Utrzymanie ruchu w przemyśle. Wstęp. Cz. 2

Sławomir Szymaniec, Marek Kacperak

1. Rodzaje uszkodzeń i ich statystyka

Na podstawie długoletnich obserwacji w zakresie oceny przyczyn awarii maszyn wirujących w przemyśle krajowym można stwierdzić, że awaryjność silników w ostatnich latach wyraźnie się zmniejsza. Wynika to przede wszystkim z poprawy jakości eksploatacji, obsługi oraz diagnostyki silników, zastosowania coraz lepszych materiałów do ich produkcji, w tym w szczególności dobrych materiałów izolacyjnych, zastosowania coraz lepszych sprzęgieł, łożysk i smarów. Zmienia się statystyka przyczyn uszkodzeń silników WN. Zmniejsza się liczba uszkodzeń obwodów elektrycznego i magnetycznego silników, a relatywnie powiększa się liczba uszkodzeń typu mechanicznego – w szczególności łożysk tocznych. Występują również coraz częściej uszkodzenia typu luz w układach (np. wał – pakiet wirnika, łożyska – tarcza łożyskowa) oraz uszkodzenia konstrukcji wsporczej i fundamentu pod napędem. Z ekonomicznego punktu widzenia dla użytkowników silników WN najkosztowniejsze są uszkodzenia izolacji ich uzwojeń oraz poważne uszkodzenia fundamentów i konstrukcji wsporczych. Dane statystyczne awaryjności maszyn elektrycznych, w tym napędów z silnikami indukcyjnymi klatkowymi WN, w literaturze przedmiotowej są podawane bardzo rzadko. Zakłady przemysłowe bardzo niechętnie udostępniają swoje statystyki przyczyn awarii maszyn, liczby przestojów spowodowanych stanem technicznym maszyn, liczby zużytych łożysk, liczby remontów itd. Pewne informacje na powyższy temat można uzyskać na podstawie obserwacji działań firm ubezpieczeniowych, które „likwidują zaistniałą szkodę" w danym zakładzie.

W technicznym piśmiennictwie polskim na szczególną uwagę zasługują prace prof. Bronisława Draka [51, 52], prof. Tadeusza Glinki [76] oraz prof. Jakuba Bernatta i dr. Macieja Bernatta [15], prezentowane między innymi w Zeszytach Problemowych KOMELU, w których omawiane są przyczyny awarii silników klatkowych WN w zakładach przemysłowych w kraju. Wymienieni autorzy podają również statystykę awaryjności tych silników. W książce [235] autorzy amerykańscy podają uogólnioną statystykę przyczyn awarii maszyn elektrycznych prowadzoną przez EPRI dla 7500 maszyn. Statystykę tę przedstawiono w tabeli 1.

Tabela 1. Statystyka uszkodzeń maszyn elektrycznych [235]

Przyczyna awarii	Procentowy udział [%]
Łożyska	41
Stojan	37
Wirnik	10
Osprzęt, wyposażenie dodatkowe i inne	12

Statystykę przedstawioną w tabeli 1 należy traktować jako uogólnioną statystykę uszkodzeń maszyn elektrycznych świata zachodniego. Od kilkudziesięciu lat, analizując szczegółowo przyczyny awarii i nieoczekiwanych, nieplanowanych postojów maszyn wirujących w przemyśle, w szczególności w krajowym przemyśle cementowym, na podstawie własnych doświadczeń i obserwacji autorzy ustalili następującą listę ich przyczyn:

1) zły stan łożysk, zwłaszcza tocznych;
2) przeciążanie maszyn, w tym silników;
3) niewyważenie, nieosiowość i luzy związane z ruchem wirnika;
4) stan fundamentów, konstrukcji wsporczych i mocowania, rezonanse;
5) uszkodzenia wyposażenia elektrycznego i izolacji uzwojeń silników;
6) uszkodzenia głowic i rozruszników w silnikach pierścieniowych oraz uzwojeń wirników w silnikach klatkowych.

Listę podano w kolejności od przyczyn najczęściej występujących do tych, które występują najrzadziej dla ogółu krajowych cementowni.

