JAK SKUTECZNIE ZABEZPIECZYĆ OBIEKT PRZED KRADZIEŻĄ ZA POMOCĄ SZTUCZNEJ INTELIGENCJI?

ANALIZA I PRAKTYCZNE WSKAZÓWKI OD EKSPERTA MARCINA NIEDOPYTALSKIEGO

OCHRONA OSÓB I MIENIA

12 MARCA 2000

CYBER SECURITY
GRUPA SZYBKIEGO REAGOWANIA ŚLĄSK

Spis treści

MOST WIEDZY Downloaded from mostwiedzy.pl

Autor: Marcin Niedopytalski ekspert ds. ochrony osób i mienia

W dobie rosnących zagrożeń, jakie stawiają przed społeczeństwami zorganizowane grupy przestępcze, terroryzm czy wzrastająca liczba przestępstw ulicznych, nowoczesne technologie stają się kluczowym elementem w walce z przestępczością. Systemy monitoringu wizyjnego, wsparte przez sztuczną inteligencję (AI), przechodzą transformację, od prostych rejestratorów obrazu do zaawansowanych narzędzi analitycznych zdolnych do detekcji zagrożeń i prewencji przestępstw w czasie rzeczywistym. W niniejszej pracy dokonamy analizy roli sztucznej inteligencji w nowoczesnych systemach monitoringu wizyjnego, ukazując jej potencjał, wyzwania oraz zastosowania praktyczne. Pierwsze systemy monitoringu wizyjnego powstały w latach 60. XX wieku jako narzędzie do nadzoru przemysłowego i wojskowego. Były to proste systemy CCTV (Closed-Circuit Television), które wymagały stałego nadzoru przez operatora. Z czasem, wraz z rozwojem technologii cyfrowych, systemy te zyskały możliwość nagrywania i archiwizacji danych, co zwiększyło ich skuteczność. Wprowadzenie algorytmów komputerowych w latach 90. umożliwiło automatyczną analizę obrazu, jednak prawdziwą rewolucję przyniósł rozwój sztucznej inteligencji w XXI wieku. Dzięki uczeniu maszynowemu (ML) i sieciom neuronowym systemy monitoringu zyskały zdolność do rozpoznawania obiektów, analizowania zachowań oraz przewidywania zagrożeń. Pozwolę sobie w tym miejscu przedstawić kilka informacji o sobie, aby uwiarygodnić zawarte w artykule treści. Od lat zajmuję się ochroną osób i mienia – początkowo w ramach dużych firm ochroniarskich, gdzie zdobywałem doświadczenie zarówno w zakresie fizycznej ochrony obiektów, jak i projektowania systemów bezpieczeństwa. Ukończyłem liczne kursy i szkolenia specjalistyczne, w tym z zakresu wdrażania rozwiązań AI w obiektach handlowych oraz kontroli dostępu w instytucjach użyteczności publicznej. Dziś prowadzę własną działalność konsultingową. Współpracuję zarówno z sieciami handlowymi o zasięgu ogólnopolskim, jak i z mniejszymi podmiotami, oferując im audyty bezpieczeństwa, rekomendacje technologiczne, szkolenia dla personelu i wsparcie we wdrażaniu procedur antypandemicznych oraz antykryzysowych. Dlaczego zdecydowałem się na specjalizację w tej dziedzinie? Głęboko wierzę, że bezpieczeństwo jest fundamentem funkcjonowania każdego biznesu. Jeżeli pracownicy czują się pewnie w miejscu pracy, a klienci mają świadomość, że sklep jest dobrze zorganizowany i skutecznie chroniony, obie strony są bardziej zadowolone. To przekłada się na lepsze relacje i zaufanie do marki. Staram się łączyć nowoczesne technologie z pragmatycznym podejściem do codziennych problemów. Wiem, że niektóre sklepy, zwłaszcza mniejsze, nie mogą pozwolić sobie na najdroższe rozwiązania AI. Dlatego zawsze poszukuję sposobów na optymalne wykorzystanie środków czasem wystarczą drobne zmiany w układzie sklepu, poprawa oświetlenia i kilka kamer z prostą analityką, by radykalnie ograniczyć liczbę kradzieży.

Funkcje nowoczesnych systemów monitoringu wspieranych AI

Rozpoznawanie twarzy

Rozpoznawanie twarzy jest jednym z najbardziej zaawansowanych zastosowań sztucznej inteligencji w monitoringu wizyjnym. Systemy te wykorzystują algorytmy analizy biometrów twarzy, pozwalając na identyfikację osób w tłumie. Funkcja ta znajduje zastosowanie w lotniskach, stadionach czy przestrzeniach publicznych, gdzie detekcja osób poszukiwanych przez policję może odbywać się w czasie rzeczywistym.

MOST WIEDZY Downloaded from mostwiedzy.pl

Analiza zachowań

Systemy oparte na AI są w stanie analizować wzorce zachowań ludzi i wykrywać potencjalnie niebezpieczne sytuacje, takie jak bójki, bieganie w miejscach publicznych czy pozostawienie podejrzanych przedmiotów. Algorytmy te uczą się na podstawie milionów danych wideo, co pozwala im na szybkie rozpoznanie nietypowych wzorców ruchu.

Detekcja obiektów

Systemy AI potrafią wykrywać konkretne obiekty, takie jak broń, noże czy pojazdy. Dzięki tej funkcji możliwa jest szybka reakcja w przypadku potencjalnego zagrożenia, np. w szkołach czy centrach handlowych.

Predykcja zagrożeń

Jednym z najnowszych osiągnięć AI jest zdolność do przewidywania zagrożeń na podstawie analizy zachowań. Przykładowo, systemy monitoringu mogą identyfikować osoby, które zachowują się podejrzanie, np. dłuższy czas spędzają w jednym miejscu, obserwując otoczenie.

Zalety AI w monitoringu wizyjnym

Skuteczność i szybkość

Tradycyjne systemy monitoringu opierały się na pracy operatorów, co powodowało ograniczenia w wykrywaniu zagrożeń. AI eliminuje ten problem, pozwalając na ciągłą analizę obrazu w czasie rzeczywistym, bez konieczności angażowania ludzi.

Redukcja liczby fałszywych alarmów

Dzięki zaawansowanym algorytmom AI jest w stanie odfiltrować błędne detekcje, np. gdy system wykrywa ruch spowodowany przez zwierzęta czy warunki atmosferyczne. Zmniejsza to liczbę fałszywych alarmów, co oszczędza czas i zasoby.

Skalowalność

Nowoczesne systemy monitoringu mogą być łatwo skalowane, co oznacza, że mogą obsługiwać od pojedynczych kamer w małych sklepach po tysiące urządzeń w dużych aglomeracjach miejskich.

Wyzwania w zastosowaniu AI w monitoringu wizyjnym

Prywatność i etyka

Jednym z największych wyzwań jest ochrona prywatności obywateli. Systemy rozpoznawania twarzy i analizy zachowań mogą być wykorzystywane do inwigilacji, co budzi obawy o nadużycia ze strony rządów czy korporacji.

Błędy algorytmów

Chociaż AI jest niezwykle skuteczna, nie jest pozbawiona wad. Błędy w rozpoznawaniu twarzy czy obiektów mogą prowadzić do fałszywych oskarżeń, co może mieć poważne konsekwencje prawne i społeczne.

MOST WIEDZY Downloaded from mostwiedzy.pl

Koszty wdrożenia

Zaawansowane systemy AI są kosztowne w implementacji i utrzymaniu, co może być barierą dla mniejszych instytucji czy państw rozwijających się.

