prof. dr hab. inż. JERZY S. MICHALIK
Centralny Instytut Ochrony Pracy
– Państwowy Instytut Badawczy
dr MIECZYSŁAW J. BORYSIEWICZ
Instytut Energii Atomowej
Centrum Doskonałości MANHAZ

Poważne awarie i zagrożenia terrorystyczne instalacji chemicznych (1) – metody oceny podatności na zagrożenia

Możliwe skutki terroryzmu chemicznego określono na podstawie przykładów niektórych katastrofalnych poważnych awarii przemysłowych oraz ocen wykonanych przez Agencję Ochrony Środowiska USA (EPA). Omówiono zasady przeciwdziałania możliwym, wskutek aktów terroru poważnym awariom, polegające na wykonaniu analiz podatności zabezpieczeń (SVA), co pozwala na określenie podatnych na działania terrorystyczne „słabych" punktów stacjonarnych instalacji przemysłowych, sieci rurociągów lub systemów sterowania i systemów informatycznych.
Przedstawiono zalecane do wykorzystania w Polsce metody i narzędzia przeciwdziałania terrorystycznym zagrożeniom poważnymi awariami zakładów chemicznych; opracowane w USA. Są to dwie metody dotyczące analiz podatności instalacji chemicznych i oceny zabezpieczeń – metoda opracowana przez CCPS (Center for Chemical Process Safety) oraz metoda opracowana przez SOCMA (Synthetic Organic Chemical Manufacturers Association). W odniesieniu do cyberbezpieczeństwa i zabezpieczeń komputerowych systemów sterowania oraz systemów informatycznych jest to podejście obejmujące systemowy profil ochrony przemysłowego systemu sterowania (SPP) oraz metodykę analizy i oceny bezpieczeństwa systemów sterowania STOE (system target of evaluation) oraz metoda analiz podatności systemów technologii informacji CVSS (wspólny system punktowania podatności).

Major accidents and terroristic hazards in chemical installations (1) – methods of assessing vulnerability to threats
The article briefly discusses potential consequences of chemical terrorism using several major accidents as examples and estimations made by the US Environmental Protection Agency. It discusses the principles of preventing possible industrial major accidents – results of a terrorist attack – using security vulnerability analysis (SVA). SVA makes it possible to determine weak points of chemical installations, pipeline networks, computer control and information systems that are vulnerable to terrorist activities.
The article also presents methods and tools developed in the USA, following potential terrorist threats, for preventing major accidents in industrial chemical establishments. Those methods and tools are recommended for Poland; they are two methods of analysing the vulnerability of chemical installation and assessing their security: one was developed by the Center for Chemical Process Safety (CCPS), the other one by the Synthetic Organic Chemical Manufacturers Association (SOCMA). The system protection profile (SPP), the system target of evaluation (STOE) and the common vulnerability scoring system (CVSS) are used to ensure cybersecurity of computer industrial control (ICS) and IT networks.

Wstęp

Poważne awarie przemysłowe w zakładach chemicznych i rafineryjnych mogą mieć dramatycznie katastrofalne skutki. Oto przykłady:

- w wyniku katastrofy w zakładach chemicznych we Flixborough (Wielka Brytania, 1974 r.) – uwolnienia z pękniętego rurociągu cykloheksanu i wybuchu (o sile ok. 30 ton TNT) – śmierć poniosło 28 pracowników, zakład został zniszczony (w promieniu ok. 5 km)
- seria wybuchów zbiorników w magazynach LPG i pożary w San Juanico, Ixhuatepec koło Meksyku (Meksyk, 1984 r.) – ok. 550 ofiar śmiertelnych, ciężkie poparzenia i inne urazy u ponad 4000 osób, ewakuacja 60 000 mieszkańców, ogromne straty materialne
- uwolnienie do atmosfery około 30 ton par izocyjanku metylu z reaktora chemicznego w Bhopalu (Indie, 1984 r.) spowodowało śmierć 16 000 mieszkańców miasta i ciężkie przypadki utraty zdrowia u ok. 100 000 osób, ok. 200 000 osób ewakuowano
- w wyniku pożaru oraz wybuchu w magazynach materiałów pirotechnicznych w Enschede (Holandia, 2000 r.) zginęło 20 osób, obrażenia odniosło ok. 1000 osób, ok. 600 budynków mieszkalnych zostało zniszczonych lub uszkodzonych
- seria wybuchów (ich siła wynosiła 20-40 ton TNT) w magazynach azotanu amonu (nawozy sztuczne) w Tuluzie (Francja, 2001 r.): 30 ofiar śmiertelnych, ok. 2500 rannych, poważne straty materialne (ok. 1,5 mld €)
- w wyniku największej dotychczas katastrofy chemicznej w Polsce – pożaru zbiorników ropy naftowej, a następnie wybuchu dwóch z nich oraz dalszych pożarów w rafinerii w Czechowicach-Dziedzicach (1971 r.) – zginęło 37 osób, ponad 100 doznało ciężkich poparzeń i innych obrażeń, wystąpiły ogromne straty materialne.

