Zeszyty Naukowe SGSP 2020, Nr 73/1/2020

dr Grzegorz Matuszek
Akademia Wyższa Szkoła Biznesu w Dąbrowie Górniczej

DOI: 10.5604/01.3001.0014.0784

Monitoring wizyjny – ujęcie prawne i technologiczne. Współczesność i perspektywy

Abstrakt

Monitoringi wizyjne są obecnie jednymi z najszerzej wykorzystywanych środków mających wpływać na bezpieczeństwo i porządek publiczny. Warunkiem pełnego wykorzystania możliwości monitoringu wizyjnego jest przestrzeganie norm technicznych na etapie budowy i eksploatacji systemu. Obecnie aspekty techniczne reguluje norma PN-EN 62676-1-1:2014-06 Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 1-1:Wymagania systemowe – Postanowienia ogólne. Dynamiczny rozwój technologii informatycznych, w tym opartych na sztucznej inteligencji daje coraz większe możliwości. Systemy wykorzystujące zaawansowane oprogramowanie pozwalają na automatyczne sygnalizowanie zagrożeń. Daje to możliwość ograniczenia personelu oraz zwiększenie skuteczności monitoringów wizyjnych. Przykładem systemu opartego na tego typu oprogramowaniu jest Katowicki Inteligentny System Monitoringu i Analiz.

Słowa kluczowe: bezpieczeństwo i porządek publiczny, monitoring miejski, monitoring wizyjny, normy techniczne, sztuczna inteligencja

Przyjęty: 31.01.2020; Zrecenzowany: 07.03.2020; Zatwierdzony: 13.03.2020

CCTV Systems – Technological and Legal Aspects. The Present and the Prospects for Future

Abstract

CCTV system is currently one of the most commonly used means of influencing the safety and public order. A necessary condition for taking full advantage of the system is following technical standards in the process of creating and using CCTV. The current standard

for technical standards is PN-EN 62676-1-1: 2014-06 CCTV Surveillance systems used in security. Part 1-1: system requirements – General provisions. The dynamic development of information technologies, including those based on artificial Intelligence, offers a wide range of possibilities. Systems based on advanced software allow automatic notification of threats. This in turn enables limiting the number of employees as well as increasing the efficiency of CCTV. An example of a system based on such software is the Intelligent System of Monitoring and Analysis in Katowice.

Keywords: safety, public order, video monitoring, city monitoring, technical standards, artificial intelligence

Received: 31.01.2020; Reviewed: 07.03.2020; Accepted: 13.03.2020

Відеомоніторинг – правовий та технологічний підхід. Сучасність та перспективи

Анотація

На даний момент відеомоніторинг є одним із найбільш широко застосовуваних заходів щодо впливу на громадську безпеку та порядок. Умовою повного використання можливостей відеомоніторингу є відповідність технічним стандартам на етапі побудови та експлуатації системи. В даний час технічні аспекти регулюються нормами PN-EN 62676-1-1:2014-06 Системи спостереження CCTV, що використовуються в забезпеченнях – Частина 1-1: Системні вимоги – Загальні положення. Динамічний розвиток інформаційних технологій, у тому числі на основі штучного інтелекту, дає все більші можливості. Системи, що використовують вдосконалене програмне забезпечення, дозволяють автоматично сигналізувати про загрози. Це дає можливість скоротити персонал та підвищити ефективність відеоспостереження. Прикладом системи на основі цього типу програмного забезпечення є Інтелектуальна Система Моніторингу та Аналізу в м. Катовіце.

Ключові слова: громадський порядок та безпека, моніторинг міста, відеомоніторинг, технічні норми, штучний інтелект

Прийнятий: 31.01.2020; Рецензованої: 07.03.2020; Затверджений: 13.03.2020

Wstęp

Jedną z najważniejszych potrzeb człowieka jest potrzeba bezpieczeństwa. Jest ona jednym z elementów hierarchii potrzeb, stanowiących naturalną drogę rozwoju człowieka. Wiedzie ona od zaspokojenia podstawowych potrzeb do potrzeb wyższego rzędu [1, s. 445–446]. Troska o bezpieczeństwo towarzyszyła, towarzyszy i będzie towarzyszyć ludziom zawsze [2, s. 291]. Potrzeba bezpieczeństwa jest mocno związana z grupą potrzeb fizjologicznych, stąd też wynika, że jednym z podstawowych celów działania jednostki jest zapewnienie sobie bezpiecznego bytu i warunków rozwoju [3, s. 23]. Jedną z nowoczesnych metod wykorzystywanych na rzecz bezpieczeństwa jest dynamicznie ewoluujący monitoring wizyjny.

Kamery monitoringu stały się naturalnym elementem naszego życia. W literaturze pojawia się uzasadniona teza, że żyjemy w społeczeństwie nadzorowanym [4, s. 8]. Monitoring jest obecnie jednym z najpopularniejszych i najszerzej wykorzystywanych środków mających wpływać na poprawę poczucia bezpieczeństwa [5, s. 30]. Przykładem skali wykorzystania monitoringu na świecie są doświadczenia brytyjskie. Praktycznie we wszystkich brytyjskich miastach wprowadzono systemy monitoringu wizyjnego, które w dalszym ciągu są rozbudowywane. Już w 2002 r. w Wielkiej Brytanii szacunkowo zainstalowanych było ponad cztery mln kamer, co oznacza, że jedna kamera przypadała na 14 osób [5, s. 36]. Obecnie krajem w którym wykorzystuje się największą ilość kamer monitoringu są Chiny. Funkcjonuje tam ponad 200 mln kamer [6]. W Polsce monitoring wizyjny, w tym monitoring miejski, jest również powszechnie wykorzystywany. Dotyczy to wszystkich miast wojewódzkich oraz ponad 85% miast powiatowych [7, s. 8]. Jedną z przyczyn gwałtownego wzrostu wykorzystania monitoringu wizyjnego w systemie bezpieczeństwa publicznego jest rozwój technologiczny. Obecnie instalowane systemy są efektywniejsze, dokładniejsze niż te stosowane jeszcze kilka lat temu. Coraz częściej wykorzystują one oprogramowanie komputerowe pozwalające automatycznie ustalić numery tablic rejestracyjnych pojazdów, rozpoznawać anomalie w monitorowanej przestrzeni, jak również identyfikować wizerunki osób.

Celem niniejszej publikacji jest przedstawienie monitoringu wizyjnego jako narzędzia wykorzystywanego na rzecz bezpieczeństwa i porządku publicznego. Autor przybliża systemy CCTV w kontekście przepisów normalizacyjnych, regulujących ich budowę oraz eksploatację. Przywołuje normy, których realizacja daje gwarancję skutecznego wykorzystania monitoringu wizyjnego. Jako przykład systemu budowanego i używanego w oparciu o obowiązujące przepisy normalizacyjne wskazuje

on Katowicki Inteligentny System Monitoringu i Analiz. Celem autora jest również wskazanie i zasygnalizowanie możliwych kierunków rozwoju systemów monitoringów wizyjnych. Jako przykład podaje on metodę uczenia maszynowego stanowiącą jeden z najważniejszych działów sztucznej inteligencji. W aspekcie możliwych kierunków rozwoju systemów CCTV autor zachęca odbiorcę do pogłębienia wiedzy.