W 2006 roku w jednej z małych opolskich cementowni, w cementowni „ODRA" SA, najstarszej cementowni w Polsce, odnotowano wysoką awaryjność układów technologicznych [114]:

- nitka wypału klinkieru – awaryjne postoje 14 dni/rok (straty to 100 tys. zł/dobę, razem straty 1,4 mln zł);
- młyny cementu – awaryjne postoje 28 dni/rok (straty 24 tys. zł/dobę, razem 670 tys. zł).

Duża awaryjność układów technologicznych była powodowana wieloma czynnikami występującymi w układach napędowych. Poprawa zdolności ruchowej urządzeń wymagała podejścia kompleksowego do zagadnienia. Określenie przyczyn występowania awarii ukierunkowało podjęcie działań naprawczych.

Stwierdzono, że awaryjne postoje były spowodowane:

- awariami wyłączników mocy 6 kV;
- złym działaniem zabezpieczeń pól 6 kV (odpływowych);
- niekontrolowanymi rozruchami silników;
- złym stanem technicznym rozruszników silników pierścieniowych;
- stosowaniem sztywnych sprzęgieł;
- złym stanem technicznym ram i fundamentów silników;
- trwałym przeciążeniem silników.

Podjęte działania modernizacyjne oraz wprowadzenie systemu diagnostycznego [115, 116] doprowadziły do poprawy zdolności ruchowej urządzeń technologicznych i zmniejszyły koszty produkcji. W 2011 roku osiągnięto znaczne ograniczenie postojów awaryjnych spowodowanych niesprawnością maszyn elektrycznych, dla przykładu [115, 116]:

- nitka wypału klinkieru – awaryjne postoje 0 dni;
- młyny cementu – awaryjne postoje 3 dni (awaria układu rozruchowego silnika synchronicznego).

Dodatkową zaletą wprowadzonych zmian było zmniejszenie rozmiarów

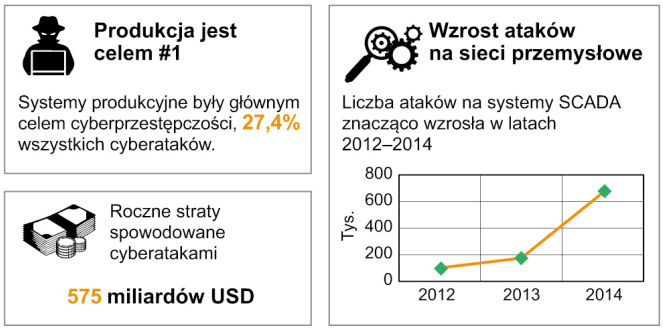
i skutków awarii mechanicznych. Ten efekt uzyskano przez wczesną detekcję rozwijających się uszkodzeń. Wprowadzenie monitoringu parametrów i diagnostyki układów napędowych wymusiło podniesienie jakości wykonywanych remontów.

Po transformacji polskiej gospodarki w system wolnorynkowy podstawowym kryterium działalności przedsiębiorstwa jest konkurencyjność na rynku. Dla uzyskania konkurencyjności konieczne jest poszukiwanie rejonów działalności przedsiębiorstwa, w których można zmniejszyć koszty produkcji. Zmniejszenie liczby awarii i ograniczenie ich skutków jest jednym z nich. Podjęte działania modernizacyjne w cementowni „ODRA" SA wpisały się w główny nurt przeobrażeń polskiej gospodarki i przemysłu.

Wyposażenie techniczne Cementowni „ODRA" SA po zmianach modernizacyjnych przedstawiono zbiorczo w tabeli 2.

2. Cyberbezpieczeństwo w zakładzie przemysłowym

Większość użytkowników komputerów cyberbezpieczeństwo w sposób naturalny kojarzy jedynie z potrzebą zainstalowania w swoim osobistym i służbowym komputerze, tablecie i ewentualnie w telefonie komórkowym skutecznego oprogramowania antywirusowego. Nie zdają sobie sprawy z tego, że we wszystkich dziedzinach działalności człowieka, w życiu gospodarczym (przemyśle, energetyce itd.) i w życiu codziennym, wszechobecne są systemy informatyczne, które należy chronić przed cyberatakami, rys. 1 [1, 12, 88, 144, 146, 151, 161, 162, 163, 175, 249, 250, 292, 323].