Przykładów podobnych zdarzeń jest wiele. Nie można więc wykluczyć takiej możliwości, że zakłady stwarzające zagrożenia poważną awarią przemysłową, a w szczególności zakłady dużego ryzyka wystąpienia poważnej awarii (ZDR), w których znajdują się duże ilości niebezpiecznych substancji chemicznych, zlokalizowane np. w aglomeracji miejskiej, staną się atrakcyjnym celem działań terrorystycznych.

Potwierdzeniem realności takich zdarzeń mogą być oceny FBI z lutego 2003 r., według których w USA w latach 1980-2001 odnotowano 353 potwierdzone lub przypuszczalne akty terroryzmu. Część z nich była wymierzona przeciwko zakładom chemicznym.

Możliwe skutki terroryzmu chemicznego

Po 11 września 2001 r. w wielu krajach, a szczególnie w USA, mając na uwadze potencjalne akty terroru, zintensyfikowano prace nad podniesieniem poziomu bezpieczeństwa instalacji przemysłowych i ważnych infrastruktur krajowych, m.in. sieci rurociągów.

Podstawową kwestią jest dokonanie oceny, jak poważne skutki mogą wywołać terroryści używając istniejących stacjonarnych instalacji wytwarzających, przetwarzających, magazynujących i rozprowadzających chemikalia. Odwołamy się tutaj do ocen wykonanych przez Agencję Ochrony Środowiska USA (Environmental Protection Agency – EPA).

Na podstawie dostępnych danych o 15 000 instalacji eksperci EPA ocenili, że w przypadku awaryjnych scenariuszy uwolnień gazów toksycznych średnia odległość od instalacji do zewnętrznej granicy strefy zagrożenia wynosi ok. 1,6 mili, czyli ok. 2,5 km (1 mila lądowa = ok. 1,6 km). W przypadku scenariuszy awaryjnych z udziałem substancji palnych średnia odległość wynosi 0,4 mili, czyli ok. 600 m.

W odniesieniu do wielu instalacji oceniono strefy zagrożeń, rozciągające się do ok. 14 mil (ok. 22,5 km) od instalacji, głównie w przypadku uwolnień w obszarach miejskich chloru zmagazynowanego w 90-tonowych cysternach kolejowych i 25 mil (ok. 40 km) w przypadku uwolnień w obszarach wiejskich chloru zmagazynowanego w takich cysternach. W przypadku innych chemikaliów strefy zagrożeń, które przekraczały 25 mil (40 km), dotyczyły uwolnień bezwodnego amoniaku, fluorku wodoru, ditlenku siarki, ditlenku chloru, dymiącego kwasu siarkowego, tritlenku siarki, chlorku wodoru, kwasu cyjanowodorowego, fosgenu, cyjanku etylu, bromu i akrylonitrylu.

Oceny przeprowadzane przez EPA pokazały, że w przypadku substancji palnych średnia liczba osób dotkniętych skutkami wynosi 15, a w przypadku substancji toksycznych – 1500 („dotkniętych" oznacza potencjalnie narażonych). Jest mało prawdopodobne, aby wszyscy w strefie zagrożenia byli narażeni, jednak każda osoba z tej strefy może znaleźć się na ścieżce chmury uwolnionych chemikaliów w określonych warunkach środowiska i pogody.