1. Pojęcie monitoringu wizyjnego

W Polsce nie ma jednej, utrwalonej definicji monitoringu wizyjnego. Jest on zamiennie nazywany telewizją przemysłową, telewizją dozorową, wideonadzorem lub CCTV. Podobnie jak M. Szumańska, autor uważa, że żadne z tych wyrażeń nie jest pozbawione wad [8, s. 11]. Najbardziej niejednoznacznym, a najpopularniejszym jest pojęcie „monitoring". Jest ono prostą recepcją angielskiego czasownika *monitor* oznaczającego wprost „kontrolować" czy też „nasłuchiwać" [9, s. 117]. Tak też pojęcie to jest tłumaczone w „Słowniku współczesnego języka polskiego", tj. monitoring rozumiany jako „[…] prowadzenie stałej obserwacji, dokonywanie ciągłych systematycznych pomiarów" [10, s. 533]. W literaturze przedmiotu próbuje się zdefiniować pojęcie monitoringu wizyjnego, mając na uwadze cel oraz sposób działania systemu. Cel działania wskazuje między innymi P. Kałużny, opisując telewizyjne systemy dozorowe jako zespoły telewizyjnych środków technicznych i programowych przeznaczonych do obserwacji, wykrywania, rejestrowania oraz sygnalizowania warunków wskazujących na istnienie niebezpieczeństwa powstania szkód lub zagrożenia osób i mienia [11, s. 11]. Definicję ukierunkowaną na sposób działania przedstawia P. Waszkiewicz. Według niego monitoring wizyjny (ang. *closed circuit television* – CCTV, niem. *Videoüberwachung*) to system pozwalający na śledzenie z odległości zdarzeń rejestrowanych przez jedną, do niekiedy nawet kilkuset kamer jednocześnie. W skład systemu wchodzą kamery, z których obraz jest transmitowany do centrum odbiorczego, gdzie personel na monitorach może obserwować rejestrowane zdarzenie. Monitoring wizyjny, określany też jako telewizja dozorowa, różni się od zwykłej telewizji tym, że obraz z kamer jest przesyłamy i odbierany tylko w centrum odbiorczym, a nie w nieograniczonej liczbie odbiorników [5, s. 30]. Brakuje ustawowej definicji monitoringu wizyjnego. Definicję monitoringu opracowaną w oparciu o „Słownik wyrazów obcych" przedstawia Najwyższa Izba Kontroli w informacji o wynikach kontroli „Funkcjonowanie miejskiego monitoringu wizyjnego". Według tej definicji monitoringiem jest system długookresowej lub powtarzalnej obserwacji danego typu zjawisk lub reakcji na nie, wielkości,

parametrów, właściwości składu itp.; potocznie jest określany jako obserwacja na monitorach obrazu transmitowanego z danego miejsca za pomocą zainstalowanych tam kamer i odpowiednich łączy (zwany także monitoringiem wizyjnym) [8]. Z tą definicją koresponduje ta przedstawiona przez A. Ordysińską. Według niej monitoring wizyjny to system przekazywania informacji polegający na planowym (ciągłym, prowadzonym w ściśle określony sposób za pomocą wytycznych funkcjonalnych i procedury) obserwowaniu (często również rejestracji) za pomocą środków technicznych zdarzeń, które zachodzą w określonym miejscu, mający na celu zapobieganie przestępstwom, wykroczeniom, wypadkom oraz przypisanie winy, odpowiedzialności za popełnione czyny [12, s. 38]. P. Wittich przywołuje definicję systemu monitoringu wizyjnego określoną w polskiej normie PN-EN 50132-7. Zgodnie z nią jest to system składający się z punktów kamerowych, urządzeń kontrolnych oraz urządzeń do przesyłu i sterowania; system może być niezbędny do dozorowania określonej strefy bezpieczeństwa. Zgodnie z definicją określoną w przytoczonej normie, kamera jest to urządzenie zawierające przetwornik obrazu, wytwarzający sygnał wizyjny z obrazu optycznego [13]. Autor uważa, że wszystkie przedstawione definicje monitoringu wizyjnego, szeroko i ogólnie opisują istotę jego działania.

2. Monitoring wizyjny a przepisy normalizacyjne

Monitoring wizyjny, będąc elementem systemu bezpieczeństwa i porządku publicznego powinien działać w oparciu o instalacje (urządzenia i oprogramowanie) służące do odbioru, rejestracji obrazu, rejestracji oraz jego odtwarzania. Całość systemu CCTV powinna dawać rękojmię realizacji założonych celów oraz określonej skuteczności działania. Ponadto powinna podlegać systematycznej ocenie. Chcąc w pełni wykorzystywać możliwości jakie dają systemy monitoringu wizyjnego, należy je dostosować do zasad określonych w przepisach normalizacyjnych. Do 2016 r. obowiązywała polska norma na systemy alarmowe – systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 7: Wytyczne stosowania (PN-EN50132-7:2012-04). Norma określała procedury związane z projektowaniem systemów oraz techniczne parametry wykorzystywanego sprzętu w zależności od zdefiniowanego celu. Rozszerzała ona regulacje w odniesieniu do poprzedniej normy (PN-EN 50132-7:2003) o technologie IP, wprowadzała zagadnienia ochrony przed dostępem do urządzeń w warstwie fizycznej, wprowadzała zagadnienia integracji systemów [14]. Między innymi, w oparciu o te normy budowano Katowicki Inteligentny System Monitoringu i Analiz. Od 2016 r. obowiązuje nowa norma:

PN-EN 62676-1-1:2014-06 Systemy dozorowe CCTV stosowane w zabezpieczeniach – Część 1-1:Wymagania systemowe – Postanowienia ogólne [15]. Norma IEC *(International Electrotechnical Commission)* wprowadza m.in. nowy termin, tj. VSS (*Video Surveillance Systems*) zamiennie stosowany z CCTV. Norma określa minimalne wymagania eksploatacyjne i funkcjonalne, które należy uzgadniać w relacjach między użytkownikiem, stróżami prawa i dostawcą. Podobnie jak w przypadku poprzedniej normy, nie reguluje ona wymagań dotyczących projektowania, planowania, instalowania, testowania, działania i konserwacji. Norma nie odnosi się do systemów zdalnie monitorujących czujek, aktywujących systemy CCTV. Norma PN-EN 62676-1-1:2014-06 ma zastosowanie w systemach VSS dzielących środki detekcji, wyzwalania, połączeń wzajemnych, sterowania, łączności oraz zasilania sieciowego z innymi aplikacjami. Szczegółowe wymagania w zakresie wykorzystania aplikacji rozpoznania i detekcji znajdują się w wytycznych IEC 62676-4. Klasyfikacja poszczególnych aplikacji rozpoznania i detekcji określa cel zastosowania CCTV, a jednocześnie determinuje standardy w zakresie stopnia wypełnienia ekranu postacią ludzką. Poszczególne aplikacje omawia Z. Szachnitowski. Wskazuje, że od aplikacji monitorowania wymaga się 5% wypełnienia ekranu, a w przypadku inspekcji standard określa skalę wypełnienia ekranu na 400% fragmentu postaci poddawanej identyfikacji. Ta aplikacja jest najbardziej pożądana w przypadku badań identyfikacyjnych, dowodowych [16, s. 38]. Nowa norma została opublikowana 2 września 2014 r. i narzuciła termin zaadaptowania nowych standardów na 2 grudnia 2016 r. Wytyczne normalizacyjne regulują następujące kwestie:

- podstawy prawne, terminologia, definicja i skróty;
- zasady organizacji systemów, w tym: ogólne regulacje dotyczące VSS, szczegółowe regulacje dotyczące rejestracji i obrabiania materiału wizyjnego;
- zasady zarządzania systemem, w tym: zarządzanie danymi, zarządzanie organizacją, współpraca z innymi systemami;
- bezpieczeństwo systemu, w tym: integralność systemu, integralność danych, stopnie zabezpieczenia;
- wymagania techniczne, w tym: wymagania w zakresie rejestracji obrazu, jego obróbki, jakości obrazu;
- określenie przestrzeni, w jakich rejestrowane są obrazy;
- zasady dokumentowania pracy systemu.