Rys. 1. Świat cyberataków – trendy [162]

2.1. Uwagi ogólne

Postęp w dziedzinie cyfryzacji, rozwój technologii informatycznych, Internet Rzeczy, sztuczna inteligencja, systemy CPS, duże zbiory danych globalnie tworzą świat nowych technologii, niosący nowe, dotychczas nieznane zagrożenia cybernetyczne [1, 12, 88, 144, 146, 151, 161, 162, 163, 175, 249, 250, 292, 323]. Dotychczasowe tradycyjne zagrożenia cywilizacyjno-techniczne (np. toksyczne, radiacyjne, medyczne) są stosunkowo dobrze rozpoznane. Prace nad zagrożeniami cybernetycznymi w kraju są stosunkowo skromne, bardzo wycinkowe, niepopularyzowane, a wręcz nieznane szerokiemu ogółowi użytkowników komputerów, w tym inżynierom i studentom. Nieznane jest również szerokiemu ogółowi prawodawstwo krajowe i unijne poświęcone temu zagadnieniu.

Według niektórych ekspertów [175] w Polsce nie podjęto dotychczas działań na poziomie państwowym, aby uregulować

Tabela 2. Wykaz maszyn i urządzeń w cementowni „ODRA" SA

L.p.	Nazwa i rodzaj urządzenia i maszyny	Liczba urządzeń
1	Piec obrotowy do wypału klinkieru	1
2	Układ młyna surowca	1
3	Układ młyna węgla	1
4	Młyny cementu	7
5	Młyn żużla	1
6	Kompresory śrubowe pow. 40 m^3/min	6
7	Kompresory śrubowe pow. 15 m^3/min	8
8	Pompy wody technologicznej pow. 50 kW	6
9	Łamacz kamienia wapiennego	2
10	Układ automatycznego pakowania i paletyzowania worków	3
11	Terminal automatycznego załadunku samochodów cystern cementu	1
12	Pompy Fulera transportu cementu	5
13	Silniki 6 kV	14
14	Silniki 400 V i 690 V	359
15	Rozruszniki wodne do silników 6 kV	5
16	Rozruszniki oporowe (taśma fechlarowa) do silników 6 kV	6
17	Układ wyważania dynamicznego wentylatora 1000 kVA	1
18	Pomiar online wnz izolacji silników 6 kV	3
19	Pomiar online drgań względnych wirnika silnika 6 kV	2
20	Pomiar online drgań bezwzględnych układu napędowego	10
21	Falownik chłodzony cieczą 1200 kVA	1
22	Falowniki powyżej 1000 kVA	4
23	Falowniki od 400 do 1000 kVA	5
24	Falowniki od 100 do 400 kVA	12
25	Falowniki od 15 do 100 kVA	48
26	Falowniki do 15 kVA	67
27	Kompresory sprężonego powietrza	34
28	Przekładnie	265
29	Wentylatory powyżej 400 kW	5
30	Wentylatory od 100 kW do 400 kW	12
31	Wentylatory poniżej 100 kW	30
32	Dmuchawy	14

rosnące zagrożenia cyberatakami na instalacje przemysłowe. Nie ma ośrodka koordynującego przeciwdziałanie takim zagrożeniom [175]. Takich działań nie podjęły również organizacje przemysłowe. Niski priorytet cyberbezpieczeństwa w przemyśle wynika z braku poczucia realnego zagrożenia [175].

Cyberbezpieczeństwo w ocenie autorów monografii w kraju jest niedoceniane i bardzo często mamy do czynienia z poglądem, że stanowi zbędne obciążenie w strukturze wydatków w zakładzie przemysłowym, banku czy w biurze projektowym. Według firmy COMARCH (Raport NERC z 2007 r.) [88] zagrożenia w zakresie cyberbezpieczeństwa w zakładzie przemysłowym, banku czy w biurze projektowym wynikają głównie z powodu:

1) nieodpowiedniej polityki bezpieczeństwa, nieodpowiednich procedur, złej kultury pracy;
2) braku wielu niezależnych warstw zabezpieczeń (ang. *defence in depth*);
3) udostępnienia zdalnego dostępu bez odpowiedniej kontroli;
4) złego zarządzania systemami administracyjnymi;
5) źle zabezpieczonej komunikacji bezprzewodowej;
6) braku dedykowanego kanału komunikacji dla sieci przemysłowych lub używania tego kanału do innych celów;
7) braku odpowiednich narzędzi do monitoringu sieci i wykrywania anomalii;
8) istnienia nieautoryzowanych aplikacji i urządzeń w sieci przemysłowej;
9) braku mechanizmów uwierzytelniania przesyłanych danych;
10) źle zaprojektowanej lub źle zarządzanej infrastruktury krytycznej.