Przyszłość systemów monitoringu wizyjnego

Integracja z innymi technologiami

W przyszłości systemy monitoringu będą łączyć się z innymi technologiami, takimi jak Internet Rzeczy (IoT) czy blockchain, co zapewni wyższy poziom bezpieczeństwa danych i lepsze zarządzanie zasobami.

Zastosowanie w miastach inteligentnych

AI w monitoringu wizyjnym będzie odgrywać kluczową rolę w inteligentnych miastach, pomagając w zarządzaniu ruchem, monitorowaniu przestrzeni publicznych czy reagowaniu na sytuacje awaryjne.

Rozwój algorytmów predykcyjnych

Algorytmy AI będą coraz lepsze w przewidywaniu zagrożeń, co umożliwi skuteczniejszą prewencję przestępstw. Możliwe będzie np. zapobieganie atakom terrorystycznym na podstawie analizy danych z wielu źródeł.

Zastosowania praktyczne

Ochrona przestrzeni publicznych

Systemy monitoringu wizyjnego wspierane AI są już stosowane w takich miejscach jak lotniska, dworce czy centra handlowe. Dzięki zdolności do wykrywania niebezpiecznych przedmiotów i analizowania zachowań pasażerów, znacząco poprawiają poziom bezpieczeństwa.

Zarządzanie ruchem drogowym

W miastach takich jak Singapur czy Dubaj systemy monitoringu z AI służą do monitorowania ruchu drogowego i zarządzania sygnalizacją świetlną w czasie rzeczywistym. Redukuje to korki i poprawia bezpieczeństwo na drogach.

Ochrona obiektów krytycznych

Zakłady przemysłowe, elektrownie czy bazy wojskowe wykorzystują zaawansowane systemy monitoringu, aby wykrywać zagrożenia, takie jak nieuprawnione wejście na teren chroniony czy pojawienie się obiektów potencjalnie niebezpiecznych. Sztuczna inteligencja w systemach monitoringu wizyjnego stanowi jeden z najważniejszych elementów współczesnych strategii bezpieczeństwa. Dzięki zdolności do analizy danych w czasie rzeczywistym, przewidywania zagrożeń i redukcji liczby fałszywych alarmów, systemy te znacząco poprawiają skuteczność ochrony. Jednocześnie, konieczne jest podejmowanie działań na rzecz ochrony prywatności i etycznego wykorzystania tych technologii. Przyszłość monitoringu wizyjnego z AI zapowiada się obiecująco, a jego dalszy rozwój może zrewolucjonizować sposób, w jaki zapewniamy bezpieczeństwo społecznościom na całym

MOST WIEDZY Downloaded from mostwiedzy.pl

świecie. Kradzież w obiektach handlowych, zwłaszcza w supermarketach i marketach o niskich półkach, stanowi poważne wyzwanie dla branży ochrony. Z jednej strony mamy potrzeby klientów, którzy oczekują wygodnych zakupów oraz szybkiej i sprawnej obsługi. Z drugiej konieczność zabezpieczenia towaru i minimalizowania strat powodowanych przez osoby kradnące. W dobie nowoczesnych technologii coraz częściej słyszy się o wdrażaniu rozwiązań opartych o sztuczną inteligencję (AI), które potrafią nie tylko rozpoznać potencjalne zagrożenia, ale także przewidywać je zanim dojdzie do straty. Nazywam się Marcin Niedopytalski i od wielu lat zajmuję się profesjonalnym doradztwem w zakresie ochrony osób i mienia. Moim celem jest pomaganie przedsiębiorcom w tworzeniu skutecznych strategii przeciwdziałania kradzieżom, a tym samym zapewnienie bezpieczeństwa personelowi, klientom oraz mieniu firmy. W niniejszym artykule przedstawię kompleksowe podejście do tematu zapobiegania kradzieżom w obiektach handlowych z wykorzystaniem najnowszych technologii oraz sprawdzonych metod organizacyjnych. Przyjrzymy się również temu, co jest najczęściej kradzione, jak postępują złodzieje oraz jakie działania należy podjąć, by te przestępstwa skutecznie zminimalizować.

1. Rola sztucznej inteligencji w monitoringu i zapobieganiu kradzieżom

1.1. Zasada działania systemów AI

Sztuczna inteligencja w kontekście ochrony obiektów handlowych to przede wszystkim zaawansowane algorytmy, które są w stanie rozpoznawać wzorce ludzkiego zachowania i anomalie w czasie rzeczywistym. Nowoczesne systemy wizyjne oparte na AI wykorzystują kamery CCTV (Closed Circuit Television), analizują obraz klatka po klatce i wychwytują niestandardowe ruchy, gesty czy sekwencje zachowań potencjalnie wskazujące na próbę kradzieży. Na podstawie danych historycznych i wyuczonych schematów (np. poruszanie się po sklepie, sięganie po produkty w nietypowy sposób, chowanie ich do kieszeni, torby czy wózka itp.) system jest w stanie rozpoznać, że istnieje wysokie prawdopodobieństwo wystąpienia kradzieży. Następnie odpowiednie alerty są wysyłane do pracowników ochrony lub managera sklepu.

1.2. Automatyczne powiadamianie personelu

Zaletą rozwiązań AI w systemach bezpieczeństwa jest możliwość natychmiastowej reakcji. O ile „klasyczny” monitoring wymaga ciągłego wpatrywania się w wiele ekranów, co jest bardzo trudne i nierzadko mniej skuteczne, o tyle sztuczna inteligencja ułatwia wychwycenie incydentu. Algorytmy przejmują na siebie odpowiedzialność za selekcję zdarzeń podejrzanych. Ochroniarz, który otrzymuje powiadomienie np. na tablet, telefon czy monitor główny, może od razu skierować uwagę na odpowiednie miejsce i zapobiec potencjalnej kradzieży.

1.3. Analiza zachowań i profilowanie sprawców

Systemy AI umożliwiają także tzw. analizę behawioralną. Algorytm gromadzi informacje na temat częstotliwości pojawiania się określonych osób w sklepie, ich trasy poruszania, tego, przy jakich półkach najczęściej przebywają. Na podstawie zebranych danych można zauważyć schematy: np. osoba regularnie wychodząca ze sklepu bez dokonywania zakupu, za to każdorazowo zbliżająca się do działu z droższymi artykułami. Równie istotne jest tzw. profilowanie sprawców. Sztuczna inteligencja uczy się, jakie gesty lub zachowania

MOST WIEDZY Downloaded from mostwiedzy.pl

poprzedzają kradzież. Nie chodzi tu jednak o stereotypowe ocenianie wyglądu klienta (to byłoby dyskryminujące i nieetyczne), lecz o realne zachowania, takie jak ciągłe rozglądanie się, długie przebywanie w jednym miejscu sklepu bez wyraźnego zainteresowania konkretnymi produktami, nerwowe ruchy czy próby „ukrywania" ciała między regałami.

2. Zapobieganie kradzieżom w supermarketach i marketach z niskimi półkami

2.1. Specyfika niskich półek

Sklepy z tzw. niskimi półkami są wyjątkowo narażone na kradzieże. Dlaczego? Ponieważ dostęp do produktów bywa bardzo łatwy – często wystarczy przegiąć się lekko nad półką i dyskretnie schować towar. Dodatkowo, w niektórych marketach jest ograniczona liczba personelu, co stanowi dodatkową zachętę dla potencjalnych złodziei.

Niskie półki sprzyjają zjawisku tzw. „kradzieży drobnych", kiedy to klienci zabierają małe produkty, takie jak słodycze, kosmetyki w małych opakowaniach, drobna elektronika czy baterie. Z pozoru niewielka strata dla sklepu, ale przy dużej skali problemu koszty rosną lawinowo.

