

risk focus

**ERGO
HESTIA®**

Grupa ERGO Hestia
1/2021

W NUMERZE:

Palące problemy branży
spożywczej

(Nie)bezpieczne
składowiska odpadów

W poszukiwaniu skutecznej
ochrony danych

**SAMODZIELNOŚĆ
POD KONTROLĄ**
WYZWANIA AUTONOMICZNYCH
POJAZDÓW







Od wielu miesięcy funkcjonujemy w nowej rzeczywistości, w świecie maseczek, dystansu społecznego i obostrzeń. Żyjemy w obliczu ciągłego zagrożenia. Jesteśmy świadkami realizacji scenariuszy znanych głównie z filmów katastroficznych pokroju „Roju” Irwina Allena z 1978 r. czy „Pandemii” Johna Suitsa z 2016 r. Tymczasem walka z COVID-19 trwa na wielu frontach. Czy i jak szybko szczepienia zgaszą pandemię? Trudno jednoznacznie wyrokować. Pewną nadzieję dają ekonomiści, którzy twierdzą, że przyszły rok będzie czasem odbicia gospodarczego i powrotu na ścieżkę wzrostu. Niestety, opinie części ekspertów branżowych nie są tak optymistyczne. Wiele wskazuje, że z pandemicznej zapaści możemy wychodzić latami.

Koronawirus SARS-CoV 2 zmienił sposoby komunikacji oraz charakter i organizację pracy. Praca zdalna czy absencja pracowników z powodu samoizolacji lub kwarantanny to nowe, dotychczas nieznane „obrazki” z życia niemal każdej firmy. To z jednej strony mniejsze ryzyko np. wypadku przy pracy czy awarii maszyny, gdyż jak wiemy człowiek jest często sprawcą zdarzeń niepożądanych. Z drugiej natomiast obserwujemy wzrost zagrożenia z uwagi na brak lub niewystarczający poziom monitoringu i kontrolowania różnych kategorii ryzyka. I nic dziwnego, że coraz trudniej w tej sinusoidzie dokonać trafnej identyfikacji i oceny ryzyka, zwłaszcza że zmienia się ona w sposób dynamiczny. Firma dotychczas pracująca pełną parą, może w ciągu kilku dni zamienić się w kompleks pustych budynków, w których hula wiatr.

Na razie nie zapominajmy jednak o innych obszarach naszych codziennych aktywności. Dlatego zachęcam do sięgnięcia po niniejszy numer naszej publikacji. Życzę przyjemnej lektury.

Zbigniew Żyra
Redaktor Naczelny

spis treści

6

Risk Cafe

8

Samodzielność pod kontrolą

14

Palące problemy branży spożywczej

20

(Nie)bezpieczne składowiska odpadów

28

W poszukiwaniu skutecznej ochrony danych

34

Na własne ryzyko

**ERGO
HESTIA**

Risk Focus, Magazyn STU ERGO Hestia S.A.
Redaktor Naczelny: Zbigniew Żyra

Sopockie Towarzystwo Ubezpieczeń ERGO Hestia S.A.
ul. Hestii 1, 81-731 Sopot
www.ergohestia.pl

Zespół Redakcyjny:
Izabela Balcerzak
Magdalena Pukownik
Kamil Bara
Jacek Woronkiewicz
Tomasz Tkaczyk

MS
GROUP

Produkcja: MS Group Sp. z o.o.
Wydawca: Michał Stankiewicz
Skład: Aneta Doromiejczuk
Korekta: Halszka Gronek

risk cafe

Auta w ogniu

Zarząd Portu Genui poinformował o pożarze kilkuset nowych aut Maserati zaparkowanych we włoskiej Savonie. Luksusowe pojazdy były przeznaczone na eksport do krajów Bliskiego Wschodu. W pożarze uszkodzonych zostało również kilka tysięcy samochodów ciężarowych i osobowych o mniejszej wartości niż Maserati. Ogień pojawił się po zalaniu portu w czasie powodzi. Słona woda morska doprowadziła do zwarcia akumulatorów samochodowych, powodując ich eksplozję. Walka strażaków z żywiołem trwała prawie dobę. W wyniku powodzi zniszczeniu uległo także portowe nabrzeże. Strat nie oszacowano.



Polska Cyberarmia

Komisja Obrony Narodowej zorganizowała debatę na temat procesu budowy kwalifikacji i gotowości do działań w obszarze cyberprzestrzeni. Z przedstawionych informacji można się dowiedzieć, że trwają prace koncepcyjne nad powołaniem Wojsk Obrony Cyberprzestrzeni. Nie są jeszcze znane: liczebność, data powołania ani kompetencje nowego rodzaju sił zbrojnych. Wiemy natomiast, że ich głównym zadaniem ma być „wykrywanie, rozpoznawanie i zapobieganie cyberzagrożeniom” oraz „planowanie i prowadzenie działań militarnych w cyberprzestrzeni”. Cyberprzestrzeń stała się drugą płaszczyzną, na której odbywają się działania militarne. Cyberwojny miały już miejsce na świecie, dlatego nie powinien dziwić fakt, że powoływane są tego typu siły zbrojne. Przykładem państw, w których takie siły już funkcjonują, są chociażby Ameryka, Chiny czy Rosja. Być może do grona państw z cyberarmią dołączy również Polska.

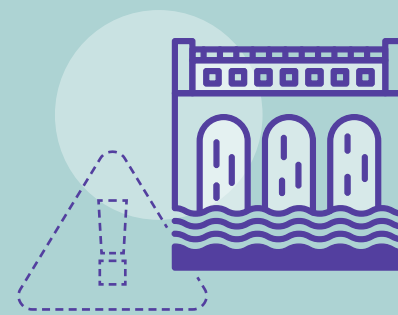


Profil zaufany?

W ostatnim czasie widoczna jest wzmożona aktywność cyberprzestępców, którzy rozsyłają wiadomości z zainfekowanymi załącznikami, podszywając się pod Profil Zaufany, ZUS, KRUK. W każdym z przypadków otworzenie załącznika powoduje zainstalowanie programu, który daje oszustom pełną kontrolę nad urządzeniem. Wiadomości zachowują stylistykę korespondencji powyższych instytucji i wyglądają bardzo wiarygodnie. Zazwyczaj informują o zaległych składkach, płatnościach lub nieopłaconych fakturach, które rzekomo dołączane są do e-maila. Należy pamiętać, aby zawsze weryfikować nadawcę wiadomości oraz nigdy pochopnie nie pobierać i otwierać załączników – zwłaszcza wtedy, gdy nie oczekujemy takiej wiadomości. W przypadku Profilu Zaufanego wiadomości przychodziły z adresu profilzaufanty@gov.pl zamiast profilzaufany@gov.pl.

Sposób na trzęsienie ziemi

Budynki w miejscach zagrożonych wstrząsami sejsmicznymi mogą być bezpieczne? Naukowcy z Politechniki Warszawskiej przedstawili pomysł na ich ochronę. Są to tzw. płyny zagęszczane ścinaniem. Praca naukowców zdobyła uznanie na międzynarodowych targach Innotech Expo w Tajwanie. Specjalna substancja, która twardnieje pod wpływem uderzenia lub innego rodzaju gwałtownego nacisku, może być wykorzystywana pod budynkami w strefie zagrożonej trzęsieniem ziemi. Płyn jest umieszczany w komorach z tłokami, montowanych w fundamentach budynków. Podczas trzęsienia ziemi wstrząsy poruszają tłokami, których ruchy powodują z kolei zagęszczenie otaczającego je płynu. Całość działa jak tłumik. Zawartość antysejsmicznej cieczy tworzy zazwyczaj twarde cząstki tlenków ceramicznych (np. krzemionka) umieszczone w ciekłym organicznym związku chemicznym.



Niebezpieczne garażowanie

Blisko 50 samochodów spłonęło w podziemnym garażu na terenie Warszawy. W akcji gaśniczej udział brało 90 strażaków, którzy walczyli nie tylko z ogniem, ale również z ogromnym zadymieniem, jakie utrudniało ewakuację mieszkańców bloku. Wskutek wysokiej temperatury uszkodzeniu uległa konstrukcja stropu podziemnego parkingu. Powiatowy Inspektor Nadzoru Budowlanego wydał decyzję o zakazie użytkowania feralnego budynku. W dwóch kolejnych zostały odłączone media z uwagi na uszkodzone instalacje: wodociągowo-kanalizacyjne oraz elektryczną.



Woda zniszczyła tamę

Podczas budowy zapory wodnej w południowym Laosie doszło do katastrofy budowlanej. W wyniku zdarzenia życie straciły dwie osoby, kilkaset zostało rannych, a prawie siedem tysięcy straciło dach nad głową. Wskutek zawalenia się części elektrowni 5 mld m³ wody zalało co najmniej siedem okolicznych wsi położonych nad rzeką Xe-Pian Xe. Pęknięcie konstrukcji było następstwem ulewnych deszczy i burz tropikalnych, jakie w lipcu nawiedziły Laos. Tama miała zostać oddana do użytku jeszcze w 2019 roku, a wartość projektu szacowano na 1,02 mld USD.



Utracona dokumentacja

Ponad 72 godziny trwała akcja gaśnicza krakowskiej straży pożarnej, której członkowie zmagali się z płonącym Archiwum Urzędu Miasta. Budynek został oddany do użytku w 2018 roku. Posiadał dwie hale. Obiekty były wyposażone w zabezpieczenia przeciwpożarowe w postaci systemu sygnalizacji pożaru czy też instalację suchego gaszenia, jednak w krytycznym momencie nie zdały one egzaminu. Pożar okazał się niemożliwy do powstrzymania, trawiąc w ogniu tysiące dokumentów, w których znajdowały się zarówno sprawy z zakresu planowania przestrzennego, jak i przetargów miasta. Ocalałe archiwa zostaną prawdopodobnie przeniesione do trzeciej hali, która miała zostać odebrana do użytku w tym roku.



Samodzielność pod kontrolą

Wyzwania autonomicznych pojazdów

Jeszcze nie tak dawno wydawało się, że pojazdy poruszające się po drogach samodzielnie, bez udziału kierowcy, to wytwór wyobraźni twórców filmów science-fiction. Po wielu badaniach i testach wiemy, że auta o różnym stopniu autonomiczności na stałe wpiszą się w codzienny krajobraz. Z punktu widzenia złożoności i wpływu na szeroko rozumiane otoczenie mogą one stanowić kolejny krok milowy w rozwoju nowoczesnych społeczeństw, z idącymi za tym szansami i zagrożeniami.



Maria Dymek

Inżynier, absolwentka Wydziału Budowy Maszyn Politechniki Poznańskiej. W Grupie ERGO Hestia pracowała od 1999 r. do 2020 roku. Zajmowała się underwritingiem ubezpieczeń gospodarczych.

Wyścig rozpoczął się jakiś czas temu. Intensywne prace nad rozwojem AV (ang. autonomus vehicle) podjęły wiodące koncerny motoryzacyjne takie jak: General Motors, Mercedes-Benz, Audi, Renault, Nissan czy Toyota. Do wyścigu dołączają również firmy spoza branży jak np. Google oraz Nvidia – spółki specjalizujące się przede wszystkim w technologii obliczeniowej i graficznej. Zresztą postęp w tej dziedzinie nie jest możliwy bez ścisłej współpracy firm działających w różnych branżach, między innymi motoryzacyjnej, informatycznej czy telekomunikacyjnej.

Samodzielne, czyli jakie?

Wprawdzie na powszechne użytkowania samochodów w pełni autonomicznych przyjdzie nam jeszcze trochę poczekać, to jednak pewne elementy „samodzielności” są już dziś dostępne w pojazdach będących w sprzedaży. W zależności od zastosowanych rozwiązań wyróżnia się kilka poziomów automatyzacji – od najprostszej, określonej poziomem 1, do tej oznaczającej całkowitą autonomię pojazdu i określonej poziomem 5.

Na drogach publicznych powoli pojawiają się pojazdy autonomiczne spełniające wymogi poziomu 3 i 4. Jak przewidują specjaliści, na w pełni zautomatyzowane konstrukcje (stopień 5) w pełni zagospodzą na drogach około 2030 roku.