Wytyczne obrazowo przedstawiają trzy obszary, które warunkują skuteczne wykorzystanie systemów VSS, tj.: środowisko rejestracji obrazu, zarządzanie systemem, bezpieczeństwo systemu. W zakresie środowiska rejestracji obrazu, głównymi płasz-

czyznami skutecznego funkcjonowania systemów CCTV jest rejestrowanie przebiegu wydarzenia, obróbka tego materiału, wyświetlenie go operatorowi wraz z powiązanymi informacjami dla łatwego i efektywnego użycia. W obszarze „Zarządzanie systemem" norma wyodrębnia zagadnienia dotyczące zarządzania danymi i działaniami oraz współpracę z innymi systemami. W zakresie współpracy z innymi systemami norma wskazuje, że poszczególne formaty danych muszą być zgodne dla wszystkich systemów. Jako przykłady współpracujących systemów wytyczne wskazują na:

- inne systemy bezpieczeństwa (np. alarmy włamaniowe, alarmy napadowe, alarmy przeciwpożarowe);
- inne systemy zarządzania bezpieczeństwem (np. centra zarządzania);
- inne systemy nie związane bezpośrednio z bezpieczeństwem (np. bankomaty, systemy rozpoznawania numerów rejestracyjnych, systemy zarządzania budynkami, systemy rejestracji w placówkach handlowych).

W obszarze „Bezpieczeństwo systemu" norma wyróżnia dwie kategorie, tj.:

- integralność systemu – rozumiana jako fizyczna ochrona elementów systemu, kontrola dostępu do systemu (ochrona fizyczna kamer i dostępu do wizji);
- integralność danych – rozumiana jako zabezpieczenie dostępu do danych, uniemożliwienie utraty danych oraz uniemożliwienie modyfikowania (manipulowania) zapisanych obrazów.

Wytyczne opisują politykę bezpieczeństwa odnoszącą się do ryzyka wystąpienia określonych zagrożeń i wypadków w odniesieniu do możliwych konsekwencji wystąpienia takich sytuacji. Wprowadzają czterostopniowy system zarządzania bezpieczeństwem i ryzykiem.

Dużą wagę norma PN-EN 62676-1-1:2014-06 przywiązuje do sposobu przechowywania danych, szczególnie w kontekście możliwej ich utraty. Wskazuje na konieczność spełnienia szeregu wymagań technicznych dla jakości obrazu, np.: rozdzielczość i rozmiar przechowywanych zdjęć, sposób kompresowania zdjęć, określenia czasu ponownej rejestracji obrazu po restarcie systemu. Zgodnie z wytycznymi system monitoringu powinien między innymi udzielać bieżących informacji o:

- objętości nagranego materiału;
- zdolności przechowywania nagranego materiału;
- czasu nagrania;
- pozostałej wolnej pamięci, pozwalającej na rejestrację obrazu.

Wytyczne określają ogólne zasady archiwizacji danych. Wynika z nich, że muszą być one przechowywane w celach dowodowych. Z drugiej strony musi istnieć możliwość

ich przekazywania oraz odtwarzania w innej lokalizacji. Jednocześnie muszą istnieć możliwości techniczne pozwalające na ciągłą pracę rejestracyjną systemu, również w momencie odtwarzania nagranego materiału. Stosując kompresje danych, norma zaleca niestosowanie oprogramowania wymagającego zgody producenta na jego używanie. Norma odnosi się do formatów, w jakich dane mogą być zapisywane. Podaje przykłady zalecanych formatów, stanowiących międzynarodowe standardy, np.:

1. formaty zapisu wideo:
- H.264: AVC: ISO/IEC 14496-10;
- MPEG-4 part 2: ISO/IEC 14496-2;
- MPEG-2: ISO/IEC 13818-1;
- H.263: ITU-T Rec. H. 263;
- JPEG 2000: ISO/IEC 15444-1;
- JPEG: ISO/IEC 10918-1.

2. formaty zapisu audio:
- G. 711: ITU-T Rec. G.711;
- G.726: ITU-T Rec. G.726;
- AAC. ISO/IEC 14496-3.

3. eksport danych, format plików:
- MP4: ISO/IEC 14496-14;
- MPEG-A: ISO/IEC 23000-10:2009.

Omawiane wytyczne wymieniają zasady, jakimi należy się kierować w trakcie przesyłania i odtwarzania danych, tj.:

- nie można zmieniać jakości nagrania, jego rozdzielczości, a w trakcie eksportu danych nie powinna następować utrata poszczególnych klatek zapisu;
- system nie powinien stosować dalszej kompresji lub konwersji eksportowanych danych – to może zredukować ich użyteczność;
- jeżeli jest to możliwe, to wraz z nagraniem powinno się przesyłać również uwierzytelnione podpisy oraz metadane;
- system nie może stracić swojej podstawowej funkcjonalności w trakcie przesyłania danych;
- metoda eksportu powinna być odpowiednia dla zdolności systemowych.

Norma określa wymagania dotyczące programu do odtwarzania materiału, który powinien posiadać następujące funkcje:

- odtwarzanie w czasie rzeczywistym (*real time play*);

- stop, pauza, przewijanie do przodu i do tyłu oraz odtwarzanie „klatka po klatce", a także oglądanie materiału wstecz;
- odtwarzanie na ekranie widoku z jednej lub więcej kamer, zachowując jednocześnie właściwy stosunek rozmiaru kadru;
- pokazywanie obrazu z jednej kamery na maksymalnej rozdzielczości nagrania;
- możliwość przeszukiwania zawartości obrazu, zgodnie z przyjętym kryterium czasu;
- możliwość zapisywania materiału, ewentualne jego drukowanie ze wskazanym czasem i datą nagrania;
- możliwość zsynchronizowania odtwarzania obrazu z kilku kamer jednocześnie;
- możliwość odtwarzania plików audio i innych metadanych;
- zdolność przesyłania obrazów w standardowych formatach;
- system powinien czytelnie wskazywać czas, datę i inne informacje dotyczące nagrania.

Istotnym wymaganiem stawianym przed administratorem systemu jest wykorzystywanie oprogramowania pozwalającego na odtwarzanie nagranego materiału na komputerach wykorzystujących system operacyjny Windows.

Kolejne wytyczne odnoszą się do obszarów związanych z zarządzaniem, tj. „zarządzanie systemem" oraz „zarządzanie czynnościami, działaniami". W przypadku zarządzania systemem, twórcy normy wskazują m.in. na następujące wymagania:

- obsługa systemu musi być dla operatora prosta, szybka i intuicyjna;
- cały czas musi być podawana czytelna informacja o stanie pracy systemu;
- system musi natychmiast identyfikować sytuacje alarmowe wraz z informacją o zdarzeniu (informacja musi być zwarta i czytelna).

W przypadku zarządzania konkretnymi działaniami, norma w szczególny sposób odnosi się do systemów wykorzystujących inteligentne komponenty analizy obrazu. Nakłada ona następujące wymagania:

- dane alarmowe (alerty) muszą mieć pierwszeństwo przed danymi rejestrowanymi automatycznie w trybie ciągłym;
- obraz, który przegląda operator musi być czytelnie opisany jako obraz oglądany „na żywo" lub też odtwarzany;
- bardzo ważne wymaganie dotyczy umieszczania informacji o tym, czy zarejestrowany obraz był nagrywany w trybie automatycznym (wywołanym przez alert), czy też w trybie manualnym (na polecenie operatora);
- materiały z nagrań alertów muszą być dostępne w takiej kolejności, w jakiej były rejestrowane. Wyjątek stanowią sytuacje, w których występuje gradacja priorytetów.

W tym przypadku alarmy priorytetowe maja pierwszeństwo przed innymi;

- system musi wykorzystywać wyraźnie odmienne sygnały dla różnych sytuacji: alertów, awarii systemu lub prób manipulacji przy systemie;
- alert musi być dla operatora widoczny (obraz) i słyszalny (dźwięk). W przypadku alertu dotyczącego zdarzenia kwalifikowanego jako poziom 3 i 4 bezpieczeństwa, system powinien podawać dodatkowe informacje (źródło alertu, typ alertu, data, godzina);
- administrator systemu powinien prowadzić dziennik.