2.2. Optymalny układ sklepu

Aby przeciwdziałać kradzieżom w marketach z niskimi półkami, kluczowe jest właściwe zaprojektowanie przestrzeni sprzedaży:

Odpowiednie rozmieszczenie towaru – droższe produkty lub najbardziej narażone na kradzież powinny znajdować się w bardziej widocznych miejscach, najlepiej w zasięgu wzroku pracowników.

Unikanie „martwych stref" – obszary, w których brak jest kamer lub gdzie personel ma ograniczoną widoczność, to idealne miejsce dla złodzieja. Nowoczesne systemy AI mogą wspierać ten proces, wskazując miejsca niedostatecznie monitorowane.

Dobra komunikacja wzrokowa – zapewnienie jasnego, dobrze oświetlonego wnętrza, w którym klienci widzą się wzajemnie, a personel może szybko dostrzec podejrzane zachowanie.

2.3. Szkolenie personelu i właściwa postawa sprzedawców

Nawet najlepsze systemy elektroniczne nie zastąpią świadomego i dobrze wyszkolonego personelu. Dlatego: *Szkolenia w zakresie rozpoznawania podejrzanego zachowania* – pracownicy powinni wiedzieć, na co zwracać uwagę w kontekście osób kręcących się po sklepie bez wyraźnego celu. *Wiedza o najnowszych metodach kradzieży* – z roku na rok złodzieje stają się coraz bardziej kreatywni. Personel musi znać najczęstsze schematy przestępców, np. zmiana metek z cenami, włożenie droższego towaru w opakowanie tańszego, wprowadzanie w błąd kasjera itp. *Kultura asertywnej obsługi* – niewerbalne sygnały, np. uśmiech czy przyjazne podejście, ale też dyskretne zaznaczenie, że „widzimy każdego klienta", potrafią zniechęcić do kradzieży.

MOST WIEDZY Downloaded from mostwiedzy.pl

3. Co najczęściej jest kradzione i dlaczego?

3.1. Produkty drobne, o wysokiej wartości jednostkowej

Na pierwszym miejscu zazwyczaj plasują się przedmioty niewielkie, jednak o dużej wartości. Mogą to być: Drogeria i kosmetyki: perfumy, drogie kremy, a także popularne, małe kosmetyki (np. tusze do rzęs). Elektronika użytkowa: słuchawki, karty pamięci, pendrive'y, ładowarki, małe głośniki Bluetooth. Markowe słodycze, kawa, alkohol: te produkty mają stosunkowo wysoką cenę, a jednocześnie można je łatwo schować.

3.2. Artykuły spożywcze często „dla zasady"

Niekiedy ludzie decydują się na kradzież tańszych produktów spożywczych, motywując to ciekawością albo fałszywym przekonaniem, że to niewielka strata dla sklepu (np. batonik, gumy do żucia, napoje). Często jest to tzw. kradzież „z potrzeby chwili" lub z braku środków na większe zakupy.

3.3. Odzież i akcesoria modowe

Choć w marketach rzadziej spotykamy się z droższymi ciuchami, to w większych supermarketach oferujących ubrania czy dodatki złodzieje potrafią szybko usunąć zabezpieczenie antykradzieżowe (klips) lub zamienić metki. Szczególnie popularne są drobne, markowe dodatki: paski, portfele, czapki z daszkiem.

4. Jak złodzieje kradną? Najczęstsze metody i schematy działania

4.1. Ukrywanie towaru w ubraniu lub torebce

Jest to najstarsza i wciąż najpopularniejsza metoda. Złodzieje wkładają towar do kieszeni, torebki, plecaka lub nawet specjalnie przygotowanych do tego ubrań, w których wnętrzu znajdują się np. specjalne kieszenie wyłożone folią aluminiową (by zablokować bramki antykradzieżowe).

4.2. Zabieranie towarów pozostawionych bez opieki

Czasami złodzieje obserwują osoby, które odkładają na chwilę zakupy czy torebki np. przy kasach samoobsługowych. Taka nieuwaga bywa wykorzystana, aby zabrać cenny produkt lub portfel.

4.3. Manipulacja przy kasach samoobsługowych

Kasy samoobsługowe bywają dużym ułatwieniem dla klientów, ale też – w przypadku braku nadzoru stanowią okazję do oszustw. Do częstych praktyk należy:

Wprowadzanie tańszego kodu kreskowego złodziej nalicza towar o znacznie niższej wartości, skanując tańszy produkt zamiast droższego.

Nie skanowanie wszystkich produktów w przypadku braku systemu weryfikacji wagi i obsługi, klient może po prostu włożyć coś do torby bez zeskanowania.

MOST WIEDZY Downloaded from mostwiedzy.pl

4.4. Zorganizowane grupy kradnące określone produkty

Zdarza się, że do sklepów przychodzą zorganizowane grupy, w których każdy ma określone zadanie: jedna osoba zajmuje uwagę obsługi, druga „czyści" półki, a trzecia „zabezpiecza" drogę wyjścia. Dodatkowo używają telefonu komórkowego do komunikacji między sobą.

5. Wdrożenie rozwiązań AI w celu przeciwdziałania kradzieży

5.1. Dobór odpowiednich kamer i oprogramowania

Pierwszym krokiem do skutecznego wdrożenia sztucznej inteligencji w systemie ochrony jest wybór kamer dostosowanych do potrzeb danego obiektu. Ważne, by kamery miały:

Wysoką rozdzielczość (co najmniej Full HD, a optymalnie 4K), aby system AI mógł rozpoznawać detale i twarze.

Funkcję rejestracji nocnej lub przy słabym oświetleniu, jeśli sklep działa w godzinach wieczornych i nocnych.

Systemy analizy obrazu w czasie rzeczywistym.

Następnie potrzebne jest oprogramowanie, które w sposób automatyczny będzie analizowało strumień wideo:

Wykrywając podejrzane zachowania, takie jak długotrwałe przebywanie w jednym miejscu, nerwowe rozglądanie się, nieuzasadnione poruszanie się w strefach mniej dostępnych dla klientów.

Sygnalizując personelowi sytuacje potencjalnie niebezpieczne (np. próby otwarcia zamkniętych szafek, wynoszenie nieopłaconych towarów, przekraczanie linii bramek bezpieczeństwa).

5.2. Integracja z systemami POS i bramek antykradzieżowych

Zaawansowane systemy antykradzieżowe powinny być też zintegrowane z systemami kasowymi (POS) i bramek bezpieczeństwa, aby:

Automatycznie porównywać listę zeskanowanych produktów z obrazem z kamer (np. jeśli w koszyku widnieje drogi alkohol, a w kasie nie został uwzględniony, system zasygnalizuje rozbieżność).

Informować o wejściu i wyjściu klientów w czasie rzeczywistym, a także o ile jest to zgodne z przepisami RODO – o powracających sprawcach.

5.3. Personalizacja alertów

Należy też zadbać o spersonalizowane alerty dla różnych scenariuszy. Inny komunikat wyświetli się, gdy system rozpozna osobę, która zeskanowała produkt o zbyt niskiej cenie (podejrzenie manipulacji), a inny, gdy ktoś wynosi produkt bez zapłaty. Manager i personel muszą otrzymywać przejrzyste powiadomienia na urządzeniach mobilnych lub na centralnym monitorze, by szybko zareagować.