Zasady przeciwdziałania poważnym awariom wskutek aktów terroru

W przypadku zagrożenia terrorystycznego punktami krytycznymi, najbardziej narażonymi na atak, są elementy strategiczne instalacji przemysłowej lub sieci rurociągów, a zwłaszcza takie, których awaria spowoduje zatrzymanie pracy znacznej części instalacji oraz elementy, których awaria spowoduje możliwie największe skutki dla ludzi i środowiska. Jak wiadomo, podstawowym elementem zarządzania ryzykiem poważnych awarii w odniesieniu do „konwencjonalnego" bezpieczeństwa procesowego jest analiza zagrożeń procesu (instalacji) – *process hazard analysis* – PHA. Natomiast w kontekście zagrożeń terrorystycznych kluczowym elementem systemu bezpieczeństwa (*security*, czyli ochrony, zabezpieczeń) jest przygotowanie i wdrożenie analiz podatności zabezpieczeń (*security vulnerability analysis* – SVA). Jest to proces analityczny, w którym wyznacza się rodzaje i warunki potencjalnych zagrożeń terrorystycznych i sabotażowych, prawdopodobieństwa skutków oraz możliwe ich następstwa.

Pozwala to na określenie „słabych" punktów instalacji przemysłowej lub sieci rurociągów, oszacowanie wrażliwości obiektów należących do instalacji stacjonarnych i rurociągów, a także określenie „słabych" punktów systemów sterowania i systemów informatycznych, szczególnie podatnych na działania o charakterze terrorystycznym.

Fot. Jerome Bei

W analizach SVA przyjmuje się z reguły, że terrorysta chce zmaksymalizować szkodę i zaatakować cel, który jest dość łatwo dostępny. Skutki niepożądanego działania rozważa się w kilku kategoriach, a mianowicie: wpływ na zdrowie ludzkie, straty finansowe i negatywne oddziaływanie na środowisko. Wykorzystanie metod SVA pozwala na wyznaczanie priorytetów w odniesieniu do opracowania i zastosowania odpowiednich środków zaradczych (rozwiązań technicznych i organizacyjnych) oraz na ocenę ich skuteczności.

Takie podejście oznacza rozszerzenie istniejących systemów zarządzania konwencjonalnym ryzykiem poważnych awarii przemysłowych instalacji chemicznych – generowanym przez właściwości fizykochemiczne stosowanych, magazynowanych lub produkowanych substancji oraz wynikającym z istniejących rozwiązań projektowych i sposobu eksploatacji systemów technologicznych i instalacji – o narzędzia, a także systemy zabezpieczeń i ochrony zakładów chemicznych przed możliwymi działaniami terrorystycznymi i sabotażem.

Narzędzia przeciwdziałania terrorystycznym zagrożeniom poważnymi awariami instalacji chemicznych

W Polsce nie było dotychczas zalecanych i dostępnych w języku polskim narzędzi do analizy ryzyka umyślnych (terrorystycznych) poważnych awarii przemysłowych, pozwalających na identyfikację zagrożeń tego typu oraz możliwych ich skutków, stanowiących podstawę wyboru zaradczych środków ochrony i oceny ich skuteczności. W Centralnym Instytucie Ochrony Pracy – Państwowym Instytucie Badawczym w latach 2005-2007, w ramach programu wieloletniego pn. *Dostosowywanie warunków pracy w Polsce do standardów Unii Europejskiej* zostało wykonane zadanie pt. „Metodyka zintegrowanych ocen ryzyka poważnych awarii i zagrożeń terrorystycznych zakładów chemicznych". Miało ono na celu wypełnienie istniejącej luki i udostępnienie zainteresowanym zakładom oraz instytucjom publicznym niezbędnych narzędzi.

W ramach tego zadania dokonano przeglądu metod i narzędzi opracowanych w krajach zaawansowanych w tej dziedzinie, w szczególności w USA, oraz wybrano najbardziej spójne i efektywne metody. Na tej podstawie dokonano adaptacji lub opracowano zalecane do wykorzy-

stania w Polsce narzędzia. Metody te i narzędzia stanowią podstawowy instrument niezbędny do racjonalnego wyboru odpowiednich zabezpieczeń, opracowania właściwych procedur oraz określenia miejsc, w których należy wprowadzić dodatkowe środki ochronne [1-3].