Wytyczne określają, które czynności muszą być dokumentowane w zależności od poziomu bezpieczeństwa, np.:

- wzbudzenie alarmu – przy poziomach od 2–4;
- manipulowanie w systemie – przy poziomach od 3–4;
- utrata nagrań lub przywracanie nagrań video – przy poziomach 3–4;
- utrata zasilania – przy poziomach od 2–4;
- ponowne uruchomienie systemu (reset systemu), zatrzymanie – przy poziomach od 2–4;
- wyszukiwanie nagrań i ich odtwarzanie – przy poziomach od 3–4;
- zmiana parametrów nagrywania – przy poziomach 3–4.

Na obszar związany z bezpieczeństwem systemu składają się: integralność systemu oraz integralność danych. Na uwagę zasługują regulacje dotyczące ujawniania usterek, gdzie podobnie jak w przypadku alertów, powinna występować gradacja awarii. System powinien być również zdolny do ciągłego zapisywania materiału. W przypadku awarii energetycznej nie może dojść do utraty zarejestrowanych już danych. Zgodnie z normą, system powinien automatycznie wykrywać i alarmować o próbach manipulowania nagraniami. Jako przykłady takich manipulacji wskazano: zmiany danych w trakcie obróbki materiału, usuwanie nagrania, zamazywanie lub zniekształcanie obrazu, zmiana pola widzenia kamery. Każda praca na materiale wizyjnym musi być autoryzowana poprzez wykorzystanie odcisku linii papilarnych, wykorzystanie cyfrowego znaku wodnego lub wykorzystanie algorytmu kryptograficznego z użyciem sumy kontrolnej.

Na uwagę zasługuje charakterystyka przestrzeni podlegających monitorowaniu. Norma dzieli przestrzeń na cztery klasy, tj.:

- Klasa I – wnętrze budynku mieszkalnego lub komercyjnego, w zakresie temperatur: od –5°C do +40°C i wilgotności około 75%;
- Klasa II – wnętrze budynku, gdzie stała temperatura nie jest utrzymywana (korytarze, piwnice, magazyny), w zakresie temperatur od –10°C do +40°C, przy 75% wilgotności;

- Klasa III – na zewnątrz, gdzie komponenty systemu nie są narażone na bezpośrednie oddziaływanie deszczu lub słońca, ewentualnie ekstremalne warunki wewnątrz budynku, w zakresie temperatur od –25°C do +50°C, przy wilgotności 75%, a przez 30 dni między 85–95%;
- Klasa IV – na zewnątrz, gdzie komponenty są w pełni wystawione na oddziaływanie czynników pogodowych, w zakresie temperatur od –25°C do +60°C , przy wilgotności 75%, a przez 30 dni między 85–95%.

W zakresie dokumentowania czynności związanych z obsługą systemu norma wskazuje, aby dokumentacja była zwięzła, jasna, kompletna, wystarczająca do zainstalowania systemu, rozpoczęcia jego funkcjonowania, eksploatacji i utrzymania w działaniu.

Reasumując, omówiona norma PN-EN 62676-1-1 szczegółowo przedstawia wymagania w obszarze skutecznej i bezpiecznej eksploatacji systemów monitoringu wizyjnego. Można zauważyć odniesienie do systemów wykorzystujących nowoczesne aplikacje do analizy obrazu opierające się na generowaniu alertów, jak również odniesienie do bezpieczeństwa danych informatycznych. Planowanie i budowa nowoczesnych systemów monitoringów miejskich musi być realizowana w oparciu o międzynarodowe normy techniczne. Inwestor powinien jasno artykułować wykonawcy obowiązek budowy systemu zgodnie z obowiązującymi normami. Przykładem takiego stanowiska jest budowa Katowickiego Inteligentnego Systemu Monitoringu i Analiz. Podkreślić przy tym należy, że stosowanie norm ma charakter dobrowolny zgodnie z treścią art. 4 pkt 3 ustawy z 12 września 2002 r. *o normalizacji*, który wskazuje, że w normalizacji krajowej stosuje się między innymi zasadę dobrowolności uczestnictwa w procesie opracowania i stosowania norm [17].

3. Monitoring wizyjny – perspektywy

Mając na uwadze skalę wykorzystania systemów monitoringu wizyjnego na świecie, należy przypuszczać, że będą rozwijać się dynamicznie również w Polsce. W 2016 r. rynek urządzeń CCTV zanotował mniejszy wzrost obrotów spowodowany głównie przez dostawców z Chin, dążących do obniżania cen i zwiększenia udziałów w rynku. Co ciekawe, przy agresywnej polityce chińskich dostawców, zachodni specjaliści z branży telewizji dozorowej nie odpowiedzieli „cięciem cen" i redukcją marży. Ich działania ukierunkowane zostały ku inwestycjom w nowe technologie i rozwiązania wykorzystujące zaawansowane oprogramowanie do analizy danych. Miały one zapewnić użytkownikom lepszy zwrot z inwestycji, niższy całkowity koszt eksploatacji,

a także poprawę jakości analityki biznesowej. Według specjalistów, rynek telewizji dozorowej w 2017 r. przestał być postrzegany jedynie jako rynek z obszaru ochrony osób i mienia. Przykładem może być wykorzystywanie algorytmów analizy wieku i płci, także rozpoznawania twarzy w sektorze handlu detalicznego. Pozwalają one na dopasowanie treści reklamy do wieku i płci osoby znajdującej się w pobliżu. Innym przykładem jest wykorzystanie technologii rozpoznawania twarzy do automatycznego rejestrowania wykładów w szkolnictwie wyższym. Kolejnym zastosowaniem są kamery 360° w branży turystycznej, gdzie w sklepach, hotelach i kurortach służą one do liczenia ludzi, śledzenia wzorców poruszania się, co przyczynia się do upraszczania operacji biznesowych [18].

Wprowadzane udoskonalenia systemu monitorowania, a w szczególności połączenie go z programami komputerowymi analizującymi obraz przekazywany do centrum odbiorczego, daje szerokie możliwości rozwoju. Jest to jeden z głównych kierunków rozwoju sieci CCTV wspieranych odpowiednim oprogramowaniem. Dotychczasowe doświadczenia mogły wskazywać na problemy związane z poprawnością, niezawodnością analityk obrazów wideo. Te okoliczności mogły sprawić wrażenie, że sieci nie spełniają pokładanych nadziei. Ostatnie lata wskazują jednak, że pojawiają się istotne zmiany, gdzie zarówno algorytmy, jak i oprogramowanie stały się bardziej dopracowane. Wykorzystują między innymi metodę uczenia maszynowego znaną jako *deep learning* (głębokie uczenie). Definicję uczenia maszynowego przedstawia P. Cichosz. Według niego „[…] uczeniem się systemu jest każda autonomiczna zmiana w systemie zachodząca na podstawie doświadczeń, która prowadzi do poprawy jakości jego działania" [19, s. 34]. Wskazuje on również, że maszynowe uczenie się należy do najważniejszych działów sztucznej inteligencji. Jest ona postrzegana jako dziedzina badań zmierzająca do wytworzenia programów komputerowych, które charakteryzuje inteligentne działanie. Systemy uczące się są bezpośrednio związane z dwoma innymi działami sztucznej inteligencji, tj.: automatycznym wnioskowaniem i przeszukiwaniem heurystycznym. Automatyczne wnioskowanie jest najstarszym nurtem sztucznej inteligencji i opiera się na osiągnięciach logiki formalnej. Dąży ono do uzyskania efektywnych algorytmów dedukcji. Przeszukiwanie dużych przestrzeni w efektywny sposób jest zagadnieniem będącym przedmiotem zainteresowania sztucznej inteligencji z powodu dwóch głównych zastosowań: rozwiązywanie problemów i gry planszowe [19, s. 50]. To właśnie automatyczne wnioskowanie jest tym kierunkiem rozwoju sztucznej inteligencji, które ma zastosowanie w przypadku rozwoju monitoringów wizyjnych, w tym monitoringów miejskich. Dotyczy to głównie elementów inteligentnej analizy obrazu połączonej z generowaniem alertów, w tym ograniczaniu występowania fałszywych