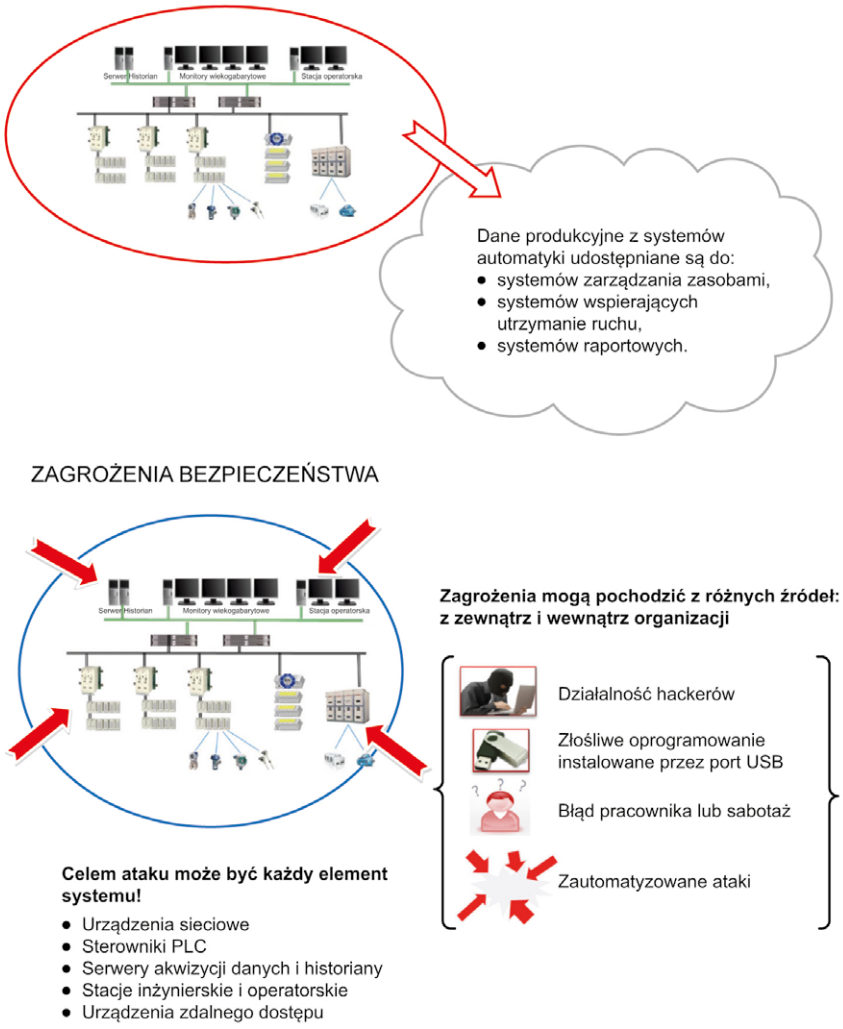
2.2. Systemy sterowania i automatyki

W ciągu ostatnich ok. 10–20 lat w wielu zakładach przemysłowych systemy sterowania i automatyki przeszły z dedykowanego sprzętu i oprogramowania na powszechnie dostępne i użytkowane również w innych celach [162]. Dawniej były:

- dedykowany sprzęt komputerowy;
- dedykowane systemy operacyjne, np. QNX, DEC Unix, Open VMS;
- głównie połączenia „po drutach" lub połączenia szeregowe, bezpośrednie. Obecnie są używane:
- uniwersalne serwery klasy PC;
- uniwersalne systemy operacyjne, np. Windows lub Linux;
- otwarte protokoły komunikacyjne.

Należy stwierdzić, że systemy sterowania i automatyki są narażone na podobne zewnętrzne zagrożenia jak inne systemy i komputery pracujące np. w sieciach biurowych, rys. 2 [162].

Systemy sterowania i automatyki we wszystkich zakładach przemysłowych, w tym w cementowniach, są coraz ściślej zintegrowane z systemami korporacyjnymi. Większa integracja to z jednej strony szereg korzyści, z drugiej powstawanie zagrożeń wynikających z łączenia dwóch odrębnych podsieci



Rys. 2. Świat cyberataków w sterowaniu i automatyce [162]

(przemysłowej i biurowej), rys. 2 [162].