POZIOM „0” – BRAK AUTOMATYZACJI

Występuje w starszych lub niższej klasy autach, które w najbliższych latach będą powoli znikać z ulic. Pojazdy mogą być wyposażone w systemy zapobiegające blokowaniu kół, stabilizację toru jazdy czy tempomat, ale za każdy możliwy aspekt prowadzenia pojazdu odpowiedzialny jest kierowca.

POZIOM „1” – WSPOMAGANIE KIEROWCY

Pojazd może wspomagać kierowcę, przejąć kontrolę nad prędkością przy użyciu tempomatu lub kontrolować pozycję na drodze przy pomocy asystenta pasa ruchu. Potrafi samodzielnie przyspieszać i zwalniać – tak, aby dostosować prędkość do poprzedzającego pojazdu oraz utrzymać prosty tor jazdy. Kierowca musi cały czas monitorować pojazd oraz drogę i być gotowym do przejęcia kontroli w każdym momencie z rękami na kierownicy i stopami na lub obok pedałów.

POZIOM „2” – CZĘŚCIOWA AUTOMATYZACJA

Samochód przejmuje funkcję przyspieszenia / zwalniania, ale także sterowania kierownicą w określonych sytuacjach. Kierowca jest jednak zobowiązany stale obserwować sytuację na drodze i być gotowy do przejęcia kontroli nad pojazdem w każdym momencie.

POZIOM „3” – WARUNKOWA AUTOMATYZACJA

System obserwuje otoczenie i w określonych sytuacjach samodzielnie prowadzi pojazd. Monitoruje drogę oraz informuje kierowcę, kiedy powinien przejąć kontrolę. Człowiek zatem musi pozostawać przed kierownicą w gotowości do podjęcia działań.

POZIOM „4” – WYSOCE ZAAWANSOWANA AUTOMATYZACJA

Samochód jest wyposażony w sztuczną inteligencję, wspomagane jest przez system sensorów, radarów oraz kamer. Pojazd kontroluje wszystkie aspekty prowadzenia pojazdu.

Auto jest już praktycznie całkowicie autonomiczne. Człowiek wciąż ma jednak możliwość kierowania takim samochodem.

POZIOM „5” – PEŁNA AUTOMATYZACJA

Auto porusza się zupełnie samodzielnie w każdych możliwych warunkach. Nie posiada kierownicy i pedałów, a miejsce dla kierowcy jest zbędne. Jego samego może też w ogóle nie być wewnątrz pojazdu. Jedynym zadaniem ludzkiego kierowcy będzie wskazanie (choćby zdalnie) miejsca docelowego.



Również producenci samochodów ciężarowych Daimler, Volvo, Tesla czy Grupy Volkswagen upatrują w samojezdnym pojazdach potencjału dla rozwoju branży transportowej.

Pojazdy ciężarowe już dziś wyposażone są w szereg systemów wspomagających kierowcę takich jak: system automatycznego hamowania przed przeszkodą, aktywny tempomat, system ostrzegający przed kolizją, układ monitorujący martwą strefę, monitor zmęczenia kierowcy oraz wiele innych rozwiązań, które znamy z aut osobowych. Branża transportowa może się zatem okazać tą gałęzią motoryzacji, która stanie się głównym beneficjentem postępującej robotyzacji.

Auto o sokolim wzroku

Skąd samochody autonomiczne czerpią informacje potrzebne do bezkolizyjnego poruszania się? Otóż AV „widzi” otoczenie przy użyciu systemu sensorów. Są to:

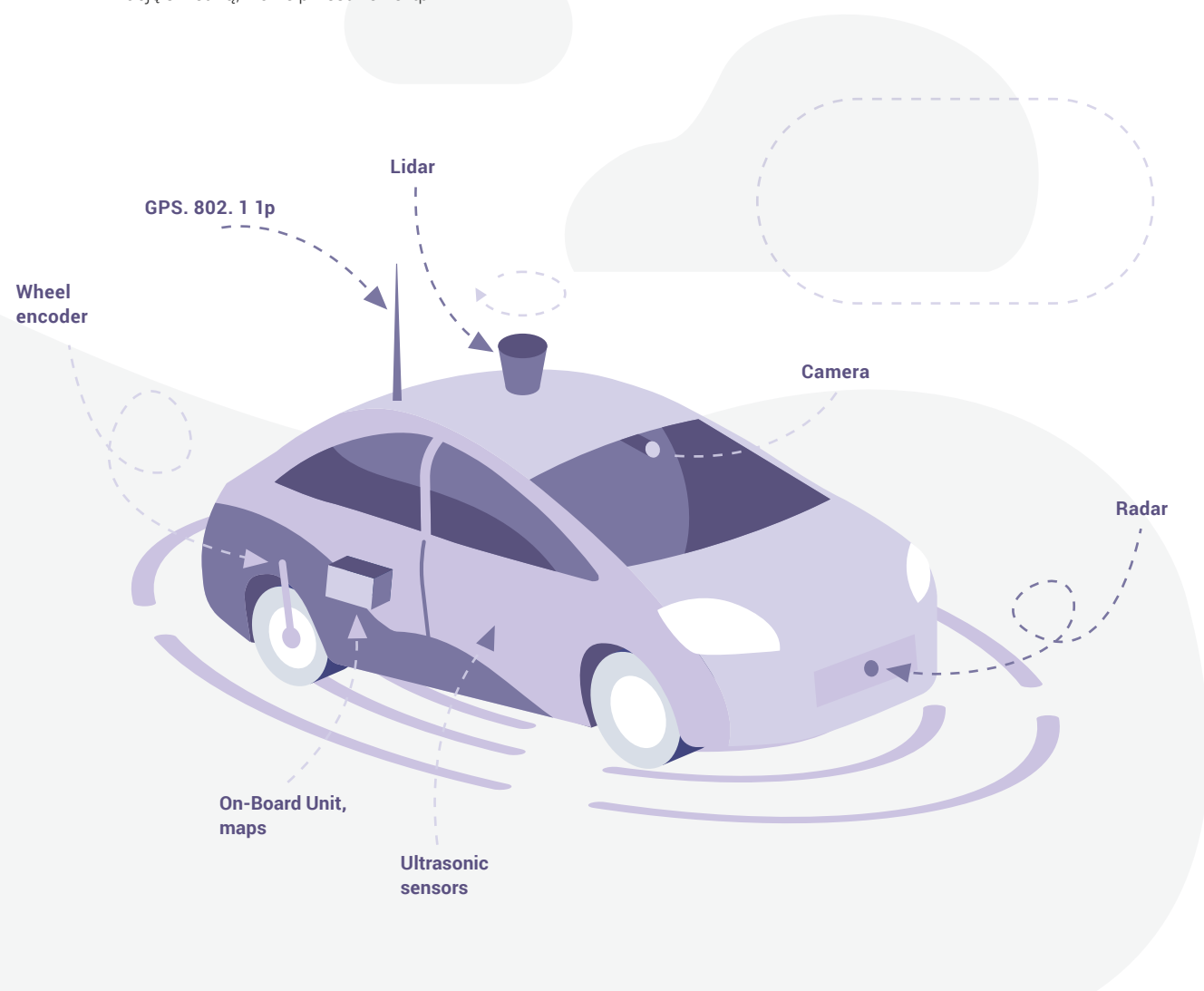
- lidary – wysokoczułe sensory laserowe, które wykrywają przedmioty nieruchome i poruszające się;
- radary – wykrywają przedmioty wokół pojazdu, rozpoznają poruszające się pojazdy z dużej odległości i w szerokim zakresie pola widzenia oraz mierzą ich prędkość;
- kamery – wykrywają i śledzą pieszych/rowerzystów, sygnalizację świetlną, wolne przestrzenie itp.

Sensory przekazują informacje do komputera, który łączy je z danymi map wysokiej rozdzielczości w celu lokalizacji pojazdu. Dzięki temu powstaje trójwymiarowy model otaczającego świata. System wykrywa i klasyfikuje przedmioty, określa ich położenie i dostosowuje prędkość oraz kierunek jazdy, a także przewiduje przyszły ruch pieszych, rowerzystów czy pojazdów. Znając lokalizację, system wie, gdzie szukać poruszających się obiektów. Kiedy widok jest zasłonięty, AV oznacza obszar jako nieznany. Z kolei jeśli z powodu deszczu lub mgły jest słaba widoczność, „mózg” maszyny odnotowuje to i dostosowuje proces podejmowania decyzji do sytuacji.

„Mniej” znaczy „więcej”

Jakich korzyści powinniśmy się spodziewać dzięki wprowadzeniu AV?

Do sprawnego działania wszystkich systemów pojazdy autonomiczne potrzebują znacznych ilości energii elektrycznej, a sprostac temu mogą pojazdy o napędzie elektrycznym lub hybrydowym. Co za tym idzie, ich użytkowanie powoduje znaczne zmniejszenie emisji szkodliwych substancji. Pozostaje jednak pytanie, z jakich źródeł będzie pozyskiwana energia potrzebna do ich zasilania.



Założeniem, które przyświeca twórcom AV, jest również dążenie do ograniczenia liczby wypadków, co oznacza zmniejszenie liczby zabitych i rannych. Przeciętnemu użytkownikowi dróg niełatwo pogodzić się z tym, że auto bez kierowcy jest bezpieczniejsze. Z pewnością jest wolne od ludzkich przywar. W stosunku do pojazdów autonomicznych nie trzeba będzie bowiem prowadzić społecznych kampanii takich jak „piłeś, nie jedź”. Możemy być również spokojni o to, że AV nie będzie pisać SMS-ów w czasie jazdy. Malkontenci ze szczególną uwagą śledzą wypadki z udziałem samochodów autonomicznych, ale ich zwolennicy przytaczają wyniki wielokrotnie powtarzanych badań, z których wynika, że za 90-95 proc. wypadków odpowiada kierowca, a nie technologia.

Brak zaufania do „samodzielnych” pojazdów może opóźnić ich upowszechnienie, ale korzyści finansowe z tego płynące z pewnością przechylą szalę na korzyść ich zwolenników.

Samochody autonomiczne zmieniają sposób funkcjonowania transportu drogowego, obniżając jego koszty poprzez między innymi ograniczenie zatrudnienia kierowców. W miarę zwiększającej się dostępności AV część osób może zrezygnować z posiadania własnego pojazdu, co przełoży się na znaczące oszczędności związane z utrzymaniem własnego auta.

Dzięki geolokalizacji AV będą mogły wybrać optymalną drogę, co sprawi, że ruch będzie bardziej płynny, a liczba zatorów na drogach zmaleje. Wreszcie AV mogą zmienić oblicze miast. Już dziś widać zmianę podejścia do korzystania z samochodów. Mieszkańcy coraz częściej korzystają z pojazdów współdzielonych i zaczynają je traktować jako jeden ze sposobów komunikacji miejskiej. Pozwoli to uwolnić wolne przestrzenie przeznaczone do tej pory na parkingi. Miasta mogłyby je wykorzystać na inne cele publiczne. Pojazdy autonomiczne mogą ten trend pogłębić. Samojeżdżące pojazdy pomogą również w mobilności tym, którzy do tej pory mieli ograniczony dostęp do transportu publicznego, a więc przykładowo osobom starszym czy niepełnosprawnym.

Mówię: „sprawdzam”

Zanim pojazdy w pełni autonomiczne będą użytkowane na szerszą skalę, muszą być przetestowane pod nadzorem człowieka siedzącego w środku lub przed monitorem komputera. Testy powinny odbywać się przy stosunkowo niewielkich odległościach i na krótkich dystansach. Na przykład Renault testuje pojazdy autonomiczne na terenie podparyskiego kampusu uniwersyteckiego. Użytkownicy, za pomocą aplikacji w telefonie, mogą zamawiać autonomiczne Renault ZOE jako taksówki (tzw. robotaxi) lub skorzystać z autobusu i-Cristal, który kursuje na razie tylko w nocy, gdy ruch na ulicach jest mniejszy. Maksymalna prędkość, z którą pojazd może się poruszać, to 30 km/h.

