Mikołaj Dobski[1]
Gerard Frankowski[2]
Norbert Meyer[3]
Michał Pilc[4]
Mateusz Twardawa[5]

Zastosowanie metod uczenia maszynowego i zaawansowanego przetwarzania zdarzeń dla ochrony przemysłowych sieci infrastruktury krytycznej

[1] Mgr inż. Mikołaj Dobski — analityk systemów i programista w Dziale Bezpieczeństwa ICT Poznańskiego Centrum Superkomputerowo-Sieciowego. W PCSS pracuje od 2010 r., jednak w Dziale Bezpieczeństwa ICT od 2016 r. Absolwent studiów dziennych magisterskich na Politechnice Poznańskiej na kierunku informatyka oraz o specjalności komputerowe systemy wspomagania decyzji i rozproszone systemy komputerowe. Uczestnik polskich i europejskich projektów naukowo-badawczych. Specjalizuje się w bezpieczeństwie systemów internetu rzeczy oraz w zastosowaniu metod uczenia maszynowego do niesygnaturowej detekcji zagrożeń bezpieczeństwa. W ramach projektu SCADvance współtworzy modele analityczne oraz odpowiada za podbudowę technologiczną opracowywanego rozwiązania.

Adres do korespondencji: <mikolaj.dobski@man.poznan.pl>.

[2] Mgr inż. Gerard Frankowski — kierownik Działu Bezpieczeństwa ICT Poznańskiego Centrum Superkomputerowo-Sieciowego, analityk systemów komputerowych. Ukończył studia magisterskie na Politechnice Poznańskiej na kierunku informatyka oraz o specjalności komputerowe systemy wspomagania decyzji. W PCSS pracuje od 2003 r. Specjalizuje się w zakresie systemowych oraz aplikacyjnych testów penetracyjnych, audytów kodu źródłowego w kilku językach programowania, bezpieczeństwa serwerów aplikacyjnych. Uczestnik licznych polskich i europejskich projektów naukowo-badawczych w zakresie badań nad cyberbezpieczeństwem, współautor kilkunastu publikacji naukowych. Kierownik techniczny badań realizowanych w PCSS w ramach projektu SCADvance.

Adres do korespondencji: <gerard.frankowski@man.poznan.pl>.

[3] Dr inż. Norbert Meyer — kierownik Pionu Technologii Przetwarzania Danych Poznańskiego Centrum Superkomputerowo-Sieciowego. Absolwent Politechniki Poznańskiej — tytuł doktora uzyskał w 2001 r. Zainteresowania badawcze obejmują m.in. zarządzanie zasobami i danymi rozliczeniowymi w gridach, technologie rozwoju interfejsów użytkownika, bezpieczeństwo sieciowe. Kierownik Pionu Technologii Przetwarzania Danych PCSS. Współtworzył centrum obliczeniowe Komputerów Dużej Mocy w PCSS. Współautor koncepcji, projektów oraz realizacji grantów celowych i europejskich PCSS w zakresie usług obliczeniowych, gridowych, bezpieczeństwa oraz składowania danych. Autor i współautor ok. 80 publikacji naukowych.

Adres do korespondencji: <meyer@man.poznan.pl>.

Wstęp

Infrastruktura krytyczna (dalej jako IK) to rzeczywiste i cybernetyczne systemy (obiekty, urządzenia bądź instalacje) niezbędne do minimalnego funkcjonowania gospodarki i państwa[6]. Infrastruktura krytyczna jest kluczowym elementem z punktu widzenia bezpieczeństwa narodowego, stabilności i rozwoju gospodarczego, funkcjonowania społeczeństw oraz pojedynczych obywateli[7].

Straty ponoszone w wyniku ataku na IK mogą być bardzo wysokie. Niezwykle trudno jest wyznaczyć globalny wzór pozwalający określić wysokość strat, jednakże przytoczyć można wybrane dane szacunkowe. Według raportu organizacji ENISA (ang. *European Union Agency for Network and Information Security*) przeciętny koszt ponoszony przez operatora IK w związku z pojedynczym atakiem może wynieść nawet 2,3–15 mln euro, zaś całkowity koszt wszystkich ataków w wybranych krajach Unii Europejskiej może sięgać 1,6% PKB. Za najbardziej zagrożone uważa się sektory: energetyczny, finansowy oraz technologii informacyjno-komunikacyjnych (dalej jako ICT), a najbardziej kosztowne ataki na IK powiązane są z zagrożeniami wewnętrznymi (ang. *insider threats*) oraz atakami odmowy dostępu do usługi (ang. *Denial of Service — DoS*)[8].

---

[4] Mgr inż. Michał Pilc — analityk systemów w Dziale Bezpieczeństwa ICT Poznańskiego Centrum Superkomputerowo-Sieciowego. Ukończył studia magisterskie na Politechnice Poznańskiej na kierunku elektronika i telekomunikacja oraz o specjalności systemy telekomunikacyjne. Specjalizuje się m.in. w bezpieczeństwie sieci bezprzewodowych, internetu rzeczy, kryptografii, bezpieczeństwie sprzętowym. Pisze rozprawę doktorską na temat zabezpieczania sieci bezprzewodowych MIMO w warstwie fizycznej. Prowadzi prace badawcze w zakresie projektowania bezpiecznej architektury sieci teleinformatycznych nowej generacji: 5G, sieci IoT i SCADA. Autor i współautor kilkunastu publikacji naukowych.

