Niczyje. *„Dziecko krzywdzone. Teoria, badania, praktyka*", t. 12, nr 1.

Makaruk K., Włodarczyk J., Michalski P. *Kontakt dzieci i młodzieży z pornografią. Raport z badań.* Fundacja Dajemy Dzieciom Siłę 2017. https://www.saferinternet.pl/pliki/Raport-kontakt_dzieci_i_mlodziezy_z_pornografia.pdf [dostęp: 26.09.2024].

Mazur J. i in. (2008). *Czynniki chroniące młodzież 15-letnią przed podejmowaniem zachowań ryzykownych*. Raport z badań HBSC 2006. Instytut Matki i Dziecka. Zakład Ochrony i Promocji Zdrowia Dzieci i Młodzieży. Warszawa.

Mishna F., Khoury-Kassabri M., Gadalla T., Daciuka J. (2012). *Risk factors for involvement in cyber bullying: Victims, bullies and bully–victims*. "Children and Youth Services Review", 34.

Mitchell K.J., Finkelhor D., Jones L.M., Wolak J. (2012). *Prevalence and Characteristics of Youth Sexting: A National Study*. "Crimes against Children Research Center". University of New Hampshire. Durham.

Nowicka E. (2015). *Rola rodziców i nauczycieli w edukacji medialnej*. „Dyskursy Młodych Andragogów", 16, 215.

Phippen A. (2009). *Sharing Personal Images and Videos Among Young People*. University of Plymouth. https://childnetsic.s3.amazonaws.com/downloads/Research_Highlights/UKCCIS_RH_10_Sexting.pdf [dostęp: 23.09.2024].

Pyżalski J., Zdrodowska A., Tomczyk Ł., Abramczuk K. (2019). *Polskie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski*. Wydawnictwo Naukowe UAM. Poznań.

Ringrose J., Gill R., Livingstone S., Harvey L., *A Qualitative study of children, young people and 'sexting': a report prepared for the NSPCC*. https://eprints.lse.ac.uk/44216/1/__Libfile_repository_Content_Livingstone%2C%20S_A%20qualitative%20study%20of%20children%2C%20young%20people%20and%20%27sexting%27%20%28LSE%20RO%29.pdf [dostęp: 15.09.2024].

Smith P.K., Mahdavi J., Carvalho M., Fisher S., Russell S., Tippett N. (2008). *Cyberbullying, its forms and impact in secondary school pupils*. "Journal of Child Psychology and Psychiatry", 49.

Temple J. R., Jonathan A. P., Van Den Berg P., Le V. D., McElhany A., Temple B. W. (2012). *Teen Sexting and Its Association With Sexual Behaviors.* "Archives of Pediatrics and Adolescent Medicine", 166(9).

Wojtasik Ł. *Kontakt dzieci z niebezpiecznymi treściami w Internecie*. Raport z badań Gemius/Fundacja Dajemy Dzieciom Siłę. https://bibe.ibe.edu.pl/475-kontakt-dzieci-z-niebezpiecznymi-tresciami-w-internecie.html [dostęp: 17.09.2024].

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

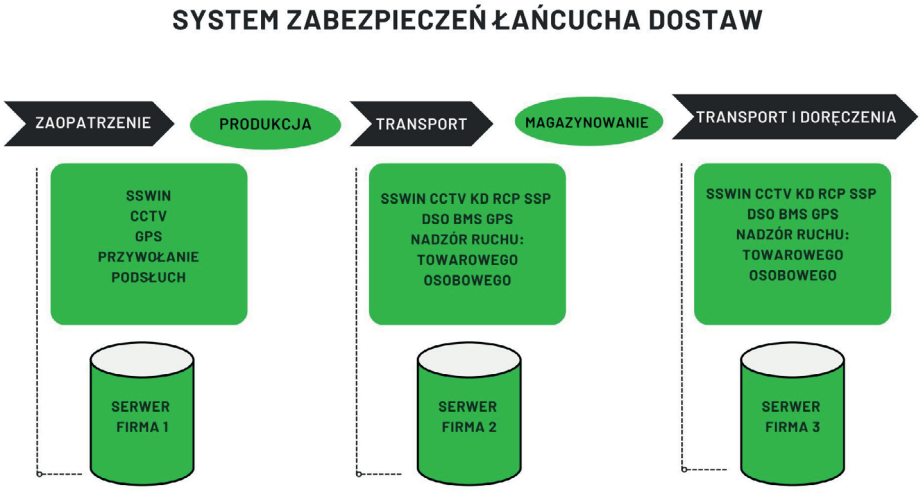
Szybki rozwój systemów ochrony technicznej przyczynia się do zwiększenia różnorodności zasobów informacji magazynowanych w pamięciach wewnętrznych urządzeń oraz na serwerach. Równocześnie uległy zwiększeniu zasoby dostępnych informacji. Stosowanie serwerów czasu oraz synchronizowanych z nimi wewnętrznych 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].

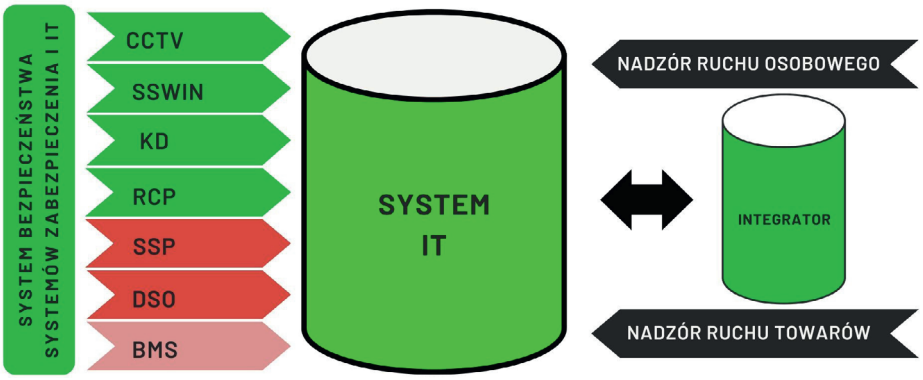
– zjazd z określonej trasy przejazdu[8].

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.