Pierwsze testy zostały przeprowadzone również w Polsce. Dla przykładu goście mogli odwiedzić jeden z polskich

W stosunku do pojazdów autonomicznych nie trzeba będzie prowadzić społecznych kampanii takich jak „piłeś, nie jedź”. Możemy być również spokojni o to, że AV nie będzie pisać sms-ów w czasie jazdy.

ogrodów zoologicznych za pomocą autonomicznego busa zabierającego na swój pokład do 12 osób. Wewnątrz nie było kierowcy, a pasażerom towarzyszył jedynie operator, którego zadaniem było czuwanie nad bezpieczeństwem podróży i reagowanie w razie nieprzewidzianych sytuacji, np. pojawienia się na drodze pieszego, innego pojazdu bądź zwierzęcia.

Przewiduje się, że AV znajdą zastosowanie podczas wykonywania czynności przy niewielkich prędkościach jako specjalistyczne pojazdy wykorzystywane w usługach komunalnych (śmieciarki, zmiatarki i inne) lub służące do przemieszczania ładunków po placach manewrowych.

Ala sprawne poruszanie się pojazdów to nie wszystko. Potrzebna jest do tego infrastruktura drogowa przystosowana do poruszania się po niej nie tylko pojazdów osobowych. Zakłada się, że ciężarówki będą mogły poruszać się przede wszystkim po autostradach, gdzie będzie można spotkać tzw. autonomiczne konwoje (platooning). Trzeba będzie zatem zapewnić możliwość porozumiewania się ze sobą pojazdów, co wymaga zaawansowanych technologii łączności takich jak sieć 5G. Miejscem, gdzie mogą zostać przetestowane autonomiczne ciężarówki, będą portowe terminale kontenerowe.

Kto pyta, nie błądzi

„Bezzałogowa” mobilność obiecuje wiele korzyści, ale stawia również wiele poważnych pytań. Regulacji wymaga wiele aspektów takich jak:

- przeprowadzanie testów – należy określić, gdzie i kiedy mogą być prowadzone testy, ile godzin testów powinien przejść AV oraz w jaki sposób powinny być zbierane i przekazywane dane;
- zarządzanie danymi – na każdym etapie użytkowania AV zbierana jest duża liczba danych. Powstaje pytanie, jak je chronić i kto powinien mieć do nich dostęp, i na jakich zasadach;



Pierwsze testy zostały przeprowadzone również w Polsce. Dla przykładu goście mogli odwiedzić jeden z polskich ogrodów zoologicznych za pomocą autonomicznego busa zabierającego swój pokład do 12 osób.

- certyfikacja i licencje – należy określić standardy bezpieczeństwa, jakie powinny spełniać AV, aby mogły zostać dopuszczone do ruchu, i w jaki sposób powinna być prowadzona ich kontrola;
- rejestracja pojazdów – jak AV powinny być oznakowane i jakie informacje nt. autonomiczności powinny zawierać dowody rejestracyjne?
- uprawnienia kierowców – jakie umiejętności i uprawnienia powinny posiadać kierowcy i operatorzy pojazdów na różnych poziomach autonomiczności?
- cyberbezpieczeństwo – należy zapewnić bezpieczeństwo wszystkich systemów kontrolnych pojazdów, usług powiązanych z AV i mobilnych aplikacji służących ich użytkownikom;
- edukacja i szkolenie konsumentów – użytkownicy będą musieli otrzymać informacje, jak identyfikować AV oraz czego można się spodziewać w trakcie jazdy i po jej zakończeniu.

Skret w prawo

Powszechne wprowadzenie pojazdów autonomicznych na ulice miast wymaga wypracowania i wejścia w życie wielu regulacji prawnych, w tym tych dotyczących odpowiedzialności za zdarzenia z ich udziałem. Mimo postępu technologicznego i nasilającej się dyskusji na temat samojeżdżących aut, żadne państwo na świecie nie jest jeszcze w pełni gotowe pod względem legislacyjnym na to rozwiązanie. Jeśli chodzi o Unię Europejską, poszczególne państwa kreują mniej lub bardziej kompleksowe rozwiązania, ale prawdziwy postęp

w tej dziedzinie wymaga zharmonizowania szeregu przepisów ruchu drogowego oraz wymogów bezpieczeństwa we wszystkich krajach członkowskich. Intensywne prace w tym zakresie prowadzi Komisja Europejska.

Z pewnością znacznym ułatwieniem w rozwoju autonomicznych maszyn byłoby wdrożenie prawa cywilnego dotyczącego robotyki, które jest przedmiotem rezolucji Parlamentu Europejskiego. W najbliższym czasie spodziewane są unijne regulacje dotyczące kwestii odpowiedzialności w razie wypadku, naruszenia ochrony danych i cyberbezpieczeństwa.

Faktyczna przyczyna szkody jest decydująca dla przypisania odpowiedzialności za zdarzenie właściwemu podmiotowi. Z tego względu proponuje się, aby pojazdy autonomiczne były wyposażone w rejestratory danych w celu wyjaśnienia, czy pojazd w momencie wypadku działał w trybie autonomicznym, czy z udziałem kierowcy. Ale to nie wszystko. Niezbędne jest również rozstrzygnięcie, w jaki sposób odpowiedzialność przypisana do pojazdu powinna być podzielona pomiędzy poszczególne podmioty biorące udział w produkcji i procesach związanych z funkcjonowaniem pojazdów autonomicznych, a mianowicie:

- właściciela/użytkownika AV,
- producenta,
- programistę/podwykonawcę,
- dostawcę usług transportowych,
- dostawcę internetu.

Gdy w wypadku drogowym brać będą zarówno pojazdy tradycyjne, jak i autonomiczne, kwestie prawne staną się bardziej skomplikowane i trudne do przewidzenia.

Regulacje prawne związane z projektowaniem, wdrażaniem i użytkowaniem pojazdów autonomicznych będą miały zasadniczy wpływ na branżę ubezpieczeniową. Ubezpieczyciele będą musieli uwzględnić nowe realia funkcjonowania komunikacji samochodowej oraz wyjść naprzeciw oczekiwaniom zarówno producentów, jak i użytkowników AV. W tym kontekście niezwykle istotne są zwłaszcza przepisy dotyczące zasad określania odpowiedzialności cywilnej w przypadku zdarzeń z udziałem samochodów autonomicznych, odpowiedzialności za produkt oraz przepisy ruchu drogowego.

Nowe regulacje nie pozostaną bez wpływu, zwłaszcza na obowiązkowe ubezpieczenie odpowiedzialności cywilnej posiadaczy pojazdów mechanicznych, ale mogą również przyczynić się do powstania produktów ubezpieczeniowych dedykowanych szeroko pojętej branży pojazdów autonomicznych. Wątpliwości towarzyszące wprowadzeniu w 2018 r. nowych przepisów w Prawie o ruchu drogowym i dotyczące kwestii przeprowadzania testów AV na drogach publicznych pokazują, że nie będzie to łatwy proces. Przewidują one, że do wniosku o wydanie zezwolenia na ich przeprowadzanie organizator prac badawczych dołączać będzie „dokument potwierdzający zawarcie umowy obowiązkowego ubezpieczenia odpowiedzialności cywilnej organizatora prac badawczych za szkody powstałe w związku z prowadzeniem prac badawczych związanych z prowadzeniem pojazdów autonomicznych, która wchodzi w życie w przypadku uzyskania pozwolenia na prowadzenie prac badawczych”. Aż tyle i tylko tyle, ponieważ brak jakichkolwiek przepisów wykonawczych do tak określonego ubezpieczenia.

Warto, aby legislatorzy stanowili prawo ubezpieczeniowe przy udziale przedstawicieli branży. W przeciwnym razie przepisy, zamiast ułatwiać wrażliwe zaawansowanych technologicznie środków transportu, będą je spowalniały.

„Warto być przyzwoitym... robotem”

Jest jeszcze jedno, być może fundamentalne pytanie: jak normy etyczne przełożyć na algorytmy? Jak roboty mogą decydować, w jaki sposób przestrzegać prawa, dzielić ryzyko i minimalizować straty w sytuacjach moralnie niejednoznacznych? „Samodzielne” pojazdy będą reagować na zdarzenia na drodze wg schematów, które zostaną zapisane w oprogramowaniu. Nie obędzie się bez poważnych dyskusji na tematy etyczne. Specjaliści będą musieli zastanowić się nad tego typu dylematami:

- jaki powinien zachować się AV, jeśli musi dokonać wyboru pomiędzy uszkodzeniem swojego błotnika a uderzeniem w pojazd kierowany przez człowieka?

- gdy na drogę wybiegnie dziecko, czy AV powinien przekroczyć w celu jego ominięcia podwójną linię ciągłą i pod jakimi warunkami?
- jakie jest właściwe działanie w sytuacji, gdy AV musi dokonać wyboru pomiędzy uderzeniem w przeszkodę i narażeniem życia pasażerów, a nagłym skretem, ominięciem przeszkody i wpadnięciem na ludzi stojących na przystanku?

Konieczność rozwiązywania takich kwestii powoduje, że proces powszechnego wdrażania pojazdów autonomicznych staje się bardzo złożony. Mimo wielu niewiadomych nie ma od niego odwrotu. Należy mieć jednak nadzieję, że zarówno ludzie, jak i roboty zdadzą w tym przypadku test na inteligencję.

Regulacje prawne związane z projektowaniem, wdrażaniem i użytkowaniem pojazdów autonomicznych będą miały zasadniczy wpływ na branżę ubezpieczeniową.



Palące problemy branży spożywczej

Artykuły spożywcze to produkty pierwszej potrzeby. Ich produkcja kojarzy się z bukietem smaków i zapachów oraz sterylnymi warunkami pracy. To nie kopalnie czy huty, gdzie zagrożenia „widać jak na dłoni”. W tej branży wszystko jest dokładnie zaplanowane – przyjęcie surowca, organizacja procesu produkcji, pakowanie i wysyłka wyrobów do odbiorców. I choć teoretycznie nie ma miejsca na błędy, czy awarie, to te jednak się zdarzają.



Paweł Michalski

Zastępca Dyrektora Przedstawicielstwa Korporacyjnego w Warszawie. Zajmuje się nadzorowaniem i likwidacją szkód majątkowych. Absolwent Wydziału Pedagogicznego Uniwersytetu Warszawskiego. W Grupie ERGO Hestia od 1999 r.

Ogień w chłodni

„Polska jabłkiem stoi”, o czym świadczy krajobraz zagłębia sadowniczego w okolicach Grójca. Widać tam hale z płyty warstwowej, często w kształcie litery L ze „skrzydłem”, w którym znajdują się chłodnie oraz „doklejony” budynek biurowy, a na zewnątrz setki zielonych skrzyniopalet. Wewnątrz, na parterze, znajdziemy jedną czy dwie linie do mycia i sortowania owoców, a na antresoli – magazyn opakowań. Jesienią okoliczni sadownicy sprzedają swoje plony, które potem są sortowane i przechowywane w chłodniach do dalszej sprzedaży w okresie zimowo-wiosennym.

Sortownie owoców to przedsiębiorstwa/firmy o wartości kilkunastu milionów złotych. Wyrobem gotowym są starannie umyte i przechowywane do transportu jabłka. W prowadzonym procesie produkcyjnym brakuje czynników inicjujących ogień – są tu duże ilości wody i wysoka wilgotność powietrza. Można by przypuszczać, że ryzyko pożarowe jest małe. A jednak wystarczyło zwarcie w instalacji elektrycznej, aby sortownia wraz z przechowalnią owoców błyskawicznie zamieniły się w tłaczę zgliszczą.

Do zdarzenia doszło w piątkowy wieczór, około godziny 22.00. Pożar powstał na poziomie antresoli, na której magazynowane były opakowania. Ogień błyskawicznie zajął część magazynową, kolejno rozprzestrzeniając się na parter, gdzie znajdowały się linie produkcyjne oraz pozostałe mienia w postaci wyposażenia i wózków widłowych. Następnie płomień przedostał się do chłodni wysokiego składowania służącej do magazynowania jabłek. Hala sortowni spłonęła doszczętnie w ciągu kilkunastu minut, na oczach pracowników i właścicieli, którzy przybyli na miejsce zdarzenia. Straty oszacowano na 70 mln złotych.