Adres do korespondencji: <michal.pilc@man.poznan.pl>.

[5] Lic. Mateusz Twardawa — analityk danych w Dziale Bezpieczeństwa ICT Poznańskiego Centrum Superkomputerowo-Sieciowego. Ukończył studia licencjackie z biologii eksperymentalnej, obecnie studiuje bioinformatykę na Wydziale Informatyki Politechniki Poznańskiej. Specjalizuje się w biologii teoretycznej, modelowaniu matematycznym, statystyce i analizie probabilistycznej oraz uczeniu maszynowym i głębokim. Od 2017 r. związany z PCSS jako programista i specjalista od analizy danych, uczenia maszynowego oraz statystyki w projekcie SCADvance, gdzie wraz z zespołem współtworzy moduł analityczny służący do detekcji anomalii w sieciach przemysłowych.

Adres do korespondencji: <mtwardawa@man.poznan.pl>.

[6] Rządowe Centrum Bezpieczeństwa, *Infrastruktura krytyczna*, <https://rcb.gov.pl/infrastruktura-krytyczna>, 20 marca 2017 r.

[7] G. Abgarowicz i in., *Bezpieczeństwo infrastruktury krytycznej — wymiar teleinformatyczny*, Kraków 2014, s. 5.

[8] ENISA, *The cost of incidents affecting CIIs — systematic review of studies concerning economic impact of cyber-security incidents on critical information infrastructures (CII)*, Athens 2016, s. 25.

Wspomniane straty nie muszą mieć charakteru ściśle materialnego. W 1999 r. wyciek ropy z rurociągu Whatcom Creeks Washington i jej pożar, spowodowany atakiem cybernetycznym na niewłaściwie zaimplementowany system SCADA rurociągu, obok 45 mln dol. strat spowodował śmierć 3 osób oraz niepowetowane straty w środowisku naturalnym[9].

Rozwiązania technologii informacyjnych i operacyjnych (dalej jako IT/OT), jako kluczowe dla funkcjonowania IK, nie są obecnie odpowiednio wyposażone w systemy zabezpieczające i monitorujące, a operatorzy IK nie są wystarczająco wykwalifikowani w kontekście ich bezpieczeństwa. Systemy te należy uważać za najsłabsze ogniwo całej IK państw, co implikuje szczególną ekspozycję na ataki, w tym przeprowadzane przez grupy o charakterze przestępczym, cyberterrorystycznym czy cyberwojennym. Celem ataków może być paraliż funkcjonowania zaatakowanej IK, jej destabilizacja lub nawet zniszczenie[10].

Wyzwania ochrony współczesnych systemów informatycznych

Aktualne spektrum zagrożeń

Liczba oraz stopień komplikacji zagrożeń w ostatnich latach wyraźnie rosną. W 2017 r. zanotowano zdecydowanie najwięcej podatności bezpieczeństwa oprogramowania opatrzonych kodem CVE (ang. *Common Vulnerabilities and Exposures*) — 14712; w latach poprzednich nie więcej niż 6–8 tys. unikalnych podatności[11]. W tym samym roku amerykański ICS CERT[12] opublikował informacje o 322 podatnościach bezpieczeństwa systemów automatyki przemysłowej. Najwięcej luk (178,55,28%) dotyczyło sektora energetycznego. Liczba podatności ocenionych jako krytyczne w skali Common Vulnerability Scoring System (co najmniej 7 punktów w 10-stopniowej skali) wyniosła 194 (60,25%)[13].

Sama liczba publicznie znanych podatności wskazuje na niekorzystne tendencje, ale nie jest szczególnym wyzwaniem. Na każdą taką podatność producent oprogramowania może opracować łatę, a dostawca systemów bezpieczeństwa — sygnaturę. Prawdziwym problemem stają się ataki

[9] S. Samtani i in., *Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques* [w:] *IEEE Conference on Intelligence and Security Informatics*, Tucson 2016, s. 25–30.

[10] G. Abgarowicz i in., *Bezpieczeństwo infrastruktury krytycznej...*, wyd. cyt., s. 69.

[11] CVE Details, *Browse Vulnerabilities by Date*, <https://www.cvedetails.com/browse-by-date.php>, 6 kwietnia 2018 r.

[12] The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), <https://ics-cert.us-cert.gov>, 22 marca 2017 r.

[13] Kaspersky Lab ICS-CERT, *Threat Landscape for Industrial Automation Systems in H2 2017*, <https://ics-cert.kaspersky.com/media/KL_ICS_REPORT_H2-2017_FINAL_EN_22032018.pdf>, 30 marca 2017 r.

o znacznym stopniu skomplikowania i bazujące na wcześniej nieznanych zagrożeniach (ang. *0-day exploits*).

Ewolucja złośliwego oprogramowania w kierunku samopropagujących się (niewymagających do rozprzestrzeniania się żadnej aktywności atakowanych użytkowników) jest jednym z najważniejszych identyfikowanych trendów w zakresie cyberzagrożeń. Ponadto zauważa się, że rzeczywistym celem autorów złośliwego oprogramowania (ang. *malware*) nie musi być bezpośredni zysk finansowy (np. okup), ale uniemożliwienie korzystania z zaatakowanych systemów — jak w przypadku ataku Nyetya, w którym złośliwy ładunek jedynie symulował działanie charakterystyczne dla oprogramowania typu *ransomware*[14].