Metoda analiz podatności instalacji chemicznych i oceny zabezpieczeń CCPS

Jedną z zalecanych do zastosowania w Polsce jest metoda analiz podatności instalacji chemicznych i oceny zabezpieczeń CCPS [4]. Jest to metoda SVA (*security vulnerability analysis* – analiza bezpieczeństwa (podatności) słabych punktów) opracowana przez Center for Chemical Process Safety – CCPS (USA), składająca się z 5 kroków. Została ona przedstawiona w artykule opublikowanym w czasopiśmie „Chemia Przemysłowa" [5]. W artykule tym zostały także szerzej przedstawione i omówione ogólne zasady SVA. Pełny opis metody CCPS w języku polskim jest dostępny w CIOP-PIB [6].

Metoda oceny odporności obiektów i zarządzania podatnością SOCMA

Metoda SOCMA [7], opracowana przez Stowarzyszenie Producentów Syntetycznych Organicznych Związków Chemicznych (Synthetic Organic Chemical Manufacturers Association, USA), jest jedną ze szczególnie rekomendowanych ostatnio metod oceny odporności obiektów i stanowi podstawowy instrument niezbędny do racjonalnego wyboru odpowiednich zabezpieczeń, opracowania właściwych procedur oraz określenia miejsc, w których należy wprowadzić dodatkowe środki ochronne.

Metoda SOCMA polega na ocenie istniejących (lub wprowadzonych) rozwiązań i uwarunkowań w zakładzie chemicznym, odnoszących się do czterech czynników (grup problemowych) i następnie na priorytetyzacji ich znaczenia w drodze określania ich wzajemnej wagi. Czynnikami stosowanymi w metodzie SOCMA są: (1) zagrożenia, (2) atrakcyjność, (3) skutki oraz (4) bezpieczeństwo.

Dla każdego z tych czynników zostały ustalone wskaźniki, które są podstawą do dokonywania ocen w formie rankingu. W przypadku uproszczonej wersji metody, przeznaczonej do analiz zgrubnych (przesiewowych), liczba tych wskaźników dla poszczególnych czynników wynosi: zagrożenia – 5, atrakcyjność – 3, skutki – 3 oraz bezpieczeństwo (głównie elementy ochrony fizycznej) – 4. W zaawansowanej wersji liczba wskaźników oceny podatności oraz ryzyka jest zdecydowanie większa i dla poszczególnych czynników wynosi: zagrożenia – 10, atrakcyjność – 16, skutki – 16 oraz bezpieczeństwo – 18.

W celu oceny poszczególnych wskaźników zastosowano czterostopniową skalę rankingową. W przypadkach, kiedy jest to możliwe, parametry poszczególnych wskaźników określono ilościowo, a w pozostałych – opisowo. Uszeregowano je według wartości punktowej od 1 – najkorzystniejsze rozwiązanie (sytuacja) do 4 – najmniej korzystne z punktu widzenia ryzyka.

Poszczególne wskaźniki mają różne znaczenia dla bezpieczeństwa i ochrony instalacji (zakładu) przed zagrożeniami terrorystycznymi. Znaczenie każdego wskaźnika poszczególnych czynników (zagrożenia, atrakcyjność, skutki oraz bezpieczeństwo) jest porównywane ze znaczeniem innych wskaźników. W tym celu została zastosowana metoda ważenia. Wszystkim wskaźnikom w obu wersjach metody (model zgrubny i zaawansowany) zostały przypisane wielkości wagi. Są to wielkości względne, ustalone na zasadzie ocen eksperckich.

Więcej informacji dotyczących metody SOCMA przedstawiono podczas VII Konferencji Naukowo-Technicznej „Bezpieczeństwo Techniczne w Przemyśle Chemicznym" [8], a pełny opis tej metody w języku polskim jest dostępny w CIOP-PIB [9].

Metoda SOCMA daje wyniki numeryczne i jest względnie prostym i efektywnym narzędziem analizy i zarządzania podatnością. Pozwala na priorytetyzację i ważenie istotnych czynników oraz na racjonalny wybór niezbędnych środków zaradczych. Należy ją uznać za szczególnie przydatną w warunkach polskich.