Nowoczesne sortownie owoców i warzyw to specjalistyczne zakłady z rozbudowanym parkiem maszynowym. Zainstalowane tam urządzenia wyposażone są w szereg elementów mogących być potencjalną przyczyną pożaru, np. rozdzielnice elektryczne, elementy zasilania i sterowania, taśmociągi. W magazynach znajduje się też zazwyczaj znaczna liczba łatwopalnych opakowań. W przypadku zwarcia elektrycznego może powstać trudny do opanowania pożar, który doprowadzi do całkowitego zniszczenia zakładu. Dlatego bardzo ważne jest prowadzenie cyklicznych pomiarów

Sektor spożywczy jest jedną z najważniejszych i najszybciej rosnących gałęzi polskiej gospodarki. Zatrudnia ok. 10,5% wszystkich pracowników zatrudnionych w przetwórstwie mięsa, mleka, płatków zbożowych, owoców i warzyw, wyrobów alkoholowych, tytoniu i innych produktów spożywczych. Polska jest szóstym największym rynkiem w Europie, dlatego na terenie naszego kraju rozwija swoją działalność szereg znanych światowych marek.

Niemal w każdym powiecie znajdują się zakłady spożywcze, będące często chlubą lokalnych społeczności. Miejsca te zapewniają ludziom pracę, inwestują w lokalne przedsięwzięcia, sponsorują różne wydarzenia. Mimo posiadanych przez nie certyfikatów i standardów, takich jak ISO 9001, ISO 14000 czy HACCAP, oraz stosowania środków prewencji i procedur bezpieczeństwa, czasami dochodzi tam również do dotkliwych szkód.



instalacji elektrycznej oraz oddzielenie magazynu opakowań od części produkcyjnej.

Zadymienie w fabryce słodkości

Pożar pojawił się w godzinach porannych, w pomieszczeniu sprężarkowni na terenie zakładu produkującego słodycze. Zainstalowany w obiekcie system sygnalizacji pożaru powiadomił straż pożarną. Po chwili uruchomiła się również instalacja tryskaczowa. Pożar został szybko zlokalizowany, a jego rozwój ograniczony. Na miejsce przyjechały jednostki straży pożarnej, które podjęły działania gaśnicze, ewakuując jednocześnie pracowników z zagrożonego obiektu. Po zakończeniu akcji ratowniczo-gaśniczej, pracownicy rozpoczęli oczyszczanie i osuszanie miejsca zdarzenia. Jak wykazało późniejsze dochodzenie, pożar powstał z powodu zatarcia wirnika wentylatora elektrycznego w dmuchawie do transportu serwatki. W jego wyniku zniszczona została jedna ze sprężarek, linie zasilające, instalacja

cja wyprowadzania sprężonego powietrza do zasypu oraz surowce w pobliskim magazynie. Toksyczne produkty spalania spowodowały bezpośrednie zanieczyszczenie sprężarkowni i pomieszczeń sąsiednich, w tym pomieszczenia przejściowego i zasypów oraz korytarza w strefie magazynu surowca.

Dym przedostał się instalacją przesyłu pneumatycznego na urządzenia i instalacje technologiczne oraz zasobniki, powodując dodatkowe straty w środkach obrotowych, takich jak mleko pełne i odtłuszczone, cukier, serwatka i kakao. Opróżnione ze „skażonej” produkcji instalacje zostały oczyszczone poprzez przepuszczenie przez nie pełnowartościowego cukru, który w związku z tym również został zanieczyszczony. Pożar spowodował 16-godzinny przestój w produkcji.

Prowadzenie produkcji wyrobów spożywczych wymaga zachowania bardzo surowych standardów sanitarnych. W przypadku wystąpienia awarii maszyny lub jej pożaru skutki zdarze-



Działanie wilgoci, oprócz pożaru i zadymienia, stanowi drugie największe zagrożenie dla środków obrotowych w zakładach przemysłu spożywczego

Duża ilość środków obrotowych przechowywanych w jednym miejscu przyczyniła się do znaczącej szkody majątkowej. W opisywanym przypadku jej wartość wyniosła kilkaset tysięcy złotych. Ponadto, doprowadzenie magazynu do stanu sprzed szkody wymagało kilkudniowego przestoju w produkcji i magazynowaniu, co zakłóciło płynność dostaw.

Działanie wilgoci, oprócz pożaru i zadymienia, stanowi drugie największe zagrożenie dla środków obrotowych w zakładach przemysłu spożywczego. Konieczność spełnienia wysokich reżimów jakościowych produktów powoduje, że zmiana wilgotności mienia, a tym bardziej jego zalanie, rodzi konieczność jego utylizacji. Regularne dokonywanie przeglądów instalacji wodociągowej może zatem uchronić przed olbrzymimi stratami.

Amoniak – zbawienny i groźny

W jednym z zakładów mięsnych doszło do rozszczelnienia instalacji chłodniczej i wycieku amoniaku, gazu o właściwościach wybuchowych i toksycznych. Zainstalowany w budynku produkcyjno-magazynowym system detekcji gazu wykrył zagrożenie. Dzięki temu podjęto szybką ewakuację oraz działania ograniczające wyciek niebezpiecznej substancji. Zabezpieczeniem miejsca zdarzenia i neutralizacją amoniaku zajęły się przybyłe na miejsce jednostki Państwowej Straży Pożarnej. Na szczęście nie doszło do wybuchu, ale kilku pracowników wskutek podtrucia amoniakiem zostało przewiezionych do szpitali.

Z powodu wycieku produkcja została wstrzymana na kilka dni. Skażeniu uległo kilkaset ton mięsa i przetworów mięsnych, przechowywanych w chłodniach, komorach szokowych i głębokiego mrożenia. Całość skażonego mienia skierowano do utylizacji. Wartość szkody, wraz z kosztami wywozu i utylizacji, została oszacowana na ok. 7 mln złotych.

Amoniak to kolejny czynnik ryzyka, charakterystyczny dla branży spożywczej, szczególnie w zakładach przetwórstwa mięsnego. Jest powszechnie używany w instalacjach chłodniczych. Ze względu na jego toksyczność instalacja amoniakalna powinna być szczególnie nadzorowana przez służby techniczne zakładu.

Wadliwa dezynfekcja

W jednym z browarów, w partii gotowego do sprzedaży trunku stwierdzono obecność drożdży szlachetnych. W ocenie działu kontroli jakości

nia nie ograniczają się do kosztu jej wymiany czy naprawy. Znacznie wyższe straty wynikają z konieczności oczyszczenia zakładu, usunięcia produktów spalania, odkażania i doprowadzenia do ponownego spełnienia wymogów sanitarnych. Stąd konieczność poniesienia ww. kosztów, typowa dla przemysłu spożywczego.

Makaron i mąka nie lubią wody

Do zdarzenia doszło w magazynie zakładu produkującego mąkę i makaron, w którym mieścił się magazyn wyrobów gotowych. Z powodu rozszczelnienia instalacji wodociągowej doszło do zalania kilkuset palet z mąką i makaronami, oczekujących na transport do kontrahentów. Zapakowana w papierowe torby mąka została całkowicie zniszczona, natomiast dużą partię makaronu w opakowaniach foliowych zakwalifikowano jako pełnowartościowy produkt skierowany do sprzedaży.



piwo to było niezgodne z normą zakładową i nie mogło zostać dopuszczone do sprzedaży. Drożdże szlachetne nie powinny znajdować się w produkcie gotowym, są one eliminowane na etapie końcowej filtracji piwa, przed rozlewem.

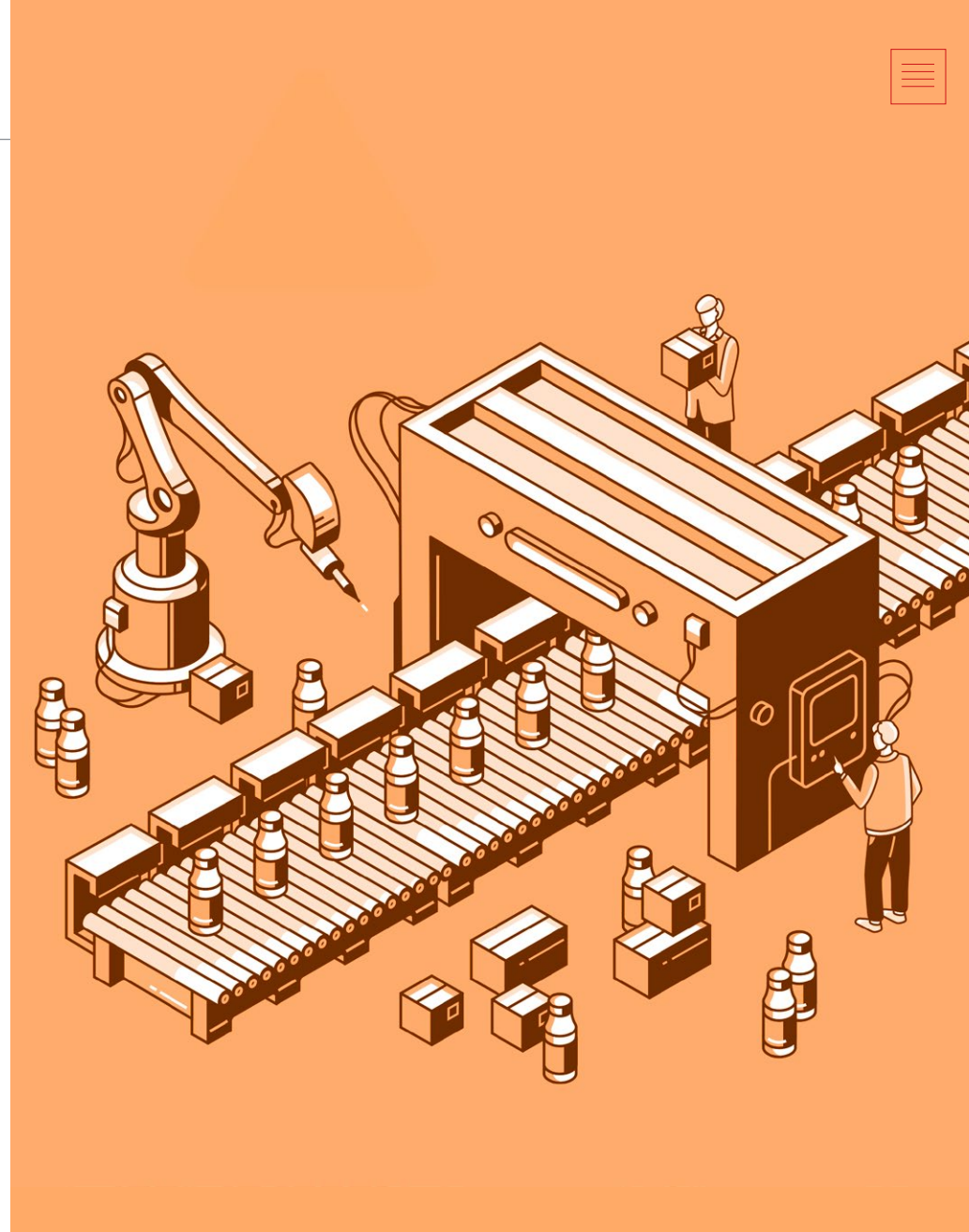
Produkcję wstrzymano i przeprowadzono szczegółowe dochodzenie przyczyn tego zdarzenia. Okazało się, że drożdże nie zostały całkowicie wyeliminowane z powodu uszkodzeń powierzchni filtrów świecowych, stosowanych w procesie filtrowania piwa. Dalsza analiza pozwoliła na znalezienie pierwotnej przyczyny – powierzchnie filtrów zostały uszkodzone przez środki chemiczne użyte podczas dezynfekcji linii produkcyjnej. W wyniku tego incydentu zanieczyszczeniu uległo piwo w puszkach (8,5 tys. zgrzewek) oraz butelkach (prawie 7 tys. skrzynek) o łącznej wartości ok. 200 tys. zł.