Problemy analityczne

Współczesne sieci teleinformatyczne zabezpieczane są zgodnie ze strategią ochrony dogłębnej (ang. *defence-in-depth*). Jest to podejście do ochrony zasobów IT, które polega na zdolności do minimalizacji ryzyka przy pomocy zróżnicowanych strategii ochronnych, aby w przypadku udanego przełamania jednego lub dwóch systemów zabezpieczeń pozostałe nadal chroniły system i dane[15].

Konsekwencją zastosowania takiego podejścia jest także zwiększona ilość danych do analizy pochodzących z systemów monitorujących (np. klasy SIEM) czy bezpośrednio z uruchomionych usług (pliki logów serwerów czy urządzeń). Przykładowo przyrost dzienny wielkości plików ze zdarzeniami przetwarzanych przez system SIEM Ministerstwa Spraw Zagranicznych to ok. 20 GB[16]. Centrum cyberbezpieczeństwa firmy HP notuje dziennie od 100 mld do nawet 1 bln zdarzeń mogących mieć związek z bezpieczeństwem, z których jest w stanie przetwarzać ok. 3 mld[17]. Z oczywistych przyczyn ta ogromna ilość informacji powinna być przetwarzana w czasie rzeczywistym albo przynajmniej quasi-rzeczywistym. Jak wynika z przytoczonych danych, a także z dorocznych raportów Mandiant Consulting — aktualnie tak nie jest. Przeciętny czas od przejęcia systemu przez cyberprzestępcę do wykrycia tego faktu (ang. *dwell time*) jest nadmiernie długi. W 2014 r. wyniósł 205 dni, skracając się do 146 dni w 2015 r. i 99 dni w 2016 r. W 2017 r. nastąpiło odwrócenie trendu — *dwell time* wydłużył się niewiele — do 101 dni[18].

---

[14] Cisco, *Cisco 2018 Annual Cybersecurity Report*, San Jose 2018, s. 3.

[15] J. Viega, G. McGraw, *Building Secure Software: How to Avoid Security Problems the Right Way*, Boston 2002, s. 96–97.

[16] Ministerstwo Spraw Zagranicznych, *Specyfikacja Istotnych Warunków Zamówienia. Postępowanie o udzielenie zamówienia publicznego na dostawę zarządzalnego i administrowanego środowiska w architekturze chmury dla Ministerstwa Spraw Zagranicznych*, Warszawa 2016, s. 56.

[17] S. Bhatt, P.K. Manadhata, L. Zomlot, *The Operational Role of Security Information and Event Management Systems*, „IEEE Security & Privacy" 2014, No. 12, s. 35–41.

[18] Mandiant Consulting, *M-Trends 2016. Special Report*, 2016, s. 2, <https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf>, 5 maja 2017 r.;

Metody badawcze w walce z zagrożeniami cyberbezpieczeństwa

Wykorzystanie paradygmatu Big Data

W kontekście modelu przetwarzania Big Data wprowadza się pojęcie jeziora danych (ang. *Data Lake*), za które uznaje się pojedyncze repozytorium dużych rozmiarów, zdolne do przechowywania wszystkich danych (o różnej strukturze) związanych z konkretnym zagadnieniem, a także łatwego udostępniania ich narzędziom analitycznym[19]. W przypadku zastosowania koncepcji jeziora danych dla cyberbezpieczeństwa, podstawowym wyzwaniem dla mechanizmów analitycznych jest ekstrakcja właściwych informacji (ang. *actionable information*) oraz utworzenie z nich wiedzy pozwalającej na podjęcie konkretnych działań w reakcji na realnie występujący problem. Celem aparatu analitycznego jest tu przede wszystkim identyfikacja nieoczywistych zagrożeń, awarii, nadużyć lub identyfikacja przyczyn źródłowych incydentów bezpieczeństwa zauważonych w inny sposób[20]. Problemem pozostaje właściwy dobór mechanizmów analitycznych pozwalających ten cel osiągnąć. Wybrane kluczowe rozwiązania opisano poniżej.

Detekcja ataków ukierunkowanych

Kluczowym problemem dla IK jest identyfikacja zagrożeń typu APT (ang. *Advanced Persistent Threats*), czyli długotrwałych ataków ukierunkowanych, przede wszystkim zorientowanych na bieżące pozyskiwanie cennych informacji lub zachowanie stałej kontroli nad celem przy użyciu ustanowionego kanału informacyjnego. Techniki APT są wykorzystywane m.in. w szpiegostwie przemysłowym. Z racji rozciągnięcia wszystkich działań w czasie i stosunkowo niewielkiego wolumenu ruchu związanego z tego rodzaju atakami nie są one łatwe do zidentyfikowania przez klasyczne systemy detekcji[21]. Co gorsza, ataki APT oparte są najczęściej na wykorzystaniu nieznanych publicznie podatności. Dla tego rodzaju luk nie są zatem dostępne sygnatury, które umożliwiłyby zasygnalizowanie zagrożenia klasycznym systemom bezpieczeństwa, takim jak np. zapora

także: tenże, *M-Trends 2017. Special Report*, 2017, s. 7, <https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html>, 5 maja 2017 r.; tenże, *M-Trends 2018. Special Report*, 2018, s. 4, <https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf>, 4 kwietnia 2018 r.