W początkowym okresie użytkowania komputerów, przy niewielkiej liczbie komputerów podłączonych do sieci, cyberbezpieczeństwo zapewniały przyjęte przez ludzi zasady używania komputerów, systemy operacyjne i oprogramowanie. Było to możliwe głównie dzięki ograniczonej liczbie profesjonalnych i wysoce odpowiedzialnych użytkowników. Z upływem czasu liczba użytkowników lawinowo rośnie, codziennie do Internetu podłączane są miliony nowych użytkowników. Model odpowiedzialnego użytkownika i samokontroli stał się niewystarczający [1]. Początkowo cyberprzestępcami byli początkujący, niedoświadczeni hakerzy, dla których celem było uzyskanie nieuprawnionego dostępu do komputera, podmiana strony internetowej itp. Współcześnie są to zmasowane udane ataki na instytucje państwowe, banki, organizacje gospodarcze, fabryki, elektrownie, systemy energetyczne, szpitale czy obiekty militarne, wykonywane najczęściej przez „zawodowców". Poważne ataki hakerskie stały się normą.

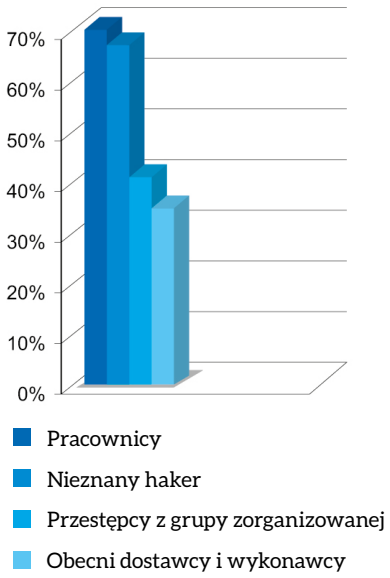
W 2015 roku, wg danych PZU, za cyberataki w Polsce byli odpowiedzialni przede wszystkim pracownicy danej firmy (rys. 3) [145].

Celem ataku jest najczęściej produkcja w zakładzie przemysłowym lub w energetyce [162].

Cyberprzestępcy realizują swoje zadanie przez:

- wykradanie bądź zmodyfikowanie wrażliwych danych;
- sabotaż sieci bądź instalacji.

Możliwe konsekwencje cyberataków [292] to:



Rys. 3. Struktura cyberataków w kraju w 2015 r. [144]

- brak dostępu do systemu produkcyjnego;
- utrata wydajności systemu;
- manipulacja / utrata / kradzież danych;
- utrata kontroli nad produkcją;
- zatrzymanie produkcji/maszyn;
- katastrofa ekologiczna;
- ryzyko śmierci i poważnych obrażeń pracowników;
- straty finansowe;
- nadszarpnięty wizerunek firmy.

Cyberbezpieczeństwo zawsze będzie zależało od najsłabszego węzła bądź ogniwa systemu. Profesjonalni użytkownicy komputerów wiedzą, że cyberbezpieczeństwo jest podstawą funkcjonowania na co dzień. Jak twierdzi Przemysław Kania, Dyrektor Generalny CISCO: *w walce z cyberprzestępczością zawsze będziemy ten jeden krok za hakerami, to ciągła pogoń i doskonalenie naszych systemów przeciwdziałania. Im większa współpraca na poziomie korporacji i państw, tym bliżsi jesteśmy zwycięstwa* [324].

Potencjalne konsekwencje ataku cybernetycznego na zakład przemysłowy są najczęściej następujące:

- wyłączenie instalacji (prostsze do przeprowadzenia);
- zniszczenie instalacji albo spowodowanie znaczących strat materialnych.

Ataki cybernetyczne dotyczą coraz niższej warstwy struktury zakładu, obiektu, biura. Są coraz trudniejsze do wykrycia i jest ich z dnia na dzień coraz więcej.