W przypadku wystąpienia awarii maszyny lub jej pożaru skutki zdarzenia nie ograniczają się do kosztu jej wymiany czy naprawy. Znacznie wyższe straty wynikają z konieczności oczyszczenia zakładu, usunięcia produktów spalania, odkażania i doprowadzenia do ponownego spełnienia wymogów sanitarnych.

W przypadku skomplikowanych linii produkcyjnych nieprawidłowe działanie pojedynczego urządzenia czy elementu może być trudne do szybkiej identyfikacji. Bardzo często ujawnienie wszelkiego rodzaju wad następuje dopiero na etapie kontroli parametrów gotowego produktu, a to skutkuje poważnymi kosztami związanymi z koniecznością utylizacji czy wycofaniem z rynku dużych partii wyrobów.

Badania ponad wszystko

Zakład produkcyjny zajmujący się przetwórstwem drobiu, wołowiny i wieprzowiny zakupił od kwalifikowanego dostawcy 8,5 ton mrożonych ćwierćtuszy wołowych o łącznej wartości 110 000 zł. Po przetworzeniu części zakupionego mięsa, gotowe wyroby trafiły na rynek.



Nowoczesne sortownie owoców i warzyw to specjalistyczne zakłady z rozbudowanym parkiem maszynowym. Zainstalowane tam urządzenia wyposażone są w szereg elementów mogących być potencjalną przyczyną pożaru.



Przeprowadzona w międzyczasie kontrola Inspekcji Weterynaryjnej Powiatowego Lekarza Weterynarii wykazała, że duża partia zakupionego przez zakład mięsa nie była poddana wymaganiom badaniom. Producent zdecydował się na natychmiastowe wycofanie wyrobów z rynku. Koszty związane z transportem i utylizacją przetworów mięsnych wyniosły ok. 75 000 zł. Na dodatkowe straty finansowe wpłynęły koszty zakupionego surowca (niepełniającego wymogów) oraz koszty produkcji.

Tak więc utrata wizerunku i osłabienie marki to kolejne konsekwencje zdarzenia, szczególnie istotne w branży spożywczej.

Konieczność badania mięsa na obecność pasożytów wynika z obowiązujących przepisów prawa. Zdarzają się jednak sytuacje, gdy dopiero po wytworzeniu znacznej partii towaru wytwórca otrzymuje wynik badania wskazujący na obecność pasożytów. W przypadku wykorzystania do produkcji mięsa niepoddanego badaniu lub z wynikiem badania wskazującym na występowanie włośni, zachodzi konieczność utylizacji całego wytworzonego produktu. Prawidłowe procedury w zakładzie powinny minimalizować ryzyko strat wynikających z wykorzystania niebadanego lub zainfekowanego paszytą mięsa.

Prewencja i ubezpieczenie

Można w nieskończoność mnożyć przykłady zdarzeń szkodowych w zakładach sektora spożywczego. Charakteryzują się one dużą różnorodnością oraz dotkliwymi konsekwencjami, nawet w przypadku małych szkód materialnych. Szczególną uwagę należy zwrócić na odpowiedzialność cywilną producentów za swoje wyroby. Roszczenia osób poszkodowanych przez produkt i/lub koszty wycofania z rynku mogą być ogromne, co może wpłynąć negatywnie na wizerunek firmy oraz jej sytuację finansową.

Biorąc pod uwagę dużą wartość majątku, jego kumulację, często w ramach jednego kompleksu produkcyjno-magazynowego zbudowanego w konstrukcji stalowej z płyt warstwowych, zakłady spożywcze są szczególnie wyeksponowane na różnego rodzaju ryzyka. Dlatego wymagają stosowania adekwatnych względem zagrożeń środków prewencji i rozbudowanych programów ubezpieczeniowych. Szkody występowały i nadal będą występować, warto jednak wyciągać z nich lekcje na przyszłość.

(Nie)bezpieczne składowiska odpadów



W powszechnej opinii składowiska odpadów są kojarzone jako tykające „bomby ekologiczne”. Największym zagrożeniem mogą być pochodzące z nich odcieki, które po przedostaniu się do wód i gleby wywierają negatywny wpływ na ludzi i środowisko. Dzięki współczesnym technologiom istnieją jednak metody pozwalające utrzymać to zagrożenie w ryzach i monitorować zjawiska zachodzące w samym składowisku.



Szczepan Bujwid

Inżynier ds. Oceny Ryzyka, zajmuje się oceną ryzyka ubezpieczeniowego w zakresie wpływu przedsiębiorstw na środowisko naturalne, szkód wyrządzonych w środowisku, gospodarki odpadowej. Absolwent kierunku Ochrona Środowiska na Uniwersytecie Warmińsko - Mazurskim w Olsztynie.

Odpady towarzyszą nam od zawsze. Pierwotnie znaczną większość nieczystości stanowiły łatwo rozkładające się odpady organiczne. Ludy koczownicze zostawiały po sobie przede wszystkim popiół z ognisk, odchody, resztki żywności oraz proste przedmioty nienadające się już do użytku. Problem zaczął narastać wraz z powstaniem pierwszych skupisk ludzkich. Gromadzone w ich obrębie odpady stanowiły źródło nieprzyjemnego zapachu oraz zanieczyszczeń sprzyjających rozwojowi chorób.

Pierwsze wysypiska śmieci istniały już 5 tysięcy lat temu na Krecie. Ze względu na swoją trwałość, stanowią obecnie cenne stanowiska archeologiczne obrazujące życie ówczesnych mieszkańców wyspy. Starożytni Ateńczycy wymyślili na przykład, że śmieci wywożone poza miasta są mniej uciążliwe. Nakazali więc lokowanie wysypisk w odległości co najmniej 1,5 kilometra od murów miejskich. W czternastowiecznym Paryżu góra odpadów usypana samowolnie przez mieszkańców dorównywała wysokością bramie wjazdowej do miasta, a o wiele większa

ich masa zalegała na ulicach. Konieczne było wprowadzenie regulacji prawnych, które skutecznie ograniczałyby zaśmiecanie miasta.

Z biegiem czasu pojawiły się nowe formy składowania odpadów oraz ich przetwarzania. Pomysł recyklingu i sortowania odpadów zawdzięczamy Japończykom, którzy już w X wieku potrafili przetwarzać makulaturę na papier. Nowoczesny system recyklingu powstał pod koniec dziewiętnastego wieku w Nowym Jorku, podobnie jak pierwsza na świecie spalarnia odpadów w brytyjskim Nottingham.

Odpady do zagłady

Dzisiaj, zgodnie z dyrektywą, 2008/98/WE odpadem jest określana „każda substancja lub przedmiot, których posiadacz pozbysza się, zamierza się pozbyć, lub do których pozbycia został zobowiązany”. Zbędne materiały i przedmioty powinny być zagospodarowane w sposób niezagrożący ludziom i środowisku naturalnemu. W przypadku odpadów przeprowadza się unieszkodliwienie polegające na poddaniu ich procesom fizycznym, biologicznym lub chemicznym. Najczęściej spotykanymi formami ich unieszkodliwiania są: składowanie, spalanie, recykling i kompostowanie.

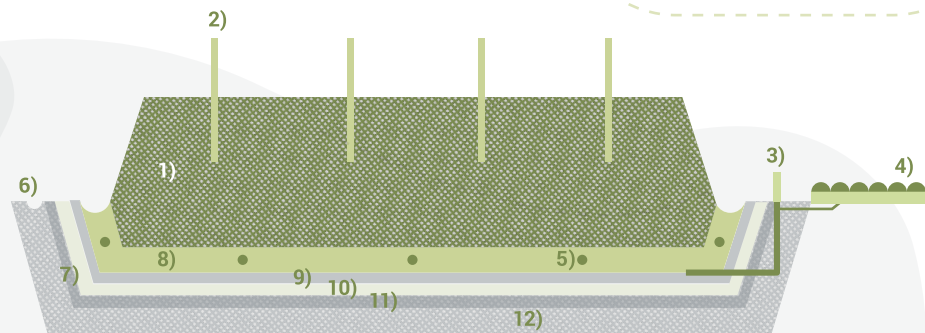
Niestety nieumiejętne gospodarowanie odpadami może bezpośrednio lub pośrednio wpłynąć na zanieczyszczenie powietrza, wody i gleby, co w konsekwencji może doprowadzić do zagrożenia dla życia i zdrowia ludzi. Dlatego też polityka Unii Europejskiej w tym zakresie zmierza do ograniczenia wpływu odpadów na środowisko naturalne i zdrowie oraz do poprawy efektywnego użytkowania zasobów. Długoterminowym celem tej polityki jest zmniejszenie ilości wytwarzanych odpadów, a jeśli ich wytwarzanie jest nieuniknione, promowanie ich wykorzystania jako zasobów, szersze upowszechnienie recyklingu i zapewnienie bezpiecznego unieszkodliwiania odpadów.

Biorąc pod uwagę skalę zjawiska, jest to wyjątkowo trudne, tym bardziej że wraz ze wzrostem konsumpcji ilość odpadów komunalnych ciągle rośnie. W 2017 roku było to około 12 milionów ton, to aż 310 kilogramów przypadających na każdego mieszkańca Polski.

Obecnie, w myśl hierarchii gospodarowania odpadami, najlepszym rozwiązaniem jest zapobieganie powstawaniu odpadów, a kolejne miejsca w przyjętym modelu zajmują odpowiednio: ponowne ich użycie, recykling materiałowy oraz odzysk energii w wyniku np. spalania.

KWATERA SKŁADOWA:

- | | |
|--|--|
| 1) Odpady | 9) Geowłóknina |
| 2) Studnie odgazowujące | 10) Syntetyczna warstwa uszczelniająca: geomembrana B= 2mm |
| 3) Pompownia | 11) Sztuczna bariera geologiczna |
| 4) Podczyszczalnia odcieków | Współczynnik filtracji |
| 5) instalacja odprowadzająca odcieki do podczyszczalni | $K < 1,0 \times 10^{-9} \text{ m/s}$ |
| 6) Rów opaskowy | miąższość 0,5m |
| 7) Obwałowanie | 12) Grunt rodzimy – glina |
| 8) Podsypka: żwir 16/32 | |
| Przewody drenarskie DN250 | |
| Warstwa drenażowa | |
| Współczynnik filtracji | |
| $K > 1,0 \times 10^{-4} \text{ m/s}$ | |
| miąższość 0,5m | |

**Wszechobecne składowiska odpadów**

Składowanie odpadów m.in. komunalnych polega na bezpiecznym lokowaniu ich w specjalnie przygotowanych do tego celu miejscach, czyli tak zwanych kwaterach. Składowiska odpadów komunalnych obsługują regiony gospodarowania odpadami, które swoim zasięgiem mogą obejmować miasta, gminy, powiaty, ale też całe ich grupy. Zazwyczaj składowaniu poddawane są odpady bytowe, gospodarcze, wielkogabarytowe, żużel i popiół, gruz budowlany oraz odpady przemysłowe o charakterze komunalnym.

Składowanie jest najtańszą i najbardziej powszechną formą unieszkodliwiania odpadów. Prawie połowa wszystkich wytwarzanych odpadów trafia na składowiska. W przyszłości powinny tam trafiać jedynie odpady, które nie mogą zostać poddane innym metodom unieszkodliwiania lub pozostałości po kompostowaniu i spalaniu. Składowiska staną się jedynie

uzupełnieniem bardziej ekologicznych form gospodarowania odpadami.

Składowanie, w przeciwieństwie do magazynowania, które jest rozwiązaniem tymczasowym, ma na celu trwałe unieszkodliwianie odpadów.