[19] R. Marty, *The security Data Lake: Leveraging Big Data technologies to Build a Common Repository for Security*, O'Reilly, 2015, s. 1, <http://www.oreilly.com/data/free/security-data-lake.csp>, 4 kwietnia 2018 r.

[20] M. Dobski i in., *Security Monitoring and Analytics in the Context of HPC Processing Model* [w:] R. Wyrzykowski i in. (red.), *Parallel Processing and Applied Mathematics, 12th International Conference, PPAM 2017, Lublin, Poland, September 10–13, 2017, Revised Selected Papers, Part I*, Cham 2018, str. 406–416.

[21] Tamże.

sieciowa (ang. *firewall*) czy oprogramowanie antywirusowe. Wykrycie tak przygotowanego ataku wymaga zdolności detekcji zachowania anomalnego, wdrożenia mechanizmu korelacji informacji z wielu systemów, możliwości zidentyfikowania zagrożenia i wreszcie — wdrożenia odpowiedniej reakcji, zatem systemy wykrywania włamań, oparte na analizie behawioralnej i detekcji anomalii, są aktualnie jedyną (i to — z uwagi na niejednoznaczność wskazań — niepełną) metodą walki z atakami APT[22].

Zaawansowane przetwarzanie zdarzeń

Paradygmat zaawansowanego przetwarzania zdarzeń (ang. *Complex Event Processing*) opiera się na idei analizy zdarzeń generowanych przez wiele źródeł oraz wykrywaniu w nich złożonych wzorców w czasie rzeczywistym lub quasi-rzeczywistym bez potrzeby długookresowego przechowywania całości informacji o danym zdarzeniu. W ramach silnika CEP zdarzenia najczęściej są dzielone na osobne strumienie zdarzeń, a następnie korelowane w ramach określonych okien czasowych oraz przy użyciu języka regułowego, w którym można budować złożone, dziedzinowe reguły korelacji. Podejście CEP ukierunkowane jest na analizę maksymalnie wielu zdarzeń oraz możliwie szybkie ich raportowanie operatorowi[23].

Kierunki technologiczne dla zapewnienia właściwej ochrony infrastruktury krytycznej

Monitoring zagrożeń i podatności jest uważany za warunek konieczny na drodze do zapewniania bezpieczeństwa systemów przemysłowych IK. Operator musi w tym celu korzystać z odpowiednich systemów bezpieczeństwa, wśród pożądanych cech których wymienia się m.in. następujące właściwości:

— brak wpływu, rozumianego jako możliwość wprowadzenia zmian w monitorowanych systemach, w szczególności ich uszkodzenia,
— wykrywanie, w miarę możliwości, podatności typu 0-day (natychmiast po pierwszym pojawieniu się na świecie, a więc jeszcze przed publikacją odpowiedniego uaktualnienia podatnego oprogramowania[24]).

Znaczenie paradygmatu Big Data dla poprawy poziomu cyberbezpieczeństwa stało się kluczowe. Zaawansowana analityka Big Data, oparta na algorytmach uczenia maszynowego, sprawdza się doskonale, przetwarzając napływające nieustannie z różnorodnych strumieni duże ilości danych oraz umożliwiając wykrycie anomalii, które inaczej pozostałyby

[22] A. Kliarsky, A. Atlasis, *Responding to Zero Day Threats*, SANS Institute 2011, s. 7–8, <http://www.sans.org/reading-room/whitepapers/incident/respondingzero-day-threats-33709>, 5 kwietnia 2018 r.

[23] G. Frankowski i in., *Application of the Complex Event Processing system for anomaly detection and network monitoring*, „Computer Science Journal" 2015, No. 4, s. 351–372.

[24] G. Abgarowicz i in., *Bezpieczeństwo infrastruktury krytycznej*..., wyd. cyt., s. 73–74.

niezauważone. Badanie przeprowadzone w Stanach Zjednoczonych Ameryki, m.in. wśród agencji rządowych, wskazało, że 84% respondentów do blokowania ataków wykorzystało analitykę Big Data[25]. Z kolei 92% specjalistów bezpieczeństwa uznało, że systemy ochronne działające na zasadzie analizy behawioralnej sprawdzają się w działaniu, a 69% przedstawicieli sektora opieki zdrowotnej uznało analizę zachowań za wyjątkowo skuteczną w identyfikowaniu autorów ataków sieciowych[26]. W istotny sposób wyraża to zarówno oczekiwania użytkowników, jak i determinuje najlepiej rokujące kierunki badań nad detekcją zaawansowanych zagrożeń.

Badania Poznańskiego Centrum Superkomputerowo-Sieciowego nad cyberbezpieczeństwem na przykładzie projektu Scadvance

Wprowadzenie

Poznańskie Centrum Superkomputerowo-Sieciowe jest afiliowane przy Instytucie Chemii Bioorganicznej Polskiej Akademii Nauk. Jest operatorem ogólnopolskiej szerokopasmowej sieci optycznej dla nauki PIONIER, stanowiącej podstawę do tworzenia zaawansowanych usług dla nauki, posiada bezpośrednie połączenia z sieciami naukowymi krajów sąsiednich, a za ich pośrednictwem — z paneuropejską siecią dla nauki GÉANT[27]. Jednym z kluczowych obszarów działalności jednostki jest realizacja projektów naukowo-badawczych, w tym z dziedziny cyberbezpieczeństwa.