MOST WIEDZY Downloaded from mostwiedzy.pl

6. Działania towarzyszące: polityka personalna i kultura bezpieczeństwa

6.1. Dbanie o właściwe postawy wśród pracowników

Jak wspomniałem, technologia nie zastąpi zaangażowanego personelu. Jeśli w firmie panuje brak zaufania, niska motywacja czy niewystarczające szkolenia, nawet najbardziej rozbudowany system AI może nie zadziałać efektywnie. Dlatego tak istotne jest:

Regularne szkolenie w tym także symulacje zachowań złodziei, by pracownicy potrafili szybko reagować.

Motywowanie pracowników systemy premiowe za obniżenie poziomu strat wynikających z kradzieży.

Budowanie kultury bezpieczeństwa – każdy członek zespołu musi mieć świadomość, że celem jest nie tylko obrona towaru, ale też ochrona klientów przed zagrożeniami.

6.2. Współpraca z ochroną fizyczną

W przypadku większych marketów nierzadko zatrudnia się pracowników ochrony. Kluczowe jest, by ich rola nie ograniczała się wyłącznie do patrolowania sklepu, lecz by realnie współpracowali z systemami AI i personelem. Ochroniarz otrzymujący alert może w ciągu kilkunastu sekund potwierdzić lub wykluczyć ryzyko. To skutecznie zniechęca potencjalnych złodziei, gdyż wiedzą oni, że w sklepie działają profesjonalne procedury bezpieczeństwa.

6.3. Przemyślane procedury interwencji

Nie wolno zapominać o tym, że ujęcie złodzieja wiąże się również z odpowiedzialnością prawną. Pracownicy powinni znać przepisy dotyczące ujęcia obywatelskiego, sposoby wzywania policji oraz zasady zabezpieczania dowodów. Nieuprawnione użycie siły czy upublicznienie wizerunku sprawcy bez podstawy prawnej może skutkować poważnymi konsekwencjami dla samego sklepu.

7. Przeciwdziałanie kradzieżom doświadczenia i rekomendacje Marcina Niedopytalskiego

Jako ekspert ds. ochrony osób i mienia, przeprowadziłem dziesiątki audytów w obiektach handlowych różnej wielkości. Chciałbym podzielić się kilkoma doświadczeniami i rekomendacjami, które sprawdziły się w praktyce:

7.1. Kompleksowy audyt zagrożeń

Zanim zaczniemy wdrażać kosztowne rozwiązania technologiczne, warto wykonać szczegółowy audyt bezpieczeństwa. Obejmuje on:

Analizę dotychczasowych strat i zapisów z monitoringu.

Ocenę rozmieszczenia towarów, wysokości półek, oświetlenia.

Przegląd procedur i metod szkolenia personelu. Po rzetelnym audycie łatwiej zaplanować środki zabezpieczenia i uniknąć przepłacania za rozwiązania, które nie są rzeczywiście potrzebne.

MOST WIEDZY Downloaded from mostwiedzy.pl

7.2. Synergia ludzi i maszyn

Najlepsze efekty przynosi połączenie sprawdzonych, tradycyjnych metod (ochroniarze, personel, bramki antykradzieżowe, system EAS – Electronic Article Surveillance) z nowoczesną analizą AI. Wtedy istnieje większa szansa na wczesne wykrycie kradzieży i skuteczną reakcję.

7.3. Transparentna komunikacja z klientami

Klienci mają prawo wiedzieć, że w sklepie działają systemy monitoringu. Nie oznacza to, że od razu należy wszędzie wywieszać tabliczki „Tu działa AI, nie kradnij!". Jednak jasna informacja o aktywnym monitoringu oraz obecności personelu i ewentualnie firmy ochroniarskiej może działać prewencyjnie. Brak ukrywania faktu, że wykorzystuje się nowoczesne technologie, zwykle obniża liczbę przypadków kradzieży.

7.4. Rejestrowanie recydywistów w ramach przepisów prawa

W niektórych krajach dopuszczalne jest prowadzenie systemów rozpoznawania twarzy (Face Recognition) w celu identyfikacji osób, które notorycznie dokonują kradzieży w danym sklepie. W Polsce i Unii Europejskiej należy jednak ściśle przestrzegać przepisów RODO, co ogranicza swobodę takiej identyfikacji. Wszelkie systemy AI muszą być wdrażane w pełnej zgodności z obowiązującymi regulacjami, w tym z rozporządzeniami dotyczącymi ochrony danych osobowych.

8. Praktyczne porady dla właścicieli i managerów sklepów

Na bazie powyższych wniosków przygotowałem kilka prostych, acz skutecznych wskazówek:

Zainwestuj w dostosowany do potrzeb system AI

Nie każdy sklep potrzebuje najbardziej zaawansowanej technologii. Jeśli masz małą placówkę, wystarczy parę dobrej jakości kamer i proste narzędzia analityczne wykrywające ruch w newralgicznych strefach.

Rozmieszczaj towary strategicznie

Artykuły najczęściej kradzione umieść w miejscach, do których trudniej sięgnąć niepostrzeżenie lub tam, gdzie personel ma ciągły wgląd.

Korzystaj z bramek antykradzieżowych

Choć złodzieje nauczyli się obchodzić podstawowe bramki, wciąż są one cennym elementem systemu bezpieczeństwa, szczególnie połączone ze sztuczną inteligencją i systemem monitoringu.

Szkol personel w zakresie detekcji i postępowania

Pracownicy powinni wiedzieć, co robić w sytuacji podejrzenia kradzieży, jakie procedury obowiązują oraz jak bezpiecznie wezwać ochronę lub policję.

MOST WIEDZY Downloaded from mostwiedzy.pl

Twórz przyjazne, a jednocześnie czujne środowisko

Klient powinien czuć się mile widziany, ale jednocześnie zauważać, że obsługa jest świadoma jego obecności i dba o bezpieczeństwo.

Regularnie analizuj dane

Jeśli system AI dostarcza statystyki, warto je przeglądać: w których godzinach dochodzi do największej liczby kradzieży, które produkty znikają najczęściej, z jakimi zachowaniami wiązały się wykryte kradzieże. Na tej podstawie można udoskonalać strategie ochrony.

9. Strategia bezpieczeństwa w dobie sztucznej inteligencji

Współczesne supermarkety i markety z niskimi półkami muszą mierzyć się z wieloma wyzwaniami w zakresie bezpieczeństwa. Kradzieże generują poważne koszty, a przy rosnącej presji na optymalizację wydatków i rentowność działalności, konieczne jest zastosowanie efektywnych środków ochrony. Sztuczna inteligencja oferuje niezwykle cenne narzędzia: analizę zachowań klientów w czasie rzeczywistym, automatyczne powiadamianie personelu, integrację z systemami sprzedażowymi i bramkami antykradzieżowymi, a także możliwość precyzyjnego profilowania powracających sprawców. Najważniejsze jest jednak, by pamiętać, że sam system AI, choć potężny, nie rozwiąże wszystkich problemów. Dobrze wyszkolony personel, odpowiednie procedury interwencji oraz przemyślane rozmieszczenie towaru i systemu kamer to klucz do skutecznej ochrony. Klient, który widzi, że sklep jest profesjonalnie przygotowany do zapobiegania kradzieżom, zwykle nie będzie podejmował ryzyka. Natomiast w sytuacjach, gdy do kradzieży jednak dochodzi, sprawny system monitoringu w połączeniu z wykwalifikowanym zespołem umożliwia szybką i właściwą reakcję.