Metody i narzędzia rekomendowane w odniesieniu do ochrony i zabezpieczeń komputerowych systemów sterowania oraz systemów informatycznych

Cyberbezpieczeństwo stanowi integralną część bezpieczeństwa przemysłu chemicznego. Organizacje w coraz większym stopniu stosują systemy wykorzystujące sieci komputerowe. W ten sposób następuje rozproszenie przetwarzania informacji, które dawniej było wykonywane w tradycyjnych centrach przetwarzania danych. W tej sytuacji atak terrorystyczny, mający na celu umyślne spowodowanie poważnej awarii, może być wykonany za pomocą komputerowych systemów sterowania i zarządzania procesem (instalacją).

Zagadnienia bezpieczeństwa systemów komputerowych (w znaczeniu angielskiego słowa *safety*) oraz zapewnienia bezpieczeństwa (w znaczeniu *security*) w odniesieniu do zagrożeń komputerowych systemów sterowania oraz systemów informatycznych, związanych z możliwymi aktami terroru, sabotażu oraz innymi nieuprawnionymi działaniami stron trzecich wobec zakładów i instalacji chemicznych, omówiono we wcześniejszej publikacji [10]. Przedstawiono w niej także interesujące

Fot. Brian E. Christiansen

Fot. Archiwum CIOP-PIB

podejście do oceny i zapewnienia bezpieczeństwa komputerowych systemów sterowania, obejmujące systemowy profil ochrony (*system protection profile* – SPP) przemysłowego systemu sterowania (*industrial control system* – ICS) oraz metodykę analizy i oceny bezpieczeństwa systemów sterowania i bezpieczeństwa procesowego STOE (*system target of evaluation* – systemowy cel (przedmiot) oceny) [11].

Ciekawym instrumentem oceny i zapewnienia bezpieczeństwa technologii informacji (*information technology* – IT) oraz ICS jest także metoda analiz podatności systemów technologii informacji CVSS (*common vulnerability scoring system* – wspólny system punktowania podatności) [12, 13]. Metodę CVSS można rozpatrywać jako rekomendowane narzędzie do prowadzenia analiz podatności systemów informatycznych i systemów sterowania oraz do zarządzania bezpieczeństwem tych systemów w Polsce. Metoda ta polega na wykorzystaniu metryk (*metrics*) do standaryzowanych obliczeń w trakcie analizy podatności i przypisywaniu odpowiednich punktów parametrom oszacowanym w analizach. Zapewnia ona uzyskanie punktowanych wartości podatności, reprezentatywnych dla faktycznego ryzyka („spriorytetyzowane ryzyko"). Ułatwia to wybór rodzajów środków zaradczych i miejsc zabezpieczeń z uwzględnieniem tych elementów systemu, które stwarzają największe ryzyko. Pełne opisy metod SPP–STOE [14] oraz CVSS [15] są dostępne (w języku polskim) w CIOP-PIB.

PIŚMIENNICTWO

[1] J. S. Michalik, M. J. Borysiewicz *Przeciwdziałanie zagrożeniom umyślnymi poważnymi awariami przemysłowymi wskutek aktów terroru.* Konferencja „Nowe wyzwania BHP i REACH w branży chemicznej", Zachodniopomorski Klaster Chemiczny „Zielona Chemia", Zakłady Chemiczne Police S.A., Międzynarodowe Targi Szczecińskie, Szczecin, 21.–22. 02. 2008

[2] M. J. Borysiewicz, J. S. Michalik *Metody przeciwdziałania terrorystycznym zagrożeniom poważnymi awariami instalacji chemicznych.* Konferencja naukowa „Zarządzanie bezpieczeństwem – wyzwania XXI wieku", Wyższa Szkoła Zarządzania i Prawa im. H. Chodkowskiej w Warszawie, Kazimierz Dolny, 27.–28. 03. 2008 r. Pr. zb. pod red. M. Lisieckiego. Wydawnictwo WSZiP im. H. Chodkowskiej. Wyd. II rozszerzone, Warszawa 2008, s. 423-442

[3] J. S. Michalik, M. J. Borysiewicz *Zagrożenia terrorystyczne. Metody i narzędzia ochrony instalacji chemicznych.* „Chemia Przemysłowa", 2(377)2008, s. 42-46

[4] *Guidelines for Analyzing and Managing the Security Vulnerabilities of Fixed Chemical Sites.* CCPS – Center for Chemical Process Safety of the American Institute of Chemical Engineers, New York, August 2002