Projekt *SCADvance (SCAda Advance): opracowanie metod i rozwiązań zwiększających bezpieczeństwo sieci przemysłowej dla firm sektora elektroenergetycznego* (dalej jako projekt SCADvance) realizowany jest ze środków Wielkopolskiego Regionalnego Programu Operacyjnego na lata 2014–2020[28]. Beneficjentem projektu jest ALMA S.A., z kolei PCSS (obok Politechniki Poznańskiej oraz XNet Communications Sp. z o.o.) świadczy w ramach projektu usługi badawcze — z przede wszystkim w zakresie tworzenia modeli obliczeniowych dla detekcji zagrożeń w 6 protokołach sieci przemysłowych: DNP3, MODBUS, ProfiNET, Powerlink, Profibus, CANopen. Tworzenie modeli analitycznych dla detekcji anomalii przewidziane jest na 2018 r.

Ogólną architekturę systemu w zakresie realizowanym przez PCSS przedstawiono na poniższym rysunku.

[25] S. Gliwa, A. Kozłowski, *Piotr Prajsnar: Big Data przyczynia się do zmniejszenia liczby włamań do systemów komputerowych*, <http://www.cyberdefence24.pl/piotr-prajsnar-big-data-przyczynia-sie-do-zmniejszenia-liczby-wlaman-do-systemow-komputerowych>, 5 kwietnia 2018 r.

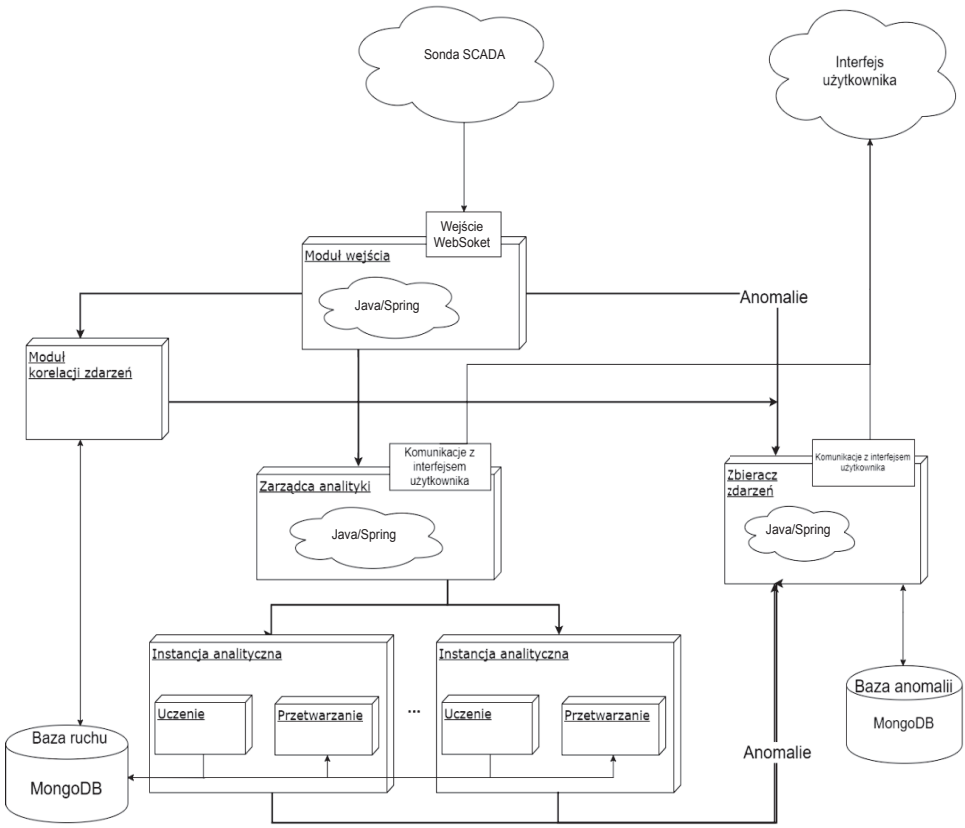
[26] Cisco, *Cisco 2018 Annual...*, wyd. cyt., s. 11.

[27] M. Stroiński, J. Węglarz, *Znaczenie e-infrastruktury dla nauki*, „Nauka" 2008, nr 2, s. 57–94.

[28] ALMA S.A., *SCADVANCE*, <http://www.alma.biz.pl/projekty-ue-2/scadvance>, 29 marca 2018 r.

Rysunek 1

Architektura modułu analitycznego systemu SCADvance



Źródło: opracowanie własne

Na schemacie wskazano najważniejsze części składowe modułu analitycznego wraz z wykorzystywanymi podstawowymi technologiami. Zaznaczono w szczególności podmoduł wykorzystujący zaawansowane przetwarzanie zdarzeń (WSO2) oraz multiplikowane komponenty uczenia maszynowego (ML_Instance) różniące się zastosowanym podejściem. Rodzaje algorytmów opisano w kolejnym podrozdziale — możliwe będzie zastosowanie więcej niż jednego algorytmu dla tych samych danych wejściowych na podstawie decyzji superwizora (ML_Supervisor).