Pożar się nie opłaca

Większość osób nie dostrzega istotnych różnic pomiędzy punktem selektywnej zbiórki odpadów komunalnych (PSZOK), magazynem, instalacją do ich przetwarzania, składowiskiem czy też zwykłym wysypiskiem śmieci usypanym gdzieś na uboczu. Są to różne obiekty, często różne ryzyka, ale łączy je jedno – w każdym z nich może dojść do pożaru skutkującego poważną emisją zanieczyszczeń do atmosfery. Jak pokazują statystyki, do głównych przyczyn pożaru odpadów należy zaliczyć nieumyślne zaproszenie ognia,

samozapalenie oraz celowe podpalenia, do których dochodzi zazwyczaj w miejscach magazynowania odpadów oraz na nielegalnych wysypiskach. Składowiska, PSZOK-i i legalnie funkcjonujące instalacje znacznie rzadziej są ofiarami podpałów, gdyż jak pokazuje praktyka celowe spalanie zdeponowanych na składowisku odpadów jest nieopłacalne i wiąże się z dodatkową odpowiedzialnością administracyjną.

Sącząca się trucizna

Pożary, wbrew medialnym doniesieniom, nie są najpoważniejszym zagrożeniem dla środowiska ze strony składowisk odpadów komunalnych. Są nim szkodliwe substancje zawarte w odciekach, które w niekontrolowany sposób mogą zanieczyszczać wodę oraz glebę. Objawem pogorszenia się stanu wody jest jej zmętnienie oraz zmiana koloru. Nieprzyjemny zapach wywołany procesami gnilnymi, które zachodzą w zanieczyszczonej wodzie, często rozchodzi się po okolicy. Woda ta, w zależności od rodzaju i właściwości składowanych odpadów, może zawierać: związki siarki i azotu, oleje mineralne, związki metali ciężkich lub mikroorganizmy.

Procesy zachodzące na składowisku odpadów komunalnych powodują powstanie takich gazów cieplarnianych jak na przykład dwutlenek węgla, siarkowodór i metan. Jako dodatkowe uciążliwości, wpływające zwłaszcza na okolicznych mieszkańców, należy zaliczyć rozwiewane po okolicy lekkie odpady np. opakowania foliowe i papierowe, a także hałas eksploatacyjny, który jest związany z transportem odpadów. Ogólne pogorszenie walorów krajobrazowych stanowi uzupełnienie katalogu niedogodności wynikających z lokalizacji składowiska.

Zagrożenie odciekami występuje również na niektórych składowiskach odpadów niebezpiecznych. Odpady niebezpieczne to substancje szkodliwe, które stwarzają bezpośrednie zagrożenie dla życia ludzi oraz dla środowiska. Ten rodzaj składowisk cechuje się podwyższonym poziomem nadzoru i ochrony. Stosunkowo najbardziej bezpieczne, z punktu widzenia ochrony środowiska, są składowiska odpadów obojętnych, czyli takich jak stałe odpady mineralne i budowlane, w tym ziemia z wykopów, która zgodnie z prawem stanowi odpad.

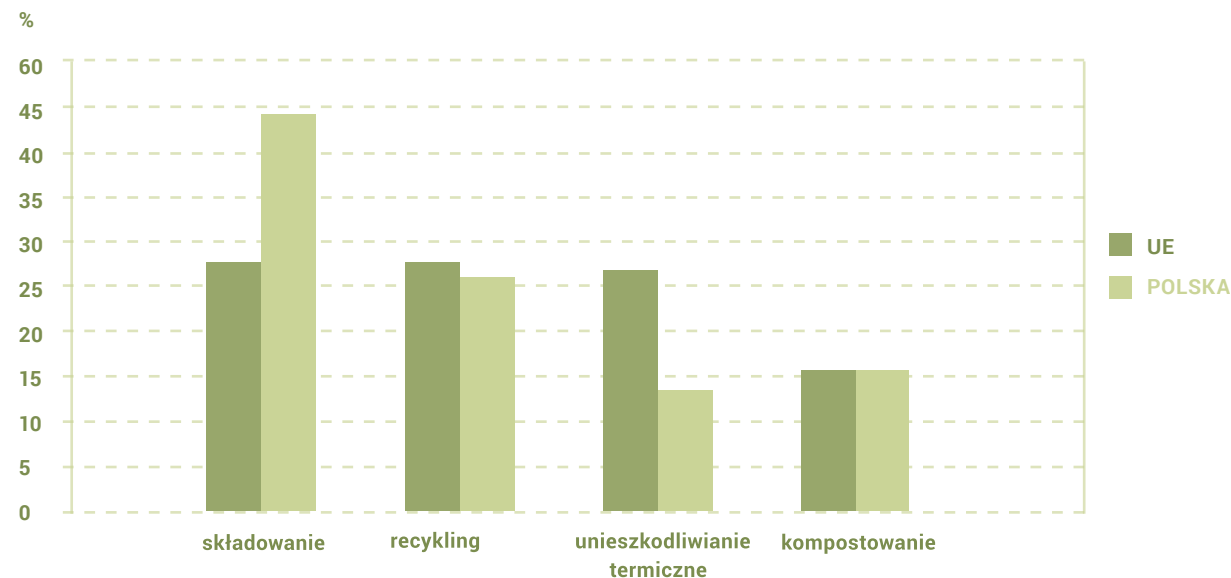
Misa, nie durszlak

Obowiązkowym elementem ochrony składowiska jest uszczelnienie dna kwatery składowej. Do tego typu zabezpieczeń najczęściej wykorzystuje się geomembrany statyczne, które stanowią nieprzepuszczalną barierę poniżej poziomu odpadów na kształt misy. Membrana ta jest rozwijana z rolek i zgrzewana na krawędziach. Cechuje ją szczelność i odporność na przebicie. Bariera musi wytrzymać napór ogromnej masy odpadów zgromadzonych na składowisku. Zazwyczaj już w trakcie budowy pod membraną umieszczony zostaje drenaż połączony z piezometrami – wąskimi, pionowymi studzienkami sięgającymi wód podpowierzchniowych, służącymi do wykrywania nieszczelności membrany. Inną formą uszczelnienia mogą być maty bentonitowe. Bentonit pod wpływem wilgoci pęcznieje, zmieniając swoją postać fizyczną oraz tworząc

Największym zagrożeniem dla otoczenia są odcieki, które po przedostaniu się do wód i gleby wywierają negatywny wpływ na ludzi i środowisko.



PORÓWNANIE SPOSOBÓW UNIESZKODLIWIANIA OPADÓW KOMUNALNYCH W POLSCE I UE W 2015 ROKU



warstwę o niskiej przepuszczalności wody. Jest to materiał samouszczelniający się pod wpływem wilgoci z otoczenia. Odcieki zebrane ze składowiska kierowane są do specjalnie przygotowanych zbiorników.

Podczyszczanie odcieków bez „lania wody”

Wysoki stopień toksyczności i duży ładunek zanieczyszczeń w stosunku do ścieków komunalnych czyni z odcieków składowiskowych trudny w zagospodarowaniu rodzaj nieczystości. Całkowite oczyszczenie odcieku jest kosztowne, czasochłonne i trudne ze względów technologicznych. Prostszy i często stosowanym w polskich warunkach rozwiązaniem jest podczyszczenie odcieku polegające na zmniejszeniu stężenia zanieczyszczeń do poziomu spotykanego w ściekach socjalno-bytowych. Podczyszczony odciek może być bezpiecznie kierowany bezpośrednio do oczyszczalni wykorzystujących metody biologiczne, bez ryzyka zniszczenia mikrofauny i mikroflory osadu czynnego. Najpowszechniejszym rozwiązaniem przy podczyszczaniu odcieków jest zastosowanie osadnika, którego zadaniem jest eliminacja zawiesiny z odcieku. Procesy w osadnikach wspierane są przez dawkowanie

substancji utleniających, redukujących lub po prostu neutralizujących zanieczyszczenia. Dochodzi wtedy do chemicznej koagulacji, czyli „kłaczkowania” roztworu, a nadmiar zanieczyszczeń pozostaje w osadniku. Należy pamiętać, że z pozoru najłatwiejsze rozwiązanie, czyli rozcieńczanie ścieków wodą do parametrów dopuszczanych przepisami, jest zagrożone odpowiedzialnością karną, ponieważ przyczynia się do jej marnowania.

W wielu krajach Europy Zachodniej popularność zyskuje metoda hydrofitowego podczyszczania ścieków. Odcieki ze składowiska wprowadzane są do specjalnie przygotowanego stawu zasiedlonego przez roślinność bagienną oraz bogatą faunę i florę mikrobiologiczną. Staw ma za zadanie imitować naturalne procesy biologiczne zachodzące między innymi na mokradłach. Nie jest to jedyna zaleta tego rozwiązania. W stawie hydrofitowym zachodzi szereg procesów fizycznych takich jak: utlenianie, redukcja, sedymentacja, asymilacja. Filtry membranowe stanowią najefektywniejszą, ale też najbardziej kosztowną metodę oczyszczania. Odwrócona osmoza zachodzi na skutek wykorzystania modułów dyskowo-rurowych. Wymuszany jest przepływ odcieku składowiskowego przez mikro membranę wbrew kierunkowi osmozy, w wyniku procesu po jednej

stronie membrany pozostają zatężone osady ściekowe, a po drugiej czysta chemicznie woda.

Neutralizacja biogazu

W wyniku rozkładania się odpadów organicznych zgromadzonych w kwaterze składowiskowej powstaje gaz wysypiskowy, będący mieszaniną metanu, dwutlenku węgla i innych związków chemicznych. Gaz ten jest niebezpieczny z wielu powodów. Dwutlenek węgla jest toksyczny dla człowieka w stężeniach od około 5%. Metan jest gazem łatwopalnym, który tworzy atmosfery wybuchowe przy stężeniu od około 4 do 15%. Jednym z elementów prewencji jest odgazowywanie, które ma na celu zabezpieczenie kwatery przed niekontrolowanym wybuchem gazu. Dodatkową funkcją instalacji odgazowującej jest umożliwienie dostępu do wnętrza składowiska – ułatwia to między innymi kontrolę stężenia i wielkości emisji biogazu.

Najczęściej występującą formą odgazowania jest wykorzystanie studni wierconych w złożu odpadów. Odwiert wykonuje się na całej miąższości złoża, a wewnątrz instaluje perforowany rurociąg z tworzywa sztucznego. Rurociąg obsypuje się żwirem o dużej granulacji. Zgromadzony w składowisku gaz dyfunduje do żwiru, a następnie za pośrednictwem perforacji do wnętrza studni. Aby zachować szczelność geomembrany w miejscach, w których rurociąg na nią napotyka, stosuje się przejścia – szczelne odgazowania przez membranę. Na powierzchni instaluje się studzienki ochronne mające na celu zabezpieczyć głowicę – zakończenie rurociągu, które pozwala na pobór próbki gazu oraz odprowadza go w kontrolowany sposób na zewnątrz. Rozwiązaniem pozwalającym zneutralizować uciążliwość zapachową są tzw. biofiltry. Dodatkowo w studni umieszcza się zrzębki roślinne i korę zasiedloną mikroorganizmami, które oczyszczają gaz przedostający się do atmosfery.

Coraz częściej jesteśmy świadkami udanych projektów rekultywacyjnych składowisk odpadów, które mogą być z powodzeniem wykorzystywane jako miejsce rekreacji i relaksu.



ODPADY KOMUNALNE WYTWORZONE WEDŁUG WOJEWÓDZTW W 2018 r.

POLSKA
12 485,4 tysięcy ton

tys.
ton
100
0

Na 1 mieszkańca w kg

	321-394
	261-320
	231-260
	201-230



Emisja pod czujnym okiem

Szczególną rolę w ograniczeniu negatywnego wpływu na środowisko ma monitoring przedostawania się zanieczyszczeń płynnych na zewnątrz składowiska. Zgodnie z polskim prawem, powinien być prowadzony nie tylko w trakcie użytkowania składowiska, ale również przez 30 lat od jego zamknięcia. Do identyfikacji niepożądanych odcieków wykorzystywane są piezometry umożliwiające przeprowadzanie badań chemicznych wód gruntowych. Dodatkowo przeprowadzane są badania wód powierzchniowych z okolicznych odcieków i zbiorników wodnych oraz wody pitnej ze studni głębinowych zlokalizowanych w pobliżu składowiska. Monitorowanie wielkości opadów na terenie obiektu pozwala w precyzyjny sposób określić ilość wody mogącej potencjalnie przekształcić się w szkodliwy odciek. Obowiązkowo bada się też wielkość emisji oraz skład gazu, który wydziela się w wyniku rozkładu martwej materii organicznej. Kluczowa ze względu na bezpieczeństwo jest też kontrola osiadania gruntu, ponieważ z biegiem lat może dochodzić do zmniejszenia się objętości składowanych odpadów w wyniku procesów zachodzących na kwaterze.