[5] M. Borysiewicz *Zagrożenia terrorystyczne* (*Metody oszacowania ryzyka w analizach podatności instalacji chemicznych na zagrożenia terrorystyczne*). „Chemia Przemysłowa", 2(281)2005, s. 40-42

[6] J.S. Michalik, M. Borysiewicz, A. Wasiuk *Metodyka zintegrowanych ocen ryzyka poważnych awarii i zagrożeń terrorystycznych zakładów chemicznych. Opracowanie metody analizy zagrożenia i podatności na uszkodzenia instalacji procesowej w wyniku działań terrorystycznych i sabotażu.* Oprac. wewn. CIOP-PIB, Warszawa, listopad 2005

[7] *SOCMA SVA Manual. Manual on Chemical Site Security Vulnerability Analysis. Methodology and Model.* Synthetic Organic Chemical Manufacturers Association, Washington DC, November 2002

[8] J. S. Michalik, M. J. Borysiewicz *Metoda oceny odporności obiektów i zarządzania podatnością SOCMA – narzędzie przeciwdziałania terrorystycznym zagrożeniom poważnymi awariami instalacji chemicznych.* VII Konferencja Naukowo-Techniczna „Bezpieczeństwo techniczne w przemyśle chemicznym", BMP Sp. z o.o., Zakłady Azotowe Kędzierzyn S.A. Zakopane, 9-10 06. 2008 r. http://www.chemia.e-bmp.pl/index.php?art=1189

[9] J. S. Michalik, M. Borysiewicz, A. Gajek *Metodyka zintegrowanych ocen ryzyka poważnych awarii i zagrożeń terrorystycznych zakładów chemicznych. Opracowanie metody selekcji, obliczania i rankingu wskaźników rozwiązań inżynieryjnych i organizacyjnych stacjonarnych instalacji chemicznych, na potrzeby zarządzania odpornością na niebezpieczne scenariusze spowodowane działaniami terrorystycznymi.* Oprac. wewn. CIOP-PIB, Warszawa, listopad 2007

[10] M. J. Borysiewicz, J. S. Michalik *Cyberbezpieczeństwo przemysłowych systemów sterowania.* „Bezpieczeństwo Pracy", 10(433)2007, s. 8-11

[11] National Institute of Standards & Technology. System Protection Profile – Industrial Control Systems – Version 1.0. April, 2004 www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.doc

[12] M. Schiffman, G. Eschelbeck, D. Ahmad, A. Wright, S. Romanosky *CVSS: A Common Vulnerability Scoring System.* National Infrastructure Advisory Council (NIAC), 2004

[13] *A Complete Guide to the Common Vulnerability Scoring System. Version 2.0.* FIRST – Forum of Incident Response and Security Teams. http://www.first.org/cvss/cvss-guide.html#i1

[14] J. S. Michalik, M. J. Borysiewicz, A. Wasiuk *Metodyka zintegrowanych ocen ryzyka poważnych awarii i zagrożeń terrorystycznych zakładów chemicznych. Opracowanie zasad prowadzenia ocen rozwiązań inżynieryjnych i organizacyjnych dotyczących niebezpiecznych scenariuszy w stacjonarnych instalacjach chemicznych z uwzględnieniem istniejących interfejsów z instalacjami transportu i przeładunku substancji niebezpiecznych oraz systemów informatycznych w aspekcie ochrony przed działaniami terrorystycznymi i sabotażowymi.* Oprac. wewn. CIOP-PIB, Warszawa, listopad 2006

[15] J. S. Michalik, M. J. Borysiewicz, Ł. Czerski *Metodyka zintegrowanych ocen ryzyka poważnych awarii i zagrożeń terrorystycznych zakładów chemicznych.* Opracowanie rozwiązań w zakresie ochrony instalacji przed niepożądanymi działaniami stron trzecich (w szczególności aktami terroru i sabotażu) w zakładach chemicznych. Oprac. wewn. CIOP-PIB, Warszawa, listopad 2007

Publikacja opracowana na podstawie wyników uzyskanych w ramach programu wieloletniego pn. „Dostosowywanie warunków pracy w Polsce do standardów Unii Europejskiej" dofinansowywanego w latach 2005–2007 w zakresie służb państwowych przez Ministerstwo Pracy i Polityki Społecznej. Główny koordynator: Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy.

Fot. Archiwum CIOP-PIB

Fot. Archiwum CIOP-PIB