Wykorzystanie algorytmów uczenia maszynowego

Detekcja anomalii w założeniu opiera się na wykrywaniu mało prawdopodobnych zdarzeń w sieci w celu zgłoszenia ich do osoby nadzorującej działanie systemu. Jest to podejście oparte zarówno o statystykę, jak i uczenie maszynowe. W ramach projektu SCADvance prowadzone są badania nad różnymi technikami uczenia maszynowego, dzięki którym

możliwe będzie dobranie optymalnych metod detekcji anomalii w sieciach przemysłowych.

Istnieją dwie ogólne kategorie uczenia maszynowego, które, opierając się na odmiennym podejściu do danych, rozwiązują różne klasy problemów, mianowicie uczenie nadzorowane (z nauczycielem) i nienadzorowane. W ramach projektu zdecydowano się na zastosowanie metod uczenia nienadzorowanego, przede wszystkim z tego tytułu, że algorytmy uczenia z nauczycielem wymagają zbilansowanej liczby przykładów ruchu normalnego i niewłaściwego (anomalii)[29]. Wymagałoby to zatem przygotowania pokaźnego zbioru przykładów ataków — wyżej pokazano, że najgroźniejsze z nich opierają się na publicznie nieznanych podatnościach, więc budowa odpowiednich przykładów jest niemożliwa.

Uczenie nienadzorowane tej wady nie posiada, nie jest jednak, jako podejście ogólne, tak rozbudowane i dobrze sprawdzone w działaniu. Pozwala jednak stworzyć ogólny model behawioralny sieci, przez co jest w stanie wykryć zdarzenia, które do niego nie pasują — nawet jeśli wcześniej nigdy nie wystąpiły. Minusem jest fakt, że jeśli sieć nie działa poprawnie podczas procesu uczenia, pewne anomalie, które na tym etapie się pojawią, mogą zostać uznane za normalne zachowanie sieci[30].

Podczas badań testowane będą metody dotyczące dwóch różnych analiz, tj. analizy ruchu w sieci oraz głębokiej inspekcji pakietów.

Analiza ruchu w sieci pozwala wykryć niewłaściwe parametry komunikacji zarówno dla całej sieci, jak i par odbiorca–nadawca. Do tego celu wykorzystuje się podejście regułowe oraz metody statystyczne i uczenia maszynowego, które najczęściej są także technikami prognozowania zmiennych[31].

Statystyczna kontrola procesów (ang. *Statistical Process Control*) jest powszechnie stosowana do kontroli jakości produkcji. Przy jej pomocy można jednak modelować zachowanie całych sieci przemysłowych, co jest wykorzystywane w celu wykrywania anomalii[32]. W podstawowym wydaniu model polega na wyznaczeniu dolnego i górnego poziomu akceptacji badanego parametru sieci na podstawie historycznych danych o jego zachowaniu (np. liczba pakietów wysłana z urządzenia A do B w czasie 1 sekundy). Każdorazowe przekroczenie wartości granic akceptacji jest traktowane jako anomalia.

---

[29] F. Schuster, A. Paul, H. König, *Towards Learning Normality for Anomaly Detection in Industrial Control Networks* [w:] G. Doyen i in. (red.), *AIMS'13 Proceedings of the 7th IFIP WG 6.6 international conference on Autonomous Infrastructure, Management, and Security: emerging management mechanisms for the future internet*, Vol. 7943, Berlin–Heidelberg 2013, s. 61–72.

[30] B. Koo, B. Shin, T.F. Krijnen, *Employing outlier and novelty detection for checking the integrity of BIM to IFC entity associations* [w:] *Proceedings of the International Symposium on Automation and Robotics in Construction*, Vol. 34, Taipei 2017, s. 1–8.

[31] D. Lee, *Anomaly Detection in Multivariate Non-stationary Time Series for Automatic DBMS Diagnosis*, <https://arxiv.org/abs/1708.02635>, 2 lutego 2018 r.

[32] D.C. Montgomery, *Statistical quality control*, Vol. 7, New York 2009, s. 179–213.

W ramach badań mających na celu znalezienie najlepszej metody detekcji anomalii w ruchu sieciowym przeprowadzane są testy trzech rodzajów prognozowania: modeli z rodziny ARIMA (ang. *Autoregressive integrated moving average*), modeli regresji oraz rekurencyjnych sieci neuronowych.

Modele ARIMA są szeroko wykorzystywane m.in. w predykcji zmiennych w ekonometrii. Metoda działa na stacjonarnych szeregach czasowych, choć w określonych przypadkach za pomocą wykorzystania metod dekompozycji trendu i sezonowości może pracować dla danych niestacjonarnych[33]. Za pomocą modeli ARIMA można przewidywać parametry ruchu sieci przemysłowej. Następnie, posiadając odpowiednio wytrenowany model, można porównywać prognozę dla zmiennej z rzeczywistymi parametrami ruchu, które przyjęła, i na tej podstawie określać, czy parametry przyjmują poprawne (typowe) dla siebie wartości, opierając się na zakresach ufności przyjętych dla modelu[34].

Metody regresji należą formalnie do metod nadzorowanego uczenia maszynowego. Istnieje jednak sposób na ich wykorzystanie w predykcji zmiennych. Dobrym tego przykładem jest użycie wektorów maszyn nośnych w odmianie regresywnej. Metoda SVR (ang. *Support Vector Regression*) może być zastosowana do przetwarzania danych o ciągłym charakterze i jest techniką niezależną od rozkładu zmiennych, które modeluje[35]. Dzięki temu ma duży potencjał jako metoda uczenia maszynowego, która pozwala na przewidywanie wartości zmiennych i detekcję anomalii w sieciach przemysłowych[36].