10 Prognozy rozwoju i wyzwania przyszłości

Patrząc w przyszłość, można założyć, że systemy oparte na sztucznej inteligencji będą się rozwijać w zawrotnym tempie. Wzrost mocy obliczeniowej komputerów, doskonalenie algorytmów uczenia maszynowego (machine learning) i deep learningu sprawi, że detekcja kradzieży będzie coraz dokładniejsza. Nowością może być także integracja z innymi systemami, np. z systemami rozpoznawania mowy, dzięki czemu AI mogłaby wykrywać niepokojące rozmowy lub hasła kluczowe wypowiadane przez klientów (oczywiście z zachowaniem przepisów dotyczących prywatności). Z drugiej strony wzrośnie też kreatywność złodziei. Mogą pojawić się zaawansowane sposoby maskowania się przed kamerami (specjalne materiały i ubrania), wykorzystywanie dronów w sytuacjach plenerowych (np. do podawania towaru przez okno magazynu) czy hacking systemów monitoringu. Dlatego tak ważne jest, by właściciele obiektów handlowych dbali o regularne aktualizacje oprogramowania, testowanie zabezpieczeń i szkolenie personelu, by nadążyć za zmieniającymi się zagrożeniami. zabezpieczenie obiektu przed kradzieżą za pomocą sztucznej inteligencji to obecnie jeden z najbardziej obiecujących kierunków rozwoju w branży ochrony. Systemy AI odpowiednio wdrożone i skalibrowane pozwalają na szybkie wykrycie podejrzanych zachowań, automatyczne powiadomienie personelu i integrację z innymi elementami infrastruktury bezpieczeństwa. Jednocześnie nie można poprzestawać na

MOST WIEDZY Downloaded from mostwiedzy.pl

technologii. Niezwykle istotna jest rola czynnika ludzkiego: wykwalifikowanego, zmotywowanego personelu, obecności ochrony fizycznej (w zależności od skali obiektu) i spójnych procedur. Właściwe rozmieszczenie towarów, szkolenia z zakresu rozpoznawania potencjalnych złodziei, przemyślane wykorzystywanie kas samoobsługowych i dbałość o kulturę bezpieczeństwa wszystko to sprawia, że ryzyko strat spada, a klienci i pracownicy czują się pewniej. Dlatego zachęcam do prowadzenia audytów bezpieczeństwa, konsultacji ze specjalistami i wdrażania rozwiązań AI dostosowanych do konkretnego sklepu. Jako Marcin Niedopytalski ekspert ds. ochrony osób i mienia zawsze rekomenduję holistyczne podejście, w którym nowoczesne technologie idą w parze z mądrym zarządzaniem i przeszkolonym personelem. Tylko wtedy można mówić o realnej, długofalowej skuteczności w przeciwdziałaniu kradzieżom i budowaniu wizerunku bezpiecznego miejsca zakupów. W poprzedniej części artykułu omówiliśmy zagadnienia związane z przeciwdziałaniem kradzieżom w obiektach handlowych, rolę nowoczesnych rozwiązań opartych na sztucznej inteligencji, a także podstawowe założenia dotyczące organizacji i rozmieszczenia towarów. Podkreśliliśmy, że sama technologia nawet najbardziej zaawansowana – nie zastąpi dobrze wyszkolonego personelu. Dotyczy to zarówno pracowników sklepu, jak i ochrony fizycznej. W niniejszej części skupimy się na tym, jak przygotować pracowników ochrony do efektywnego działania w środowisku, w którym kluczową rolę w zapobieganiu kradzieżom odgrywa AI. Poruszymy kwestie kompetencji niezbędnych w codziennej pracy, metody szkoleniowe i organizacyjne, a także zwrócimy uwagę na aspekty prawne i etyczne szczególnie istotne w kontekście wykorzystywania technologii analitycznych.

11 Wprowadzenie do szkolenia znaczenie roli ochrony

Ochrona fizyczna, czyli pracownicy ochrony przebywający na terenie sklepu, pełni kluczową rolę w procesie przeciwdziałania kradzieży. Nowoczesne systemy monitorujące i analizy wideo (z wykorzystaniem sztucznej inteligencji) służą głównie wczesnej detekcji i identyfikacji potencjalnych zagrożeń, ale to człowiek decyduje o formie i momencie interwencji. W środowisku, w którym nadzór wizyjny jest coraz bardziej zaawansowany, rola pracownika ochrony ewoluuje z pozycji „patrolowania i reagowania doraźnego" do „aktywnie wspieranej technologicznie interwencji precyzyjnej". Oznacza to, że szkolenie ochrony musi obejmować zarówno tradycyjne techniki pracy (obserwacja, umiejętność przeprowadzenia interwencji fizycznej czy ujęcia obywatelskiego), jak i podstawy działania systemów AI.

Kluczowe elementy wstępnego szkolenia obejmują:

Świadomość zagrożeń – zrozumienie, jak działają złodzieje, jakich metod używają i na co zwracać uwagę w codziennej pracy.

Znajomość procedur sklepu – wiedza o tym, gdzie znajdują się newralgiczne punkty (kasy samoobsługowe, regały z drogimi artykułami, strefy niedostatecznie oświetlone).

Komunikacja z personelem – ustalenie jasnych reguł wymiany informacji, kanałów łączności oraz priorytetów reakcji (kogo powiadomić w pierwszej kolejności, jak dokumentować incydenty itp.).

MOST WIEDZY Downloaded from mostwiedzy.pl

12 Analiza zagrożeń i schematów kradzieży kontekst praktyczny

Przeciwdziałanie kradzieżom wymaga rzetelnej analizy dostępnych danych statystycznych oraz zrozumienia typowych schematów kradzieży:

Kradzieże „drobne”: produkty łatwe do schowania, szybko zbywalne, takie jak perfumy w małych flakonach, baterie, słodycze, używki, drobna elektronika.

Kradzieże „zorganizowane”: działanie w grupie, odwracanie uwagi personelu i ochrony, jednoczesna kradzież z kilku sektorów sklepu.

Wykorzystywanie kas samoobsługowych: skanowanie tańszych produktów, wprowadzanie niepoprawnych kodów, fałszywe ważenie owoców i warzyw, a także „pomijanie” niektórych artykułów w procesie kasowania.

Kradzieże z użyciem narzędzi i technologii: torby i ubrania wyłożone folią aluminiową, manipulacja przy bramkach antykradzieżowych (przecięcie kabli, dezaktywacja metek).

W ramach szkolenia pracowników ochrony warto przeprowadzać zajęcia praktyczne, podczas których omawia się najczęstsze taktyki wykorzystywane przez złodziei. Dzięki temu ochrona łatwiej rozpoznaje sytuacje nietypowe i odpowiednio wcześnie reaguje.

13 Technologie AI w sklepach i ich wpływ na pracę ochrony

Jak już wiemy z poprzedniej części opracowania, systemy AI wykorzystywane w monitoringu mogą automatycznie rozpoznawać potencjalnie podejrzane zachowania. Algorytmy przeprowadzają analizę behawioralną klientów w czasie rzeczywistym, a następnie:

Wysyłają alert do pracownika ochrony (np. w postaci powiadomienia na urządzenie mobilne).

Udostępniają wideo na żywo z danej kamery, dzięki czemu ochroniarz w kilka sekund może ocenić sytuację.

Sugerują priorytet zdarzenia w zależności od wykrytych okoliczności (np. czy dotyczy produktu wysokiej wartości, czy wykryto próbę niszczenia zabezpieczeń).

W efekcie rola ochrony polega na przetworzeniu otrzymanych informacji z systemu AI i podjęciu decyzji: *Czy wysłać pracownika do obserwacji z bliska? Czy poprosić personel sklepu o nawiązanie kontaktu z klientem? Czy też wezwać policję?*

Szkolenie w tym zakresie powinno obejmować:

Znajomość interfejsu systemu – gdzie pojawiają się powiadomienia, jak reagować na poszczególne komunikaty, jak odtwarzać zarejestrowany materiał wideo w trybie natychmiastowym.