2.3. Przykłady ataków cybernetycznych

Oto kilka przykładów ataków cybernetycznych [1, 12, 88, 144, 146, 151, 161, 162, 163, 175, 249, 250, 292, 323]:

- 2003 – atak na elektrownię atomową w Ohio (USA) i przewoźnika kolejowego CSX Corporation;
- 2004 – atak na British Airways, Railcorp, Delta Airlines;
- 2009 – atak na koncerny petrochemiczne Shell, Exxon, BP;
- 2009–2010 – wirus *Stuxnet* w obiektach nuklearnych w Iranie, który ponad rok skutecznie uszkadzał wirówki do produkcji paliwa jądrowego w zakładach wzbogacania uranu w Natanz; atak nastąpił przy wykorzystaniu zainfekowanej pamięci podręcznej USB, a dotyczył programowalnych sterowników logicznych PLC, a na przeszkodzie nie stanęły ani specjalistyczne oprogramowanie, ani brak połączenia z Internetem [1];
- 10 kwietnia 2014 roku amerykański niszczyciel Donald Cook przypłynął na Morze Czarne. Dnia 12 kwietnia przelatywał nad nim rosyjski bombowiec Su-24, nie posiadając ani bomb, ani rakiet, tylko elektroniczny przyrząd wojenny – gondolę zamontowaną pod kadłubem, która według rosyjskiego czasopisma „Rossiyskaya Gazeta" zawierała elektroniczny przyrząd wojenny. Podczas fazy zbliżania się przyrząd ten miał zneutralizować wszystkie radary niszczyciela Donald Cook, urządzenia kontrolne, systemy informacyjne itp. Niszczyciel USA był wyposażony w system ostatniej generacji Aegis, który zapewnia łączność między systemami obrony przeciwrakietowej wszystkich okrętów, na których jest zainstalowany (w ten sposób tworzy się sieć, która gwarantuje wychwytywanie, ściganie i zniszczenie setek celów w tym samym czasie). Innymi słowy, ten wszechpotężny system, współcześnie używany i montowany na okrętach wojennych NATO w celach obronnych, został wyłączony jak telewizor pilotem. Donald Cook jest niszczycielem z wyrzutniami rakiet czwartej generacji, którego podstawową bronią jest rakieta samosterująca Tomahawk z zasięgiem 2,5 tys. km, mogąca przenosić głowice nuklearne. W ramach rutynowej misji USS Donald Cook ma na pokładzie 56 rakiet Tomahawk, a w konfiguracji ofensywnej – 96. Donald Cook jest również wyposażony w cztery duże radary, których wydajność można porównać z mocą wielu stacji radarowych. W celach obronnych ma on jeszcze 50 rakiet przeciwlotniczych różnych typów. Ministerstwo Spraw Zagranicznych USA przyznało, że załoga niszczyciela Donalda Cooka była mocno zdemoralizowana po ataku cybernetycznym wykonanym przez rosyjski bombowiec Su-24 [323];
- 2014 – atak na huty stali w Niemczech;
- 2015 – wirus BlackEnergy przejął kontrolę nad systemami automatycznego sterowania lokalnymi sieciami energetycznymi w zachodniej Ukrainie [1];
- cyberatak na sektor energetyczny Ukrainy [151]: 23 grudnia 2015 roku o 15:30 operator w centrum sterowania zauważa podejrzane zachowanie się systemu operacyjnego. Intruzi, działając zdalnie, doprowadzają do wyłączenia na 3 godziny stacji elektroenergetycznych: 7–110 kV i 23–35 kV. Atak na trzech dystrybutorów powoduje brak dostaw energii elektrycznej dla ponad 200 000 odbiorców (zdarzały się szacunki mówiące o 1 milionie klientów);
- 10 listopada 2017 roku została zaatakowana strona internetowa lotniska w Modlinie [250];
- w marcu 2018 roku zaatakowano serwery Teatru Współczesnego w Warszawie – w cyberataku przejęto plany widowni na spektakle grane od 21 marca do 6 maja [250];
- 20 marca 2018 roku nastąpił groźny cyberatak na polskie banki – w zamiarze atakujących było przejęcie prawdziwych loginów i haseł, a następnie wyprowadzenie pieniędzy z kont ich właścicieli [250].