alarmów. Z drugiej strony uczenie maszynowe opierające się na wnioskowaniu może rozwijać możliwości pozwalające na przewidywanie określonych wydarzeń, zachowań. W tym przypadku uczenie się jest wynikiem zachodzenia dwóch procesów: wnioskowania, prowadzącego do generowania wiedzy oraz zapamiętywania, dzięki któremu nowa wiedza zostaje zapisana w pamięci systemu, zgodnie z przyjętą metodą reprezentacji [19, s. 53]. Metoda *deep learning* była wykorzystywana w aplikacji do analizy obrazu *Suspect Search,* pozwalająca między innymi w kilka sekund określić miejsce pobytu osoby będącej w zasięgu systemu monitoringu wizyjnego [18, s. 20]. Jednym z pierwszych zaawansowanych rozwiązań wykorzystywanych w monitoringach wizyjnych był system ANPR *(Automatic Number Plate Recognition*). System (początkowo funkcjonujący w Wielkiej Brytanii) rejestruje tablice rejestracyjne przejeżdżających pojazdów, kierowcę i pasażera, a następnie identyfikuje je automatycznie. Kiedy poszukiwany samochód zostaje zidentyfikowany, podnoszony jest alarm. Londyński system ANPR, rozbudowany w drugiej połowie lat 90., jest w stanie zanalizować do 5000 tablic w ciągu minuty. System powala na identyfikację numerów rejestracyjnych samochodu poruszającego się z prędkością 200 km/h i jest w 98% skuteczny [5, s. 49]. Jak wskazuje fundacja Panoptykon władze 21% polskich miast zadeklarowały, że ich systemy monitoringu są wyposażone w funkcje ANPR [9, s. 17].

Kolejnym rozwiązaniem, które jest wdrażane na szeroką skalę jest system identyfikacji VCA (*Video Content Analysis)* – analiza zawartości obrazu. Pozwala on ogólnie mówiąc na identyfikowanie „podejrzanych zachowań" [20, s. 29]. Podstawowymi funkcjami inteligentnej analizy obrazu są:

- wykrywanie sabotażu;
- inteligentne wykrywanie ruchu (podejrzane zachowanie);
- strefowa detekcja (alarm wywoływany jest wykryciem ruchu w określonej strefie);
- rozpoznawanie numerów tablic rejestracyjnych;
- liczenie osób;
- detekcja przekroczenia linii (np. przekroczenie linii bezpieczeństwa na peronie kolejowym);
- śledzenie obiektów;
- detekcja audio (przekroczenia określonego poziomu głośności);
- detekcja dymu i ognia;
- rozpoznawanie twarzy [21].

Funkcja VCA staje się bardzo popularną usługą z zakresu tworzenia i wykorzystania systemów CCTV. Świadczyć może o tym duża ilość ofert usługowych zamieszczonych

w sieci internetowej [22, 23]. Tego typu rozwiązanie wykorzystali twórcy Katowickiego Inteligentnego System Monitoringu i Analiz. Wraz z systemem monitoringu miejskiego w Zielonej Górze jest on uznawany za jeden z najnowocześniejszych w Polsce. O jego fenomenie decyduje wykorzystywanie specjalistycznego, zaawansowanego oprogramowania. System wykorzystuje następujące komponenty:

- system rozpoznawania numerów rejestracyjnych LPR (*Milestone*). System jest zainstalowany na 10 punktach drogowych zlokalizowanych na głównych trasach drogowych w Katowicach;
- system IBM IVA (*Intelligent Video Analytics*) – komponent zaawansowanych analityk wideo. W systemie KISMiA, na wybranych kamerach, zostały skonfigurowane analityki rozpoznające następujące sytuacje: leżący człowiek, pozostawiony obiekt, usunięty obiekt, zbiegowisko, przekroczenie strefy, włamanie do pojazdu, jazda pod prąd, parkowanie, kolizja pojazdów, pojawienie się zwierząt w strefie, dewastacja, zmiana położenia obiektu. Alarmy wygenerowane przez analityki są wyświetlane na ekranie operatora;
- aplikacja IBM IOC (*Intelligent Operations Center*) – system operacyjny pozwalający obsługiwać komponent IBM IVA. Dokonuje on weryfikacji danego alarmu pod względem prawdziwości, przekazanie zdarzenia zasygnalizowanego przez alarm do realizacji służbom, itp.

Zastosowane oprogramowanie pozwala na automatyczne dokumentowanie pracy operatorów systemu, poprzez:

- automatyczne generowanie raportów dotyczących, np. liczby alarmów, rodzaju alarmów itp.;
- automatyczne generowanie logów systemowych (m.in. logowania do systemu, czas obsługi danej kamery, czas i zakres eksportowanego materiału wideo, blokady materiału wideo);
- automatyczny rejestr interwencji podjętych przez daną służbę na podstawie zdarzeń z monitoringu.

Nowe możliwości systemów CCTV były między innymi przedmiotem badań i rozwoju w ramach projektu INDECT, tj. inteligentnego systemu informacyjnego wspierającego obserwację, wyszukiwanie i detekcję dla celów bezpieczeństwa obywateli w środowisku miejskim, (ang. *Intelligent information system supporting observation, searching and detection for security of citizens in urban environment*). Był to międzynarodowy projekt badawczy, mający na celu wykorzystanie innowacyjnych algorytmów i metod z zakresu informatyki do wykrywania i walki z terroryzmem oraz innymi

działaniami przestępczymi. Projekt finansowany był przez Unię Europejską. INDECT zakładał powstanie zestawu rozwiązań do inteligentnej obserwacji i automatycznego wykrywania podejrzanych zachowań lub przemocy w środowisku miejskim. Partnerami w realizacji projektu były polskie uczelnie, tj. Akademia Górniczo-Techniczna w Krakowie, Politechnika Gdańska oraz Politechnika Poznańska [24]. Prace nad tym projektem rozpoczęły się 1 stycznia 2009 r. Od początku miał on obejmować badania zwiększające bezpieczeństwo obywateli oraz zabezpieczenie zarejestrowanych i przechowywanych informacji. Dotyczyło to użycia innowacyjnych metod do wykrywania zagrożeń, tak w sferze rzeczywistej, poprzez wykorzystanie inteligentnych systemów monitoringu, jak i w sferze wirtualnej, tj. w sieciach komputerowych i internecie. W zakresie szczegółowych celów związanych z monitoringiem wizyjnym projekt INDECT zakładał stworzenie inteligentnego systemu przetwarzania informacji multimedialnych do automatycznego wykrywania zagrożeń i rozpoznawania działań przestępczych lub przemocy. Ponadto przewidywanym efektem projektu miało być stworzenie inteligentnej analizy danych wideo i audio w celu wykrywania zagrożeń w obszarze miejskim [25, s. 27]. W literaturze brak jest szczegółowych informacji dotyczących realizacji projektu INDECT. Brak jest informacji o efektach prac zespołu. Są natomiast uwagi wskazujące na obawy związane z funkcjonowaniem systemu INDECT. Szczególnie interesująca jest strona technologiczna. System nie tworzy nowych narzędzi nadzoru. Wykorzystuje istniejące systemy nadzoru wizyjnego, nowością nie mają być środki, a sposób ich wykorzystania. Wskazują również na opcjonalne wykorzystanie kamer prywatnych użytkowników, kamer w sklepach, na stacjach paliw itp., połączonych w jedną sieć. Wyjątkowo futurystycznie brzmi tworzenie w ramach projektu algorytmów pozwalających na bieżąco analizować obraz widziany przez kamery, wykrywając zachowania mające wskazywać na zamiar popełnienia przestępstwa [26]. Jak wskazano wcześniej, jest to element uczenia się maszynowego, opartego na wnioskowaniu. Jako przykład detekcji zachowania podawany jest przypadek pedofila, którego będzie można zidentyfikować na podstawie typowych dla tych przestępców zachowań. W przypadku identyfikacji takiego zachowania system powiadomi operatora lub inną osobę. Sama identyfikacja nie będzie pociągać skutków prawnych, a ostateczna decyzja w zakresie interpretacji i dalszych działań będzie należała do człowieka. Podobne procedury postępowania organów ścigania, opierające się na ujawnianiu zamiarów przestępczych znane są z filmu z gatunku *science-fiction,* pt. „Raport Mniejszości" [27]. Jednym z partnerów projektu było między innymi Ministerstwo Spraw Wewnętrznych, jednak w 2012 r. podjęto decyzje o wstrzymaniu współpracy Policji nad projektem INDECT.