Identyfikacja fałszywych alarmów AI, choć zaawansowana, nie jest nieomylna. Czasem algorytm błędnie zaklasyfikuje zupełnie normalne zachowanie jako podejrzane. Dobry

MOST WIEDZY Downloaded from mostwiedzy.pl

pracownik ochrony potrafi szybko wychwycić takie sytuacje, unikając niepotrzebnych interwencji.

Procedury eskalacji – rozpoznanie momentu, w którym trzeba powiadomić wyższe kierownictwo lub służby zewnętrzne (np. policję), a także sposoby zabezpieczenia miejsca zdarzenia oraz dowodów (materiał z kamer, opis sytuacji, dane świadków).

13 Kompetencje kluczowe: obserwacja, komunikacja, interwencja

4.1. Obserwacja

Podstawą skutecznego działania ochrony jest uważna obserwacja. Nawet w erze zaawansowanej analizy wideo, wiele sytuacji wymaga ludzkiego oka i wyczucia. System może nie wychwycić subtelnych oznak stresu, nerwowych ruchów czy interakcji między kilkoma osobami. Dlatego szkolenia powinny rozwijać:

Uważność przestrzenną – rozpoznawanie potencjalnie niebezpiecznych zakamarków sklepu, obserwowanie zachowań w wąskich korytarzach, przy niskich półkach.

Rozpoznawanie emocji i mowy ciała – szybkie zauważanie, że ktoś unika kontaktu wzrokowego, nadmiernie się rozgląda, nerwowo przechodzi między regałami, często dotyka kieszeni lub torby.

4.2. Komunikacja

Skuteczne zapobieganie kradzieżom nie istnieje bez odpowiedniej komunikacji. Pracownik ochrony powinien umieć w kulturalny i zdecydowany sposób zwrócić się do klienta, kiedy pojawia się podejrzenie kradzieży. Ważne są tu:

Umiejętność asertywnego podejścia – np. poproszenia o okazanie paragonu, bez jednoczesnego naruszania godności klienta (co mogłoby się skończyć zarzutem o zniesławienie).

Współpraca z personelem sklepu – szybkie przesyłanie informacji o pojawiających się podejrzanych osobach, a także reagowanie na sygnały od kasjerów czy kierownika sklepu.

Rozmowa z grupą – jeżeli mamy do czynienia z grupą potencjalnych sprawców, pracownik ochrony musi wiedzieć, jak rozdzielić role i wezwać wsparcie, aby nie dopuścić do ucieczki całej grupy.

4.3. Interwencja

Interwencja to moment najbardziej newralgiczny. Pracownik ochrony może dokonać tzw. ujęcia obywatelskiego, jeśli jest świadkiem przestępstwa. Jednak musi to robić w sposób zgodny z przepisami. Szkolenie powinno obejmować:

Podstawy prawa – kiedy można zatrzymać osobę na gorącym uczynku, jak wygląda procedura przekazania policji, jakie dokumenty trzeba wypełnić i w jaki sposób zabezpieczyć ewentualne dowody.

MOST WIEDZY Downloaded from mostwiedzy.pl

Techniki obezwładniania – używane wyłącznie w ostateczności, zgodnie z zasadą minimalizacji środków przymusu. Pracownik ochrony musi być przygotowany na sytuacje, w których sprawca stawia opór lub próbuje użyć przemocy.

Bezpieczeństwo własne i osób postronnych priorytetem jest uniknięcie eskalacji konfliktu, ochronienie klientów i personelu przed zagrożeniem.

14 Program szkoleniowy etapy, metody i narzędzia

5.1. Etapy szkolenia

Szkolenie wstępne (podstawowe)

Zapoznanie z regulaminem sklepu i procedurami bezpieczeństwa.

Prezentacja najczęstszych metod kradzieży.

Podstawy komunikacji i podejścia do klienta.

Szkolenie zaawansowane

Udział w symulacjach kradzieży i obserwowanie zachowań złodziei.

Nauka obsługi systemów AI i interpretacji alertów.

Rozwijanie umiejętności współpracy z zespołem kasjerów i kierownictwem.

Szkolenie specjalistyczne (cykliczne)

Aktualizacja wiedzy o nowych metodach kradzieży, możliwościach obejścia bramek antykradzieżowych.

Doskonalenie umiejętności interpersonalnych, w tym prowadzenia negocjacji w sytuacjach kryzysowych.

Pogłębianie wiedzy prawniczej (zmieniające się przepisy dotyczące ochrony danych, praw konsumenta, RODO itp.).

5.2. Metody szkoleniowe

Wykłady teoretyczne dotyczące regulacji prawnych, zasad użycia siły i uprawnień pracowników ochrony.

Ćwiczenia praktyczne i scenariusze symulacyjne – inscenizacje kradzieży, w których uczestnicy wcielają się w rolę złodziei, ochroniarzy i klientów.

Case studies – analiza autentycznych przypadków kradzieży i sposobu postępowania.

Platformy e-learningowe – szczególnie przydatne do omawiania funkcjonowania systemów AI, prezentacji nagrań wideo czy demonstrowania kroków postępowania w ramach przydzielonych procedur.

5.3. Narzędzia wspomagające proces szkolenia

Urządzenia mobilne z zainstalowaną aplikacją do obsługi systemów AI, które pozwalają trenować na realnych alertach i ćwiczyć szybkie reagowanie.

MOST WIEDZY Downloaded from mostwiedzy.pl

Kombinezony treningowe – przy nauce technik obezwładniania lub ujęcia sprawcy.

Wirtualna rzeczywistość (VR) – coraz częściej stosowana do symulowania sytuacji ekstremalnych i trudnych do zainscenizowania w warunkach sklepowych (np. współpraca z dużą grupą klientów, ewakuacja itp.).

15 Szkolenie z obsługi systemów AI podstawy i poziomy zaawansowania

6.1. Poziom podstawowy

Na tym etapie pracownik ochrony poznaje ogólny interfejs systemu:

Gdzie pojawiają się alerty?

Jak rozpoznawać podstawowe komunikaty i priorytety?

W jaki sposób system sygnalizuje lokalizację zdarzenia w obrębie sklepu (np. plan pomieszczeń, sektorów)?

Co oznaczają różne kody alertów (np. czerwony – pilny, żółty – podejrzany, szary – do weryfikacji)?

Ważne jest, aby ochroniarz nabrał intuicji i pewności w poruszaniu się po interfejsie AI. Dla wielu osób, zwłaszcza tych mniej biegłych w nowych technologiach, obsługa specjalistycznego oprogramowania może być wyzwaniem. Dlatego szkolenie podstawowe powinno być przeprowadzone w formie warsztatów praktycznych.

6.2. Poziom zaawansowany

Na poziomie zaawansowanym skupiamy się na interpretacji zachowań i zrozumieniu mechanizmów, na których opierają się algorytmy AI:

Analiza behawioralna – zrozumienie, jakie wskaźniki (np. tempo poruszania, spędzony czas w danym obszarze, nietypowe ruchy rąk) wpływają na to, że system oznacza klienta jako „podejrzanego”.

Rozpoznawanie fałszywych alarmów – doświadczenie podpowiada, że pewne osoby mogą po prostu dłużej oglądać produkt, co jeszcze nie świadczy o kradzieży. Ochroniarz musi wypracować umiejętność rozróżniania takich sytuacji.

Integracja z innymi systemami (POS, bramki antykradzieżowe, liczniki ruchu w sklepie) – na tym etapie ochroniarz uczy się, jak weryfikować spójność danych (np. klient przeszedł przez bramkę, system AI sygnalizuje potencjalną kradzież, a jednocześnie w POS nie ma zarejestrowanej płatności za dany towar).