Rekurencyjne sieci neuronowe (ang. *Recurrent Neural Networks — RNN*) są jedną ze znanych architektur głębokiego uczenia maszynowego W przeciwieństwie do typowych sieci neuronowych pozwalają na wykrycie zależności dla zmiennych w czasie, wobec czego nadają się do operowania na szeregach czasowych i danych, w których kolejność ma znaczenie (np. w przetwarzaniu języka naturalnego, gdzie ważna jest kolejność wyrazów w zdaniu)[37]. Dodanie do RNN jednostek LSTM (ang. *Long Short-Term Memory*) zapewnia im lepszą pamięć lokalną dotyczącą zmiennych, co w przypadku tej metody usprawnia proces optymalizacji rozłożenia wag połączeń w sieci. Obecnie jest to najlepsza z dostępnych technik

[33] D. Asteriou, S.G. Hall, *ARIMA Models and the Box–Jenkins Methodology* [w:] ciż, *Applied Econometrics*, New York 2011, s. 265–286.

[34] Q. Yu, L. Jibin, L. Jiang, *An Improved ARIMA-Based Traffic Anomaly Detection Algorithm for Wireless Sensor Networks*, „International Journal of Distributed Sensor Networks" 2011, No. 12, s. 1–9.

[35] N.I. Sapankevych, R. Sankar, *Time Series Prediction Using Support Vector Machines: A Survey*, „*IEEE Computational Intelligence Magazine*" 2009, Vol. 4, No. 2, s. 24–38.

[36] A. Candelieri, *Clustering and Support Vector Regression for Water Demand Forecasting and Anomaly Detection*, „Water" 2017, Vol. 9(3), No. 224, s. 1–19

[37] A.F. *Gers, E. Schmidhuber, LSTM recurrent networks learn simple context-free and context-sensitive languages,* „IEEE Transactions on Neural Networks" 2001, Vol. 12(6), s. 1333–1340.

w obszarze uczenia maszynowego, która przy odpowiednim użyciu może okazać się bardzo wyrafinowaną metodą detekcji anomalii[38].

W głębokiej inspekcji pakietów przesyłanych w ramach komunikacji w sieci przemysłowej badane są m.in. metody detekcji anomalii dla sekwencji komunikatów oraz niespecyficzna dla protokołów głęboka inspekcja pakietów.

Z uwagi na to, że komunikacja w protokołach przemysłowych opiera się na wymianie informacji zdefiniowanej nie tylko przez ich treść, ale także przez ściśle określoną kolejność wysyłania wiadomości, badane są metody pozwalające na wykrycie mało prawdopodobnych sekwencji wymiany informacji, które powinny być traktowane jako anomalie. Do tego celu wykorzystywane są ukryte łańcuchy Markowa[39] oraz estymatory maksymalnej entropii i prawdopodobieństwa[40].

Zastosowana zostanie również bardziej ogólna metoda pozwalająca na wykrycie anomalii niezależnie od protokołu — autoenkodery. Są to niewielkie sieci neuronowe, które w oryginalnym zamyśle służą do kompresji danych. W praktyce dokonują ekstrakcji specyficznych cech dla danych wejściowych, jednocześnie tworząc ich ogólną reprezentację. Metoda pozwala na wprowadzenie nieliniowości do modelu[41]. Dzięki temu można będzie uzyskać informację, na ile dany pakiet różni się od poprzednio widzianych przez sieć. Istnieją praktyczne zastosowania tej techniki dla ruchu w sieci, np. klasyfikacja szyfrowanej komunikacji na podstawie zawartości pakietów[42]. W projekcie umożliwi to np. detekcję niektórych anomalii bez potrzeby dogłębnej znajomości szczegółów konfiguracji protokołu sieci przemysłowej dla pojedynczego wdrożenia czy sterownika.

Na poniższym schemacie przedstawiono przepływ informacji w ramach komponentu uczenia maszynowego.

---

[38] P. Malhotra i in., *Long Short Term Memory Networks for Anomaly Detection in Time Series* [w:] *ESANN 2015 proceedings, European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning*, Bruges 2015, s. 89–94.

[39] N. Gornitz, M. Braun, M. Kloft, *Hidden Markov Anomaly Detection* [w:] F. Bach, D. Blei (red.), *Proceedings of the 32nd International Conference on Machine Learning*, Lille 2015, Vol. 37, s. 1833–1842.