Decyzję podjął minister po rozmowach z Komendantem Głównym Policji. Według niego Policja dysponuje środkami, które pozwalają zapobiegać zagrożeniom porządku publicznego [28]. Zdaniem naukowców z AGH podejrzliwość wobec INDECT zrodziła się na fali ówczesnego sprzeciwu wobec ACTA. System INDECT i ACTA nie miały ze sobą nic wspólnego, ale społeczeństwo było wyczulone na wszystko, co wiązało się z działalnością służb, w tym przede wszystkim, w intrenecie. Teza ta została poparta przez publicystów. D. Maciejasz stwierdziła, że najprawdopodobniej ministerstwo przestraszyło się fali protestów, do których w ostatnich tygodniach nawoływano w intrenecie, przyrównując INDECT do ACTA. Jednocześnie przytoczyła słowa posłanki B. Bubuli, która nazwała INDECT „orwellowskim system wielkiej inwigilacji" [29, s. 3]. W dyskusji nad decyzją MSW podnoszono lakoniczność komunikatu bez obszernego uzasadnienia [30]. Jednocześnie wskazywano, że zakupem systemu INDECT były zainteresowane zagraniczne podmioty, w tym m.in Europol, hiszpańskie ministerstwo obrony oraz policje: łotewska, rumuńska, maltańska, czeska [29, s. 3].

Innym projektem nawiązującym do doskonalenia analityk obrazu wideo był projekt COPCAMS, w którym brały udział uczelnie techniczne i instytuty badawcze z Francji, Hiszpanii, Turcji, Danii, Słowenii, Wielkiej Brytanii i Polski. W latach 2013–2016 uczestniczyło w nim 25 partnerów, w tym Politechnika Gdańska. Projekt był współfinansowany przez Narodowe Centrum Badań i Rozwoju oraz inicjatywę unijną ARTEMIS. Sama nazwa projektu COPCAMS (*Cognitive and Perceptive CAMeraS)* oznacza w polskiej wersji „Kamery umożliwiające kontekstowe rozumienie pozyskiwanego obrazu". Badania dotyczyły opracowania i przetestowania nowych inteligentnych rozwiązań dla kamer przemysłowych, systemu dozoru wizyjnego, diagnostyki wizyjnej na liniach produkcyjnych i innych dziedzin zastosowania analityki wizyjnej [31, s. 20]. Politechnika Gdańska w ramach projektu koordynowała realizację zadań w ramach pakietu „Zaawansowane koncepcje dla systemów kamer", który poświęcony był nowym metodom przetwarzania obszarów wideo i danych wielomodalnych, tj. pochodzących z dodatkowych czujników różnego typu oraz kompresji sygnałów wizyjnych i transmisji danych. Pierwszym innowacyjnym rozwiązaniem w tym zakresie było opracowanie radaru akustycznego zintegrowanego z kamerą obrotową. Jego zadaniem jest analizowanie na żywo danych o wektorowym gradiencie ciśnienia akustycznego, z których można pozyskać informacje o położeniu źródeł dźwięku w całej przestrzeni wokół kamery. W tym przypadku wykorzystanie odpowiedniego oprogramowania do detekcji i lokalizacji źródła dźwięków, istotnych z punktu widzenia bezpieczeństwa, jest w stanie wykryć i skierować obrotową kamerę w miejsce krzyku, wybuchu, wystrzału

czy tłuczonej szyby. Algorytm klasyfikacji źródeł został opracowany w oparciu o rzeczywiste nagrania i rozróżnia przykładowe ich klasy. Nie reaguje przez to na dźwięki typowe, np. hałas uliczny i rozmowy. Liczba zdarzeń, na które ma reagować kamera jest nieograniczona, a o ich skali i rodzajach decyduje operator (może ustawić system na źródło najbliższe, najgłośniejsze, czy wyższy priorytet ma mieć krzyk, wybijana szyba, czy też wystrzał). Kolejnym rozwiązaniem zaproponowanym przez uczonych Politechniki Gdańskiej było opracowanie kierunkowej anteny wielosektorowej do wykrywania i lokalizacji aktywnych znaczników radiowych wykonanych w technologii RFID. Znaczniki takie wykorzystywane są do ochrony towarów w sklepach i są aktywowane w momencie przechodzenia przez wąskie bramki stanowiące anteny nadawczo-odbiorcze. Standardowo znaczniki działają w wersji pasywnej (bez wbudowanej baterii). Naukowcy wykorzystali wersję aktywną znacznika i antenę kierunkową, umożliwiającą ciągłe monitorowanie obecności i lokalizowanie chronionego przedmiotu. Uczestnicy projektu wskazali, że szczególnie interesujące i potrzebne jest usprawnienie metod wykrywania ruchu i śledzenia obiektów. W wykorzystywanych obecnie „inteligentnych" systemach, urządzeniach wyposażonych w mało wydajne procesory, zbyt często dochodzi do generowania fałszywych alarmów, np. falowanie liści, wody, odbicia. Podstawową operacją wykonywaną na każdym pikselu obrazu jest modelowanie tła w taki sposób, aby adaptować się do:

- powolnych zmian w obrazie, np. zachmurzenie zmieniające jasność i kolorystykę całego kadru nie może być interpretowane jako ruch;
- szybkich cyklicznych zmian w obrazie, np. ruch listowia powodujący naprzemienne zmiany z koloru zielonego (liście) na niebieski (niebo), gdzie powinno to być interpretowane jako tło obrazu, a nie ruch.

Tym samym konieczne jest stosowanie wysokowydajnych procesorów mogących dokonać stosownych obliczeń[1]. Ciekawie i obiecująco przedstawiały się wyniki badań pozostałych partnerów projektu COPCAMS. Jako przykłady prac naukowych mogących mieć zastosowanie w realizacji zadań związanych z bezpieczeństwem i porządkiem publicznym, można podać:

- połączenie możliwości monitorowania akustycznego i radiowego z wizyjnym w celu poprawy możliwości skutecznego oraz precyzyjnego wykrywania i śledzenia zdarzeń;

1 Dla klatki wideo o rozmiarze 1 Mpix konieczne jest obliczanie i aktualizowanie 24 razy na sekundę miliona pikseli w module tła. Źródło: [31].

- rozwinięcie metod współpracy między algorytmami sterującymi kamer szerokokątnych i kamer obrotowych w celu nadzoru rozległego terenu;
- usprawnienie metod poprawy czytelności obrazu w przypadku zamglenia i niedoświetlenia.

W krajach Unii Europejskiej inteligentna inwigilacja prawdopodobnie przybierze masową skalę, gdyż Komisja Europejska przeznaczyła w 2004 r. ponad 60 mln euro na wstępne badania, których owocem ma być system zwany ISCA PS (*Integrated Surveillance of Crowded Areas for Public Safety* – zintegrowany system obserwacji miejsc publicznych w celu zapewnienia bezpieczeństwa). Ma on sięgać po wszystkie nowe narzędzia inteligentnej inwigilacji, m.in. technikę elektronicznego podsłuchu rozmów za pomocą automatycznego czytania z ruchu warg, nad której rozwojem pracują naukowcy z brytyjskiego Surrey University [25, s. 25–26].