6.3. Poziom ekspercki (dla osób zarządzających)

Dla kadry zarządzającej ochroną i menedżerów bezpieczeństwa przewiduje się jeszcze wyższy poziom specjalizacji:

Analiza danych i statystyk – ocena trendów kradzieży w danym sklepie, ustalanie planu dyżurowania na podstawie najczęstszych godzin incydentów.

MOST WIEDZY Downloaded from mostwiedzy.pl

Projektowanie polityki bezpieczeństwa oparte na długofalowej współpracy z dostawcami systemów AI, audytach bezpieczeństwa i bieżących obserwacjach.

Opracowywanie procedur kryzysowych np. jak postępować w sytuacji awarii systemów AI, jak szybko przejść na „tryb ręczny" obserwacji czy jak koordynować działania z policją.

15 Wdrożenie procedur reakcji kooperacja z personelem i integracja systemowa

Często bagatelizuje się znaczenie spójnego łańcucha reagowania, który łączy ochronę, pracowników kas, kierowników działów i obsługę administracyjną sklepu. Dobrze wyszkolony zespół ochrony musi:

Otrzymywać alert od AI – wstępnie go zinterpretować (np. podejrzenie kradzieży na dziale elektroniki).

Powiadomić personel w danym dziale – by upewnić się, czy klient nie prosił o pomoc, czy nie prowadził dłuższej rozmowy np. o produkcie. Czasami towarzyszy temu weryfikacja w systemie POS (czy towar został zeskanowany).

Skierować pracownika ochrony na miejsce zdarzenia – w celu obserwacji z bliska lub dyskretnej interwencji.

Ewentualnie wezwać wsparcie – jeśli sytuacja jest poważniejsza (np. podejrzenie kradzieży przez zorganizowaną grupę lub próba agresji).

Procedury te należy ćwiczyć w warunkach symulacyjnych. Im częściej pracownicy ochrony realizują zadania według ustalonych reguł, tym sprawniej przechodzą do działania w realnej sytuacji.

16 Aspekty prawne i etyczne w szkoleniu ochrony

Wykorzystanie sztucznej inteligencji w ochronie obiektów handlowych nie odbywa się w próżni prawnej. Istnieją liczne regulacje (zwłaszcza w zakresie RODO i ochrony danych osobowych) oraz wymogi etyczne, których naruszenie może skutkować poważnymi konsekwencjami. Dlatego w szkoleniu pracowników ochrony należy uwzględnić:

Zasady retencji danych wideo – jak długo można przechowywać nagrania i w jakim celu?

Ograniczenia w stosowaniu rozpoznawania twarzy – w wielu krajach (w tym w Polsce) pełne wykorzystanie systemów Face Recognition w sklepach jest istotnie ograniczone lub wymaga wyraźnej zgody klientów.

Prawo do prywatności – klient nie może czuć się nadmiernie inwigilowany. Oznacza to, że ochrona musi powstrzymać się od zbyt intensywnego „śledzenia" klienta, jeśli brak uzasadnionego podejrzenia kradzieży.

Granice użycia siły – ujęcie obywatelskie dotyczy sytuacji, w której pracownik ochrony jest świadkiem przestępstwa. Musi działać proporcjonalnie, nie może przekroczyć uprawnień (np. przeszukiwanie bagażu klienta bez jego zgody i bez obecności policji jest wątpliwe prawnie).

MOST WIEDZY Downloaded from mostwiedzy.pl

Uwzględnienie tych aspektów ma istotne znaczenie dla reputacji sklepu, a także minimalizuje ryzyko roszczeń ze strony klientów, którzy mogliby poczuć się poszkodowani.

17 Motywowanie i rozwój zawodowy pracowników ochrony

Niezwykle ważnym elementem, który decyduje o skuteczności systemu ochrony, jest motywacja pracowników. Niskie płace, brak perspektyw rozwoju i monotonność zadań mogą prowadzić do braku zaangażowania. Dlatego warto inwestować w:

System motywacyjny

Premie za wyraźne obniżenie wskaźnika kradzieży w danym okresie.

Dodatki za udział w szkoleniach lub za uzyskanie certyfikatów specjalistycznych (np. z zakresu pierwszej pomocy, obsługi AI czy technik interwencyjnych).

Ścieżkę rozwoju kariery

Awans na stanowisko starszego inspektora ochrony, koordynatora zespołu czy kierownika ds. bezpieczeństwa.

Możliwość udziału w ogólnokrajowych konferencjach branżowych lub specjalistycznych szkoleniach dotyczących rozwoju systemów bezpieczeństwa.

Dobre warunki pracy

Zapewnienie odpowiedniej liczby pracowników w zespole ochrony, by nie byli przeciążeni i mieli czas na rzetelną obserwację (zamiast nerwowego biegania od jednego incydentu do drugiego).

Dostarczanie nowoczesnych narzędzi i wyposażenia (np. kamery na mundurach, radiotelefony cyfrowe, ergonomiczne stanowiska monitorowania).

Z punktu widzenia systemu AI, posiadanie wysoko zmotywowanego zespołu ochrony jest kluczowe. Tylko wtedy alerty generowane przez algorytmy będą właściwie interpretowane, a interwencje sprawne i skuteczne.

19 Ochrona w erze sztucznej inteligencji

Rozwój technologii AI bez wątpienia przynosi nową jakość w zakresie zapobiegania kradzieżom w obiektach handlowych. Sklepy wyposażone w systemy detekcji zachowań klientów, integrację z kasami samoobsługowymi i bramkami antykradzieżowymi mogą w szybkim tempie redukować straty. Jednak nawet najlepszy system analizy wideo będzie niewystarczający, jeśli pracownik ochrony nie potrafi go obsługiwać, a w sytuacji kryzysowej nie zareaguje profesjonalnie i z poszanowaniem prawa. Właśnie dlatego kompleksowe szkolenie personelu ochrony w zakresie kradzieży i sztucznej inteligencji jest kluczem do sukcesu. Technologia i personel muszą wzajemnie się uzupełniać. AI wychwytuje podejrzane zdarzenia, a człowiek nadaje im kontekst i weryfikuje zasadność interwencji.

MOST WIEDZY Downloaded from mostwiedzy.pl

Wielopoziomowy program szkoleniowy

Od wprowadzenia w podstawy pracy ochrony i rozpoznawania kradzieży, przez naukę obsługi systemów AI, aż po zaawansowane szkolenia dla kadry menedżerskiej.

Stała aktualizacja wiedzy

Metody działania złodziei ewoluują; systemy AI również się rozwijają. Szkolenia cykliczne pozwalają nadążyć za zmianami w przepisach i nowinkach technologicznych.

Etyka i prawo na pierwszym miejscu

Użycie AI wiąże się z kwestiami prywatności. Pracownicy ochrony muszą działać w ramach wyznaczonych norm prawnych i z poszanowaniem godności klienta.

Motywacja i rozwój

Zespół ochrony, który widzi możliwości awansu i docenienia wysiłków, będzie bardziej skuteczny. Przyjazne środowisko pracy sprzyja zaangażowaniu i większej odpowiedzialności.