Budowa z rekultywacją w tle

Składowiska odpadów posiadają szereg zabezpieczeń mających na celu eliminację lub całkowite ograniczenie ich negatywnego wpływu na środowisko. Każdy tego typu obiekt powinien funkcjonować na podstawie instrukcji eksploatacji zatwierdzonej przez marszałka województwa lub regionalnego dyrektora ochrony środowiska, jeśli mamy do czynienia ze składowiskiem zlokalizowanym na terenie zamkniętym. Realizacja zapisów tego dokumentu zapewnia prawidłowe i bezpieczne użytkowanie instalacji. Nowe składowiska budowane są według ściśle określonych wytycznych wynikających z Rozporządzenia Ministra Środowiska z dnia 30 kwietnia 2013 r. w sprawie składowisk odpadów (Dz. U. 2013 poz. 523).

Obiekty, historyczne oraz współczesne, powstałe z naruszeniem powyższych ustaleń stanowią zagrożenie nie tylko dla środowiska naturalnego, ale też zdrowia i życia okolicznych mieszkańców. Nie jest tajemnicą, że standardy bezpieczeństwa produkcji chemikaliów w XX wieku odbiegały znacznie od dzisiejszych norm. Nieczynne składowisko odpadów po dawnych Zakła-

dach Chemicznych w Bydgoszczy stanowi nie lada problem dla mieszkańców pobliskiego Łęgnowa. Już w 1969 r. ze względu na fatalną jakość wody, władze zdecydowały o zaopatrywaniu mieszkańców w wodę pitną za pomocą beczkowsów. W tamtejszych wodach gruntowych do dziś znaleźć można substancje mutagenne i toksyczne takie jak między innymi: fenol, alanina, tuloidyna. Obecnie już na etapie projektowania składowiska opracowuje się kierunek i plan rekultywacji tego miejsca po zakończeniu jego eksploatacji.

Przekorny los

Rekultywacja dawnych składowisk odpadów jest dużym wyzwaniem. Zdarzenia losowe takie jak osunięcia terenu czy powodzie mogą zaprzepaścić wielomilionowe inwestycje poczynione, aby przywrócić te tereny naturze i społeczeństwu. Do głównych zagrożeń należą zanieczyszczenia wód odciekami ze składowisk czy też osunięcia i rozmycia warstw ochronnych odsłaniające zakopane w ziemi odpady. Przy projektowaniu nowych składowisk konieczne jest właściwe oszacowanie ryzyka związanego ze zdarzeniami losowymi. Co do zasady nowopowstałe składowiska odpadów nie mogą być lokowane na terenach chronionych, zagrożonych osunięciem terenu czy też w jakimkolwiek stopniu zagrożonych powodzią. Kryterium warunkującym podatność obiektu na zagrożenia naturalne jest jego wiek oraz ewentualna data wyłączenia z eksploatacji.

Bomba ekologiczna czy medialna?

W opinii społecznej składowiska odpadów to tykające „bomby ekologiczne”, które prędzej czy później spektakularnie dadzą o sobie znać. Największym zagrożeniem dla otoczenia są powstające wskutek deponowania odpadów odcieki, które po przedostaniu się do wód i gleby wywierają negatywny wpływ na ludzi i środowisko. Istnieją jednak metody pozwalające utrzymać to zagrożenie w ryzach i monitorować zjawiska zachodzące w samym składowisku. Prawidłowo zabezpieczony i eksploatowany obiekt nie tylko ogranicza swój negatywny wpływ, ale jest też bezpieczny dla otoczenia. Coraz częściej jesteśmy świadkami udanych projektów rekultywacyjnych składowisk odpadów, które mogą być z powodzeniem wykorzystywane jako miejsce rekreacji i relaksu. Obiekty takie dzięki fachowej wiedzy i prawidłowej eksploatacji mogą zostać przekształcone z groźnych „bomb ekologicznych” w miejsca przyjazne ludziom.

W wielu krajach Europy Zachodniej popularność zyskuje metoda hydrofitowego podczyszczania ścieków. Odcieki ze składowiska wprowadzane są do specjalnie przygotowanego stawu, zasiedlonego przez roślinność bagienną oraz bogatą faunę i florę mikrobiologiczną. Staw ma za zadanie imitować naturalne procesy biologiczne zachodzące między innymi na mokradłach.



W poszukiwaniu skutecznej ochrony danych

Dane coraz częściej określone są mianem kluczowego surowca XXI wieku. Stanowią paliwo napędzające cyfrową gospodarkę, dlatego ich bezpieczeństwo jest priorytetem w wielu firmach i organizacjach. Niestety czasami dochodzi do ich utraty lub zniszczenia. I nie zawsze jest to wina urządzenia lub oprogramowania, czasami „cyfrowe skarby” trafiają w niepowołane ręce w wyniku nieuwagi lub roztargnienia pracownika.



Daniel Świątek

Inżynier ds. Oceny Ryzyka, zajmuje się przeprowadzaniem testów penetracyjnych, audytów teleinformatycznych i szkoleń podnoszących świadomość cyberzagrożeń. Absolwent Wydziału Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej. W Grupie ERGO Hestia od 2017 r.

Pewnego dnia pracownik naukowy jednej z warszawskich uczelni jechał autem do pracy, gdy nagle poczuł dziwne zachowanie pojazdu. Okazało się, że podczas jazdy z tylnej opony uszło całe powietrze. Gdy kierowca próbował wyciągnąć koło zapasowe z bagażnika, do samochodu podszedł pewien jegomość. Raptownie otworzył drzwi, chwycił torbę z laptopem oraz pozostawione na tylnym siedzeniu inne wartościowe przedmioty i zaczął z nimi uciekać w stronę oczekującego na niego pojazdu. Cała akcja trwała kilka sekund i jak się później okazało była dokładnie zaplanowana. Złodziei skusiły pozostawione w aucie przedmioty, dlatego niepostrzeżenie przebili oponę na parkingu. Dalsze wypadki potoczyły się zgodnie z założonym przez nich scenariuszem: śledzenie samochodu, zatrzymanie w celu wymiany koła, szybka kradzież i ucieczka z miejsca zdarzenia.

Przebita opona, utrata wartościowych rzeczy oraz prywatnego laptopa to nie wszystkie straty tego dnia. Naukowiec uświadomił sobie, że w ręce przestępców wpadły dane osobowe kandydatów na studia, które od dłuższego czasu, bez wiedzy i zgody uczelni, przechowywał na swoim komputerze. Jego obowiązkiem w takiej sytuacji była konieczność zgłoszenia utraty wrażliwych informacji do inspektora ochrony danych na uczelni. Po kilku dniach od zajścia zdarzenia na stronie uczelni pojawił się oficjalny komunikat, w którym poinformowano o całym incydencie.

Wkrótce policja zatrzymała podejrzanych o kradzież obywateli Gruzji, którzy wyspecjalizowali się w dokonywaniu podobnych kradzieży metodą „na kole”. Laptop po usunięciu wszystkich danych trafił zapewne do jednego z warszawskich lombardów. Przestępcy nie mieli pojęcia, do jakich informacji mieli w tym czasie dostęp. Jak pokazuje powyższy przypadek, naruszenie bezpieczeństwa informacji, które w obecnych czasach najczęściej utożsamiamy z atakiem hakerskim, może być także spowodowane przez pospolitych przestępców.

Nowe wyzwanie czy odwieczny problem?

Naruszenia bezpieczeństwa informacji występowały zanim jeszcze komputery na stałe pojawiły się na każdym biurku. Pierwsze incydenty miały zazwyczaj postać utraty lub wycieku danych. Były one rezultatem zgubienia lub kradzieży dokumentów, ujawnienia osobie nieupoważnionej poufnych informacji lub ich przypadkowego upublicznienia. Jeszcze 50 lat temu jednym z głównych przykazań bezpieczeństwa każdego pracownika było niewynoszenie żadnych dokumentów poza miejsce pracy. Kłóciło się to jednak z innymi wytycznymi: „praca w godzinach nadliczbowych w miejscu pracy jest niedozwolona”. Terminy goniły, sterty kartek na biurkach rosły, dzieci w domu płakały. Aby jakoś pogodzić to wszystko, pracownicy często decydowali się na nadgonienie zaległości podczas nieoficjalnej pracy w domu. Jest to oczywiście niedopuszczalne z punktu widzenia bezpieczeństwa informacji, ale co zrobić, jeśli wszystkie faktury są do opisania „na wczoraj”? Dopóty nie będzie żadnego problemu, dopóki wszystko będzie zrobione na czas oraz nic nie zostanie zgubione, zniszczone lub skradzione. Pracodawca, nawet jeśli był świadomy, że taki proceder ma miejsce, często przymykał na niego oko. Jednak działało się tak jedynie do czasu. Gdy wydarzył się z tego powodu jakiś poważny incydent, takie zachowanie było piętnowane i uznawane za niedopuszczalne. Czasy się zmieniają, a owe problemy pozostają. Wszystko to, co kiedyś zalegało na



Bezpieczeństwo to proces, tak samo jak edukacja. Dlatego warto pomyśleć o tym wcześniej, a nie gdy będzie na to za późno.

biurku, teraz zakrywa nam cały pulpit. Zamiast wszystko drukować (choć nadal się to zdarza), wolimy skopiować pliki na pendrive'a, przysyłać do chmury, wysyłać pocztą e-mail albo w ostateczności zabierać służbowego laptopa do domu. „Wędrujące” w ten sposób dane i sprzęt w połączeniu z niedostatecznie świadomym użytkownikiem są nieustannym zagrożeniem dla firm.

Prywatny czy służbowy?

Obecnie firmy, zatrudniając pracowników umysłowych, albo zapewniają im służbowy komputer/laptop oraz telefon, albo stosują politykę BYOD (praca na sprzęcie prywatnym, z ang. Bring Your Own Device). W przypadku urządzeń służbowych zwykle nie wyklucza się ich okazjonalnego wykorzystania do celów prywatnych. Jednak takie podejście, po pewnym czasie, często powoduje zatarcie tego rozróżnienia. Pracownik zaczyna traktować otrzymany sprzęt jak swój i niejednokrotnie rezygnuje z prywatnego, aby np. nie nosić dwóch telefonów i zaoszczędzić na rachunkach. Zapomina tym



samym, że sprzęt służbowy nie jest de facto jego własnością. Może zająć również sytuacja odwrotna – swój sprzęt prywatny traktuje jako służbowy. Dzieje się tak na przykład dlatego, że komputer w pracy ma zwykle wiele ograniczeń np. brak uprawnień administratora, brak możliwości odtwarzania plików multimedialnych lub ograniczony katalog dostępnych na urządzeniu stron internetowych. Innym powodem może być częste zabieranie pracy do domu lub fakt, że sprzęt służbowy działa wolniej od prywatnego. Wystarczy tylko przenieść wszystkie dane i zainstalować niezbędne programy, aby prywatny laptop był gotowy do pracy. Jest to o tyle niebezpieczne, że sprzęt ten nie jest monitorowany, a tym bardziej zabezpieczony przez dział IT. Czy według użytkowników takie postępowanie jest bezpieczne? Paradoksalnie tak. W przypadku gdy pracownik korzysta ze sprzętu służbowego, jest przekonany, że nie odpowiada za jego bezpieczeństwo. Zrzuca on całą odpowiedzialność w tej kwestii na dział bezpieczeństwa lub IT. Natomiast w przypadku gdy używa własnego sprzętu, zazwyczaj uważa, że nie jest on atrakcyjnym celem dla hakerów i nikt go nie zhakuje, więc jest bezpieczny. Zarówno jedno, jak i drugie podejście do sprawy daje pracownikowi iluzoryczne poczucie bezpieczeństwa. Takie myślenie sprawia, że nie jest on świadomy faktu, że to on stanowi pierwszą linię obrony przed hakerami.