Jak wskazują specjaliści, w 2017 r. jedną z głównych płaszczyzn zainteresowania w przypadku telewizji dozorowej stała się cyberprzestępczość. Wiązało się to z atakiem DDoS, który miał miejsce na początku 2016 r. Pojęcie DDoS pochodzi od angielskiego określenia *distributed denial of service,* co można przetłumaczyć jako rozproszona odmowa dostępu. To jedna z wielu metod wykorzystywanych do blokowania internetowych serwisów lub blokowania łączy internetowych. Istnieją dwa podstawowe rodzaje ataków DDoS, tj.:

- atak wolumetryczny – polegający na masowej wysyłce niechcianych danych na wskazany adres IP, co w konsekwencji powoduje zablokowanie lub spowolnienie łącza internetowego;
- atak aplikacyjny – polegający na wyczerpaniu zasobów informatycznych aplikacji internetowej, np. mocy obliczeniowej lub pamięci [32].

Atak DDoS w 2016 r. na amerykańską spółkę zarządzającą serwerami spowodował m.in. wstrzymanie usług serwisów Amazon i Netflix. Podczas tego ataku, jako zdalnie sterowanych „napastników" zwanych botami, wykorzystano kilka kamer sieciowych i rejestratorów systemów, zainfekowanych przez malware Miari. Ten incydent ponownie zasygnalizował potrzebę właściwego zabezpieczania urządzeń i systemów IP.

Innym kierunkiem rozwoju technologii monitoringu wizyjnego jest wykorzystanie do tego celu bezzałogowych statków powietrznych, tzw. dronów. Bezzałogowe statki powietrzne to automatyczne urządzenia latające, posiadające własny napęd, mogące samodzielnie latać w powietrzu. Mogą być również zdalnie sterowane, a w zależności od wyposażenia pełnią różne zadania [33, s. 119]. Zasady użytkowania dronów w pewnym zakresie regulują przepisy ustawy z 3 lipca 2002 r. *Prawo lotnicze* [34]. Pomijając

kwestie użytkowania dronów w przestrzeni powietrznej i związane z tym zagrożenia w ruchu lotniczym, mogą być one wykorzystywane jako platformy przenoszące kamery. Tym samym mogą być przydatne do realizacji zadań, które były dotychczas trudne, a w niektórych przypadkach niebezpieczne do wykonania lub kosztowne. Do takich zadań zaliczyć można: reagowanie na klęski żywiołowe, kontrolowanie granic, kontrolowanie demonstracji, zwalczanie przestępczości. W Polsce dronami, poza Siłami Zbrojnymi, dysponują Policja oraz straż pożarna. Są również powszechnie wykorzystywane przez prywatne osoby. W Polsce jest obecnie około 100 tys. właścicieli dronów – tylko dziewięć razy mniej niż użytkowników w Stanach Zjednoczonych, co plasuje nas w ścisłej światowej czołówce. W 2015 r. przychody ze sprzedaży bezzałogowych statków powietrznych wyniosły 164 mln zł, rok później przekroczyły 200 mln zł, a przed rokiem osiągnęły ćwierć miliarda złotych [35, s. 8]. Drony wzbudzają spore kontrowersje głównie z powodu niespotykanej na dużą skalę ingerencji w prywatność. Mogą one być wykorzystywane do śledzenia ludzi i pojazdów oraz obserwowania przestrzeni prywatnej. Taki monitoring może być realizowany w sposób właściwie niezauważalny dla osób obserwowanych.

W kontekście przyszłości systemów CCTV, ciekawą opinię przedstawia U. Segall – dyrektor ds. rozwoju biznesu w izraelskiej firmie Qognify. Odnosi się on do wykorzystania postów i filmów publikowanych z urządzeń użytkowników w mediach społecznościowych. Jak wskazuje, niektóre technologie umożliwiają zbieranie postów z mediów społecznościowych i scalanie tych danych. Ilość danych powiązana z możliwością lokalizacji użytkownika oraz czasu rejestracji może mieć znaczenie w odniesieniu do ochrony osób i mienia. Tym samym uważa on, że najlepszym obiektywem i najbardziej inteligentną „czujką" jest wciąż człowiek. Wykorzystując smartfony (wyposażone w lokalizator GPS, zaawansowane systemy video oraz narzędzia do komunikacji), użytkownicy są w stanie rejestrować i przekazywać dużą ilość danych przydatnych ze względu na bezpieczeństwo i porządek [18, s. 18].

Podsumowanie

Systemy monitoringów wizyjnych są obecnie powszechnie wykorzystywane jako narzędzia służące zapewnieniu bezpieczeństwa i porządku publicznego. Jednym z warunków skutecznego funkcjonowania systemów CCTV jest dostosowanie do obowiązujących międzynarodowych norm technicznych regulujących ich budowę i eksploatację. Obowiązująca norma PN-EN 62676-1-1 szczegółowo przedstawia wymagania w obszarze

skutecznej i bezpiecznej eksploatacji systemów monitoringu wizyjnego. Norma odnosi się do systemów wykorzystujących nowoczesne aplikacje do analizy obrazu, opierające się na generowaniu alertów. Dużą wagę przywiązuje ona do zabezpieczenia zapisów wizyjnych, tak pod względem informatycznym, jak i fizycznym. Ma to istotne znaczenie w kontekście wykorzystania materiałów przez organy ścigania i wymiar sprawiedliwości. Budowa i wykorzystanie systemów monitoringu wizyjnego w oparciu o obowiązujące normy daje częściowo gwarancję skutecznego i bezpiecznego działania. W oparciu o europejskie normy techniczne tworzono między innymi Katowicki Inteligentny System Monitoringu i Analiz.

Rozwój technologiczny daje systemom monitoringu wizyjnego możliwości, które pozostawały dotychczas w sferze wyobrażeń twórców filmów fantastycznych. Możliwości te wynikają głównie z dynamicznego rozwoju branży informatycznej. Budowane obecnie systemy wykorzystują już narzędzia pozwalające na „inteligentną" obserwację obszaru monitorowanego. Opierają się one na analizie wizyjnej i akustycznej obserwowanej rzeczywistości. Generują alerty w przypadku zarejestrowania anomalii, automatycznie analizują rejestrowany obraz, autonomicznie reagują na zdarzenia. Wszystkie te udogodnienia wspomagają lub wręcz wyręczają operatorów systemu z bieżącej analizy rejestrowanego obrazu. W dalszym ciągu jednak to człowiek ostatecznie interpretuje znaczenie rejestrowanego obrazu i podejmuje dalsze decyzje.

Podkreślić należy, że „inteligentne" systemy nie są pozbawione wad. Jednym z problemów jest generowanie „fałszywych alertów". Alarmy mogą być wywoływane przez nieznaczące zmiany w obserwowanej rzeczywistość (np. liście drzew poruszane wiatrem, refleksy świetlne). Z tego powodu jednym z kierunków rozwoju oprogramowania sterującego systemami monitoringów wizyjnych jest praca nad maszynowym uczeniem się, stanowiącym jeden z najważniejszych działów sztucznej inteligencji. Pozwoli to automatycznie i właściwie interpretować rejestrowany obraz.