Przyszłe kierunki rozwoju szkolenia ochrony

W perspektywie kolejnych lat możemy spodziewać się dalszej integracji systemów AI z rozszerzoną rzeczywistością (AR), co umożliwi pracownikom ochrony np. wyświetlanie w czasie rzeczywistym informacji o kliencie (w granicach prawa) czy analizę najnowszych alertów bezpośrednio w okularach AR. Możliwe jest także jeszcze ściślejsze wykorzystanie „big data" łączenie danych z wielu źródeł (np. programów lojalnościowych, statystyk marketingowych, systemów IoT) pozwoli na dokładniejsze przewidywanie wzorców kradzieży. W takiej rzeczywistości rola człowieka stanie się bardziej menedżerska i koordynacyjna, ale wciąż niezastąpiona w momentach bezpośredniej interakcji z potencjalnym sprawcą **profesjonalnie wyszkolona ochrona** to dzisiaj jeden z najważniejszych filarów skutecznego wdrożenia AI w obiekcie handlowym. Dzięki temu sklep nie tylko lepiej chroni swój towar, lecz także kreuje wizerunek bezpiecznego, przyjaznego miejsca zakupów. A to przekłada się na lojalność klientów i stabilny rozwój biznesu.

Kim jestem? Jeszcze słów kilka o autorze

Nazywam się **Marcin Niedopytalski** i od lat zajmuję się doradztwem w zakresie ochrony osób i mienia. Mam za sobą wieloletnie doświadczenie w pracy w dużych korporacjach ochroniarskich, a także w mniejszych firmach, gdzie ceni się indywidualne i elastyczne podejście do problemów bezpieczeństwa. Przez moją karierę zrozumiałem, jak ogromny wpływ na skuteczność systemów bezpieczeństwa ma odpowiednie przygotowanie ludzi. Technologie – choć niesamowicie pomocne stają się realnym wsparciem dopiero wtedy, gdy są we właściwy sposób używane. Dlatego w mojej działalności koncentruję się nie tylko na doborze najnowszych rozwiązań AI, ale również na komponowaniu profesjonalnych szkoleń dla personelu ochrony i kadry zarządzającej. Pracowałem z klientami z różnych sektorów, jednak temat zabezpieczania sklepów i supermarketów jest mi wyjątkowo bliski. Każdy dzień w branży ochrony to nowe wyzwania: dynamiczny ruch klientów, różnorodność asortymentu, kasy samoobsługowe i presja na optymalizację kosztów. W tej scenerii **wyszkolony zespół ochrony** wspierany przez algorytmy AI – staje się kluczowym czynnikiem sukcesu.

MOST WIEDZY Downloaded from mostwiedzy.pl

Jeśli chcesz dowiedzieć się więcej o możliwościach szkoleń praktycznych, z chęcią pomogę w zaprojektowaniu takiego programu dla Twojego sklepu. Wierzę, że równowaga między nowoczesną technologią a dobrze przeszkolonymi ludźmi to najlepszy sposób na ograniczenie kradzieży i zbudowanie pozytywnego, bezpiecznego doświadczenia zakupowego. Patrząc w perspektywie kolejnych 5–10 lat, można śmiało stwierdzić, że **sektor ochrony czeka głęboka transformacja**, napędzana rozwojem sztucznej inteligencji, zmianami w modelach biznesowych i ewoluującymi przepisami prawnymi. Poniżej przedstawiam najważniejsze wnioski i rekomendacje:

Technologia będzie się rozwijać w zawrotnym tempie
Algorytmy deep learning staną się coraz skuteczniejsze w analizie wideo i detekcji podejrzanych zachowań, co wyraźnie obniży koszty związane z kradzieżami. Dla firm oznacza to konieczność stałego aktualizowania systemów i ponoszenia wydatków na infrastrukturę IT.

Potrzebna będzie wyspecjalizowana kadra
Pracownicy ochrony przyszłości muszą łączyć wiedzę prawną i psychologiczną z umiejętnością obsługi narzędzi AI. Pojawi się też zapotrzebowanie na „operatorów AI" czy analityków danych dedykowanych branży ochrony.

Architektura sklepów będzie projektowana pod kątem minimalizowania kradzieży
Nowoczesne układy półek, eliminacja martwych stref, kasy zintegrowane z systemami rozpoznawania produktów – wszystko to sprawi, że trudniej będzie dokonać kradzieży niepostrzeżenie.

Równowaga między prywatnością a bezpieczeństwem
Z jednej strony klienci oczekują ochrony i niskich cen (co wymaga skutecznego zapobiegania stratom), z drugiej – pragną czuć się wolni od nadmiernej inwigilacji. Sukces osiągną te sieci, które umiejętnie wyważą te dwie potrzeby.

Wzmocniona współpraca między branżą ochrony i organami ścigania społecznościami lokalnymi
Już teraz wiele sieci wymienia dane i informacje z policją, co pozwala szybciej reagować na kradzieże czy akty wandalizmu. W przyszłości ta współpraca może się zacieśnić jeszcze bardziej, zwłaszcza w kontekście systemów rozpoznawania twarzy i przepisów szczególnych dotyczących przetwarzania danych o przestępcach.

Etyka i odpowiedzialność społeczna
Odpowiedzialne korzystanie ze sztucznej inteligencji oznacza przestrzeganie przepisów i wysokich standardów etycznych. Firmy, które zdecydują się na radykalnie agresywny monitoring, mogą narazić się na krytykę opinii publicznej. Transparentna polityka informowania klientów o stosowanych systemach monitoringu, jasne procedury postępowania w razie podejrzenia kradzieży i ochrona prywatności staną się kluczowe dla utrzymania zaufania konsumentów.

Ciągłe doskonalenie szkoleń i procedur
Rola człowieka w procesie bezpieczeństwa w sklepie nie zniknie, ale będzie się zmieniać. Wciąż potrzebni będą pracownicy zdolni do szybkiego reagowania i rozwiązywania nieprzewidzianych sytuacji. Jednocześnie należy ich regularnie szkolić w obsłudze coraz bardziej złożonych systemów AI, zapewniać im wsparcie techniczne oraz dbać o atrakcyjne

MOST WIEDZY Downloaded from mostwiedzy.pl

warunki pracy i perspektywy rozwoju. Kradzieże w sklepach zawsze będą istnieć – tak długo, jak istnieje okazja i impuls do nielegalnego przywłaszczenia towaru. Jednak dzięki systemom sztucznej inteligencji oraz świadomie prowadzonym szkoleniom i rozwiązaniom organizacyjnym można znacząco ograniczyć ryzyko i skalę tego zjawiska. Najważniejsze to spojrzeć na problem w sposób **holistyczny**: od analizy przestrzeni i technologii, przez edukację i motywację personelu, aż po spójne działania prawne i komunikacyjne. **Marcin Niedopytalski**, ekspert ds. ochrony osób i mienia, z pełnym przekonaniem zachęcam do rozwijania i unowocześniania dotychczasowych procedur bezpieczeństwa. Wchodzimy w epokę, w której interdyscyplinarność łączenie wiedzy z zakresu AI, bezpieczeństwa fizycznego, prawa i psychologii odegra kluczową rolę. Sklepy przyszłości, które umiejętnie wprowadzą inteligentne systemy monitoringu i dobrze przeszkolą swoje zespoły, zyskają przewagę konkurencyjną, ograniczą straty i jednocześnie zapewnią klientom poczucie bezpieczeństwa oraz komfort podczas zakupów. **Z perspektywy przyszłości** możemy zatem mówić o trendzie, w którym **technologia i człowiek** tworzą nierozerwalną symbiozę. Dzięki innowacyjnym rozwiązaniom możliwe będzie wczesne wykrywanie zagrożeń, precyzyjne identyfikowanie nieetycznych zachowań oraz zapobieganie im w sposób profesjonalny i zgodny z prawem. Właściwie przeszkolony zespół ochrony, wsparty sztuczną inteligencją, stanie się fundamentem nowoczesnego, efektywnego i przyjaznego dla klientów środowiska zakupowego.

MOST WIEDZY Downloaded from mostwiedzy.pl