2.4. Krajowe uregulowania prawne

Regulacje prawne w zakresie cyberbezpieczeństwa w naszym kraju współcześnie są określone w dokumentach [33, 163]:

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dn. 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii;
- Uchwała nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022;
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. z dn. 13 sierpnia 2018, poz. 1560.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa ma następujące cele:

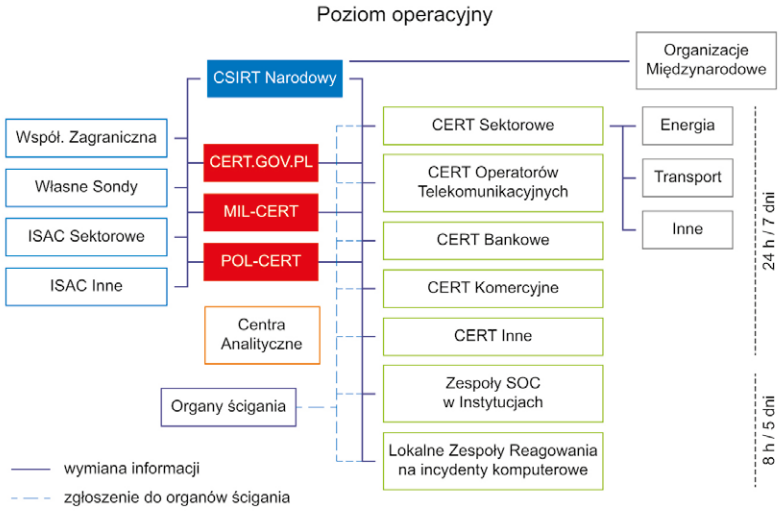
- organizacja systemu cyberbezpieczeństwa na poziomie krajowym;
- ustanowienie obowiązków podmiotów zobowiązanych;
- określenie zasad nadzoru i kontroli;
- określenie zakresu Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Krajowy system cyberbezpieczeństwa (rys. 4) [163] ma na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym:

- niezakłócone świadczenie usług kluczowych i usług cyfrowych;
- osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług;
- obsługę incydentów.

W ustawie zdefiniowano następujące pojęcia:

- usługa kluczowa – usługa o kluczowym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymieniona w wykazie usług kluczowych;
- operator usługi kluczowej – podmiot z sektora energetyki (w tym m.in. podsektorów energii elektrycznej, ropy, gazu, wydobywania kopalin, ciepła), transportu, bankowości, infrastruktury rynków finansowych, służby zdrowia, zaopatrzenia w wodę pitną, infrastruktury cyfrowej, w stosunku do którego została wydana decyzja o uznaniu za operatora usługi kluczowej;
- dostawca usługi cyfrowej – podmiot świadczący usługę przetwarzania w chmurze, wyszukiwarki internetowej oraz internetowej platformy handlowej;



Rys. 4. Organizacja systemu cyberbezpieczeństwa w kraju [163]

- cyberbezpieczeństwo – odporność systemów informacyjnych na działania naruszające dostępność, autentyczność, integralność i poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne;
- incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo;
- incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości świadczonej usługi kluczowej lub przerwanie ciągłości świadczenia usługi kluczowej;
- incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV;
- incydent w podmiocie publicznym – incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny;
- CSIRT – zespół reagowania na incydenty poziomu krajowego;
- obsługa incydentu – czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu.

Dobrymi praktykami w przeciwdziałaniu cyberatakom są następujące czynności i techniczne przedsięwzięcia [292]:

- zabezpieczenie komputerów i sterowników przed szkodliwym oprogramowaniem, nieuprawnionym dostępem, sabotażem, szpiegostwem i manipulacją;
- stosowanie bezpiecznej komunikacji w sytuacji globalnego wykorzystania maszyn;
- wykorzystanie komunikacji zdalnej w celu uniknięcia drogich wizyt serwisowych;
- systematyczne diagnozowanie systemu zabezpieczeń przed cyberatakami, aktualizacja zabezpieczeń.

W jaki sposób można zatem praktycznie zapewnić cyberbezpieczeństwo w firmie, na przykład w cementowni? Najlepszym rozwiązaniem jest skorzystanie z usług specjalistycznej firmy informatycznej mającej doświadczenie w tej dziedzinie. Wyboru można dokonać, chociażby uczestnicząc w specjalistycznych konferencjach [1, 12, 88, 144, 146, 151, 161, 162, 163, 175, 249, 250, 292, 323]. Zagadnienia o wadze strategicznej (usługa kluczowa) można skonsultować z Ministerstwem Cyfryzacji RP. ■

Bibliografia dostępna pod linkiem:
nis.com.pl/bibliografia.html

Fragment pochodzi z książki:
Utrzymanie ruchu w przemyśle,
Sławomir Szymaniec, Marek Kacperak
Wydawnictwo Naukowe PWN,
Warszawa 2021