Praca nad sztuczną inteligencją wspomagającą pracę monitoringów wizyjnych jest jednym z głównych kierunków rozwoju technologicznego. Inne kierunki dotyczą możliwości wykorzystania różnego rodzaju kamer obserwujących rzeczywistość. Koncepcja dotyczy możliwości dostępu do wszystkich klasycznych punktów kamerowych, jak również kamer zainstalowanych w smartfonach, obsługiwanych przez prywatnych użytkowników czy kamer zainstalowanych na dronach. Znamienny jest fakt, iż rozwój technologii nie jest determinowany wyłącznie możliwością wykorzystania przez podmioty publiczne (np. na rzecz bezpieczeństwa i porządku publicznego). Istotne znaczenie ma również presja sektora prywatnego. Przykładem może być branża reklamowa, gdzie

systemy wizyjne potrafią samodzielnie rozpoznawać płeć czy wiek osoby i dzięki temu właściwie dobierać treść reklamy. Zapotrzebowanie sektora publicznego, jak i prywatnego daje tym samym gwarancję kontynuowania prac nad rozwojem systemów CCTV.

Bibliografia

[1] Spencer A.R, *Psychologia współczesna*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2004.

[2] Wiśniewski B., *Bezpieczeństwo wewnętrzne państwa – pojęcie, istota, system, konteksty* [w] *Od nauk wojskowych do nauk o bezpieczeństwie,* B. Wiśniewski (red.), Wyższa Szkoła Policji w Szczytnie, Szczytno 2014

[3] Wiśniewski B., *System bezpieczeństwa państwa. Konteksty teoretyczne i praktyczne.* Wyższa Szkoła Policji w Szczytnie, Szczytno 2013.

[4] Wróblewski M., *Podstawy prawne funkcjonowania monitoringu wizyjnego w Polsce,* „Monitor Prawny" 2013, nr 8.

[5] Waszkiewicz P., *Wielki Brat Rok 2010. System monitoringu wizyjnego – aspekty kryminalistyczne, kryminologiczne i prawne,* Wolters Kluwer, Warszawa 2011.

[6] www.PreciseSecurity.com (dostęp: 15.01.2020 r.).

[7] Informacja o wynikach kontroli Najwyższej Izby Kontroli *Funkcjonowanie miejskiego monitoringu wizyjnego,* https://www.nik.gov.pl/plik/id.6400.vp.8169.pdf (dostęp: 14.11.2019).

[8] M. Szumańska, *Życie wśród kamer. Przewodnik,* Fundacja Panoptykon. http://zycie – wśród – kamer. panoptykon. org/ (dostęp: 06.11.2019 r.).

[9] Krassowski K., *Monitoring wizyjny z punktu widzenia kryminalistyki* [w:] *Prawo Kryminalistyka Policja. Księga pamiątkowa ofiarowana prof. B. Młodziejowskiemu,* (red.) J. Kasprzak, J. Bryk, Wyższa Szkoła Policji w Szczytnie, Szczytno 2008.

[10] Dunaj B., Słownik współczesnego języka polskiego, Przegląd Reader's Digest, Warszawa 2001.

[11] Kałużny P., *Telewizyjne systemy dozorowe,* Wydawnictwa Komunikacji i Łączności, Warszawa 2008.

[12] Ordysińska M., *Aspekty prawne funkcjonowania systemów monitoringu wizyjnego w Polsce. Cz. I.,* „Systemy Alarmowe" 2006, nr 4

[13] Wittich P., *Instalacja kamer to za mało, żeby zbudować skuteczny system monitoringu wizyjnego,* „Kwartalnik Policyjny" 2016, nr 1 (36).

[14] http://www.sa-portal.pl/nowosci/samsung-techwin-i-mr-system-sponsorami-projektu-polskiej-normy – prpn-en-50132-72012/ (dostęp: 10.12.2019).

[15] Norma PN-EN 62676-1-1 dostępnej https://czytelnia.pkn.pl/#/reading-room/PN – EN%2062676-1-1:2014-06E/~/PN-EN%2062676-1-1_2014-06E_ KOLOR.pdf/1 (dostęp: 04.11.2019 r.).
[16] Szachnitowski Z., *„Systemy dozorowe CCTV i ich przydatność dowodowo-wykrywcza,* „Ochrona mienia i informacji. Projekty, instalacje, zarządzanie" 2014, nr 2.
[17] Ustawa z 12 września 2002 r. *o normalizacji* (t.j. Dz.U. z 2015 r . poz. 1483).
[18] Pao W., *Telewizja dozorowa. Światowe trendy 2017*, „A&S Polska" 2017, nr 2.
[19] Cichosz P., *Systemy uczące się,* Wydawnictwa Naukowo-Techniczne, Warszawa 2007.
[20] Mroczek A., *Rejestracja obrazu w miejscach publicznych,* „Ochrona Mienia i Informacji" 2013, nr 3.
[21] VCA-inteligentna analiza obrazu. http://www.tvprzemyslowa.pl/vca-inteligentna--analiza-obrazu-3/ (dostęp: 17.12.2019 r.).
[22] http://www.wimax.pl/inteligentna_analiza_wideo-s121.html (dostęp: 17.12.2019 r.).
[23] http://www.ismeurocenter.com/ismeurocenter.pl/produkty/cctv/vca-analiza--zawartoci-obrazu (dostęp: 17.12.2019 r.).
[24] http://www.kt.agh.edu.pl/pl/projekt/281 (dostęp: 12.12.2019 r.).
[25] Wróbel J., Podsiedlik P., *Monitoring wizyjny cz. I. Geneza i czasy współczesne.* Materiały Dydaktyczne nr 37, Szkoła Policji w Katowicach, Katowice 2016.
[26] Michalik Ł., *Projekt INDECT – AGH tworzy narzędzie masowej inwigilacji ?* http://www. gadzetomania. pl/6611,projekt-indect-agh-tworzy-narzedzie-masowej--inwigilacji#comments (dostęp: 12.12.2019 r.).
[27] Spilberg S. (reż.) , *The Minority Report*, 20th Century Fox (dystr.), 2002.
[28] Komunikat w sprawie systemu INDECT z 13 kwietnia 2012 r. www.mswia.gov.pl/pl/aktualności /9729,dok.html (dostęp: 12.12.2019 r.).
[29] Maciejasz D., *AGH już dziękujemy,* „Gazeta Wyborcza" 2012, nr 88.
[30] Wasilewska – Śpioch A., *MWS wycofuje się z projektu INDECT*, 14.04.2012, http://www://di.com.pl/msw-wycofuje-sie-z-projektu-indect-44743#dalej (dostęp: 12.12.2019 r.).
[31] Szczuko P., *Nie tylko kamery. Tematyka i wyniki badań projektu COPCAMS,* „A&S Polska" 2017, nr 2.
[32] *Co to jest atak DDos i jak się przed nim chronić*? https://dataspace.pl/assets/ddos_broszura_web.pdf (dostęp: 06.12.2019 r.)
[33] Lis S., *Bezpieczeństwo a bezzałogowe statki powietrzne (drony) w działaniach militarno-wojskowych i w służbie cywilnej* [w:] *Bezpieczeństwo w kontekście zglo-*

balizowanego świata (red.) P. Maciaszczyk, Państwowa Wyższa Szkoła Zawodowa im. prof. Stanisława Tarnowskiego w Tarnobrzegu, Tarnobrzeg 2017.
[34] Ustawa z 3 lipca 2002 r. *Prawo lotnicze* (Dz.U z 2018 r. poz.1183, 1629, 1637).
[35] Wojciechowski K., *Oblatani w dronach,* „Dziennik Gazeta Prawna" 2018, nr 155.

dr Grzegorz Matuszek – absolwent Wyższej Szkoły Policji w Szczytnie. Doktor nauk społecznych w dyscyplinie nauk o bezpieczeństwie. Pracownik dydaktyczny Akademii WSB w Dąbrowie Górniczej. Pierwszy Zastępca Komendanta Powiatowego Policji w Wodzisławiu Śląskim.

Grzegorz Matuszek – he graduate from the Police Academy in Szczytno. Doctor of social sciences in the discipline of security science. Teaching employee at the WSB Academy in Dąbrowa Górnicza. First Deputy Commander of the Poviat Police in Wodzisław Śląski.