Komputer jako narzędzie

Działy bezpieczeństwa i IT ustawiają filtry antyspamowe, konfiguruje zapory sieciowe i inne zabezpieczenia, jednak to nie one są najważniejszym czynnikiem decydującym o bezpieczeństwie firmy. Większość ataków hakerskich zaczyna się od zabiegów socjotechnicznych wymierzonych w użytkowników – stąd tak ogromna liczba kampanii phishingowych. Decyzja przeciętnego użytkownika o tym, czy otworzyć dany email, czy kliknąć w załącznik i czy podać swoje dane uwierzytelniające na wyświetlonej stronie, jest kluczowa dla powodzenia ataku. Zabezpieczenia techniczne to obecnie kwestia drugorzędna. Dlaczego tak się dzieje? Mechanizmy bezpieczeństwa stają się coraz bardziej skomplikowane, coraz trudniejsze do zhakowania i obejścia. Oczywiście nie są (i nigdy nie będą) remedium dla zagrożeń stwarzanych przez hakerów. Utrudniają one cały proces przełamывania zabezpieczeń, minimalizują ryzyko, jednak nie niwelują go całkowicie. Dlatego aby zwiększyć szanse powodzenia ataku, przestępcy celują w najsłabsze ogniwo w całym łańcuchu zabezpieczeń, którym od dawien dawna jest użytkownik. Może on nieświadomie „wpuścić” hakerów do sieci wewnętrznej. To znacznie ułatwi napastnikom zadanie, bo tak jak i w życiu zazwyczaj najsolidniejsze zamki mamy przy drzwiach zewnętrznych. Oczywiście pracownik nie ułatwia hakerom pracy świadomie. Po prostu nie wie, jak „od środka” działają komputery i mechanizmy zabezpieczeń. Korzysta on z komputerów oraz systemów informatycznych jak z narzędzi do



Aby zwiększyć szanse powodzenia ataku przestępcy celują w najsłabsze ogniwo w całym łańcuchu zabezpieczeń, którym od dawien dawna jest użytkownik.

wykonywania swojej codziennej pracy. O ile nie jesteśmy mechanikiem samochodowym, nie zastanawiamy się, jak działają nasze „cztery koła” – nie jest to nam potrzebne do kierowania nimi. Hakerzy wykorzystują brak tej świadomości, skłaniając użytkownika do wykonania na pozór niegroźnej akcji, jak np. otwarcie pliku lub wyświetlenie strony, która w rezultacie pozwoli mu na ominięcie sporej liczby ograniczeń. Z tego też powodu edukacja użytkownika jest kluczowa do zwiększenia bezpieczeństwa organizacji. Jest ona również poważnym wyzwaniem.

Bezpieczny na co dzień

Niezwykle trudno jest przekonać użytkowników do skrupulatnej weryfikacji maili i innych bezpiecznych zachowań, podczas gdy nie robią tego w przypadku swoich własnych urządzeń. Firmy starają się zwykle budować świadomość zagrożeń u pracowników tylko w kwestiach bezpośrednio związanych z pracą. Na takich szkoleniach często słyszy się zdania pokroju: „jak klikniesz zainfekowany załącznik, narazisz pracodawcę na straty”. To zdanie pojawia się zazwyczaj w towarzystwie informacji o ogromnych wyciekach



danych, wyrafinowanych atakach hakerskich oraz ogromnych stratach z nich wynikających. Połączenie ich z wspomnianym wcześniej nastawieniem użytkownika do bezpieczeństwa z pewnością nie zmieni aktualnego stanu rzeczy. Utwierdzi go to raczej w przekonaniu, że hakerzy atakują tylko firmy a nie pojedyncze jednostki – a to nie prawda! Przytoczone incydenty nigdy nie będą tak bardzo na niego oddziaływać jak studia przypadku, w których hakerzy ukradli oszczędności życia „szarego Kowalskiego”. Pracownikowi bardziej niż na zabezpieczeniu przed hakerami pracodawcy zależy na ochronieniu przed cyberprzestępcami swoich bliskich i swoich oszczędności na koncie bankowym. Oczywiście ta tematyka odbiega od celów biznesowych pracodawcy, jednak powoduje, że użytkownicy uświadamiają sobie istnienie cyberzagrożeń. Dzięki niej poczują się oni zmotywowani do zgłębiania tematu, dostrzegą potrzebę zabezpieczenia siebie i swoich bliskich, obserwowania zmian i ciągłego doszkalania się. Takie nastawienie trzeba ciągle pielęgnować i podtrzymywać, żeby zwiększyć efektywność edukacji.

Zanim zaczniesz biegać, naucz się chodzić

Aby szkolenia dla pracowników przynosiły zadawalające efekty, należy zacząć od podstaw. Błędne zrozumienie bazowych pojęć i terminów będzie narastało się wraz ze zdobywaniem nowej wiedzy. Czasami może ono nawet spowodować niechęć do stosowania jakichkolwiek mechanizmów bezpieczeństwa, co pokazał mi przykład pewnego użytkownika. Podczas podsumowania jednego ze szkoleń dla pracowników, radziłem jego uczestnikom, aby regularnie wykonywali kopie zapasowe swoich ważnych plików. Miałby być one umieszczone w innym miejscu niż oryginalne dane. Później w czasie rozmowy w kuliarach zupełnie przypadkowo okazało się, że jeden z uczestników nie zamierza stosować tej wskazówki. Argumentował to, mówiąc, że kiedyś zawsze wykonywał backupy na dysku D, a wszystkie oryginalne pliki trzymał na C. Raz przypadkowo upuścił laptopa powodując fizyczne uszkodzenie dysku zawierającego system operacyjny. Z racji używania w pracy swojego prywatnego



sprzętu musiał oddać go, na własną rękę, do serwisu. Po wymianie dysku na nowy i ponownym zainstalowaniu systemu nie znalazł on jednak swoich plików. To zdarzenie utwierdziło go w przekonaniu, że nie warto wykonywać kopii zapasowych swoich danych. Nie był on świadomy, że dyski C i D mogą być jednym, podzielonym na dwie logiczne części, dyskiem twardym. Druga osoba natomiast z dumą twierdziła, że na szkoleniu nie było dla niej nic nowego, bo wszystkie rady zna i chociażby od dawna robi „backupy” w osobnym folderze na pulpicie tego samego komputera. Uczestnicy szkoleń często boją się pytać o rzeczy uznawane za najprostsze. Według nich mogłoby to w oczach pozostałych świadczyć o ich niekompetencji. O wiele bardziej prawdopodobne natomiast jest zadawanie pytań odnośnie nieznanych i mniej trywialnych aspektów. Dlatego tego typu edukacja powinna zawsze zaczynać się od zbudowania solidnych podstaw i wytłumaczenia możliwie jak najprostszymi słowami nawet tych „oczywistych” terminów.

Maksymalizuj prewencję, aby minimalizować konsekwencje!

Wspomniana wcześniej motywacja i uświadomienie to jednak nie wszystko. Wiedza to jedno, jej praktyczne wykorzystanie i stosowanie to zupełnie coś innego. Możemy wiedzieć, co to jest phishing, pamiętać o kluczowych elementach umożliwiających jego zidentyfikowanie, a mimo to otwierać wszystkie wiadomości i załączniki oraz klikać we wszystkie zawarte w nich linki. Ponadto gdy przypomnimy sobie przytoczoną na początku historię, dostrzeżemy, że szkolenie z bezpieczeństwa przyniosło jakiś efekt – pracownik uczelni przyznał się do tego jakie dane „chomikował” na swoim dysku. Jednak czy o taki efekt chodziło? Dlatego niezwykle ważne

Hakerzy wykorzystują brak świadomości użytkowników, skłaniając ich do wykonania na pozór niegroźnej akcji, jak np. otwarcie pliku lub wyświetlenie strony, która w rezultacie pozwoli mu na ominięcie sporej liczby ograniczeń. Z tego też powodu edukacja jest kluczowa do zwiększenia bezpieczeństwa organizacji.

jest budowanie dobrych nawyków u pracowników. Motywacja pozwoli im wkroczyć na dobrą ścieżkę, natomiast nawyk utrzyma ich na właściwym kursie. Będzie to bardzo trudne na początku, gdyż teraz korzystają oni z utartych schematów, które często stoją w opozycji do bezpiecznego używania sprzętu. Jednak wysiłek włożony w edukację jest warty swojej ceny. Początkowo pracownik przestraszy się hakerów. Zabezpieczy on dzięki temu swój komputer, na którym być może „przypadkiem” znajdują się dane służbowe. Wiedząc, jak działają hakerzy, będzie on dokładniej weryfikować e-maile, aby nie stracić swoich oszczędności – zarówno w pracy, jak i w domu. Na komputerze służbowym przecież też zdarza mu się wykonywać operacje na swoim koncie bankowym – jeżeli pozwoli na zhakowanie komputera służbowego narazi on również swoje oszczędności. Gdy zobaczy, jak wiele od niego zależy, po czasie zrezygnuje z brania na siebie odpowiedzialności za dane służbowe i ograniczy ich przetwarzanie na swoim prywatnym sprzęcie. Bezpieczeństwo to proces, tak samo jak edukacja. Dlatego warto pomyśleć o tym zawczasu, a nie gdy będzie na to za późno.

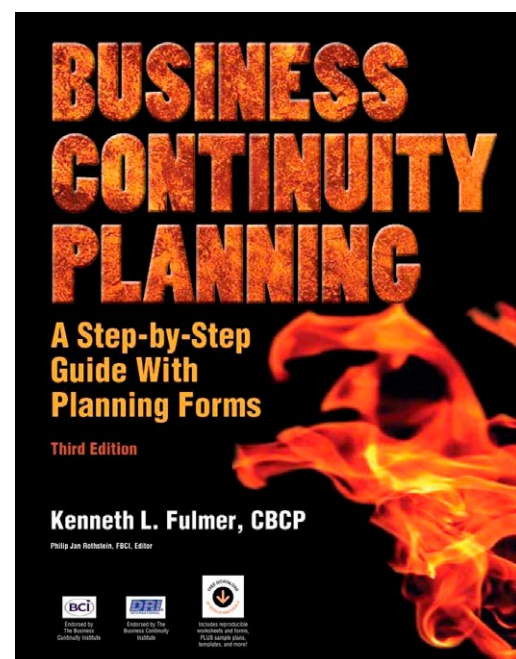


Na własne ryzyko



Metody i narzędzia wspomagające proces oceny ryzyka awarii w zakładach przemysłowych

Bartłomiej Połeć oraz Jarosław Tępiński są autorami publikacji, zawierającej opisy programów do oceny ryzyka wystąpienia awarii przemysłowych oraz zasięgu ich oddziaływania. W książce zawarto wnioski dotyczące metod i narzędzi wspomagających ocenę ryzyka wystąpienia awarii przemysłowej w zakładach, w których występują substancje niebezpieczne stwarzające zagrożenie pożarem, wybuchem lub emisją substancji toksycznych. Omawiana publikacja systematyzuje wiedzę na temat zjawisk związanych z rozprzestrzenianiem się zanieczyszczeń w atmosferze i ich matematycznego modelowania. Opracowanie jest dostępne na stronie internetowej www.cnbop.pl.



Business Continuity Planning

Prosty i użyteczny przewodnik dla nowicjuszy w zakresie planowania ciągłości działania. Kenneth L. Fulmer dzieli się dobrymi praktykami nabytymi podczas wieloletniej pracy w tym obszarze. Skutecznie rozprawia się z mitem, że systemy zarządzania kontynuacją biznesu są dla dużych przedsiębiorstw. Kryzys może dopaść każdego, dlatego niezwykle ważne jest odpowiednie przygotowanie się na kryzysowe sytuacje, niezależnie od skali prowadzonej działalności.



HESTIA
CORPORATE
SOLUTIONS



ERGO
HESTIA

Kolekcja ERGO Hestii

**Malarstwo holenderskie
i flamandzkie**