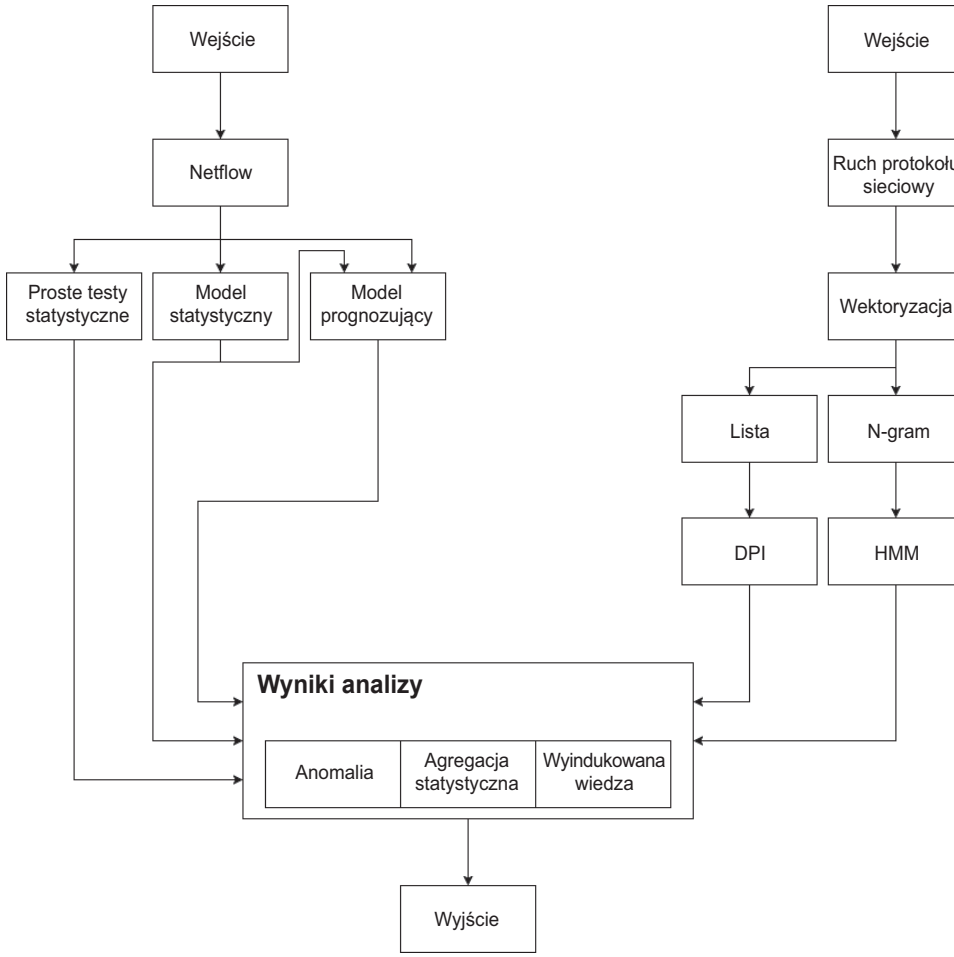
[40] A. Haque, A. DeLucia, E. Baseman, *Markov Chain Modeling for Anomaly Detection in High Performance Computing System Logs* [w:] *Proceedings of the Fourth International Workshop on HPC User Support Tools (HUST'17)*, New York 2017, s. 1–8.

[41] M. Sakurada, T. Yairi, *Anomaly Detection Using Autoencoders with Nonlinear Dimensionality Reduction* [w:] A. Rahman, J. Deng, J. Li (red.), *Proceedings of the MLSDA 2014 2nd Workshop on Machine Learning for Sensory Data Analysis (MLSDA'14)*, New York 2014, s. 4–11.

[42] J. Höchst i in., *Unsupervised Traffic Flow Classification Using a Neural Autoencoder*, Singapore 2017, s. 523–526.

Rysunek 2

Proces detekcji anomalii przez rozwiązanie SCADvance



Źródło: opracowanie własne

Poszczególne modele analityczne mogą potrzebować tych samych danych wejściowych w różnej formie, np. jako „surowe" pakiety lub w formie rekordów przepływów (ang. *netflow*s) do badania zmian w charakterystyce ruchu sieciowego. W zależności od protokołu, a nawet konkretnego wdrożenia, przydatność danego modelu może być znacząco różna. Do docelowego działania w ramach konkretnej IK wybierane będą ostatecznie modele najlepiej przystosowane do specyfiki wdrożenia. Wyjaśnia to potrzebę multiplikacji podmodułów odpowiedzialnych za uczenie maszynowe.

Wykorzystanie wyników dla ochrony infrastruktury krytycznej

Założenia projektu SCADvance wpisują się w następujące aspekty ochrony IK wspieranej przez rozwiązania ICT:
— gromadzenie danych z monitorowanych procesów lub obiektów (w tym wyselekcjonowanych danych pochodzących z monitorowanych systemów automatyki przemysłowej),
— automatyczne analizowanie zebranych danych w czasie rzeczywistym,
— przechowywanie i archiwizacja zgromadzonych danych w późniejszym terminie (również działania z zakresu informatyki śledczej — ang. *forensics*)[43].

Projekt SCADvance spełnia warunki opisane powyżej. Warstwa sprzętowa — sonda SCADA — fizycznie zabezpiecza sieć przemysłową przed zbyt daleko idącą ingerencją systemu w działanie sieci (właściwa reakcja może zostać uruchomiona tylko przez zaalarmowanego operatora oraz przy użyciu odrębnych narzędzi). Rozwiązanie stosuje również podejście zaawansowanego przetwarzania zdarzeń i udostępnia mechanizmy analityki Big Data przede wszystkim w odniesieniu do analizy śledczej po wykryciu incydentu w czasie rzeczywistym lub quasi-rzeczywistym (ang. *post mortem*). Dla potrzeb takiej analizy system gromadzi przez wskazany czas całość wygenerowanego ruchu sieciowego.

W ramach projektu SCADvance powstaje biblioteka modeli analitycznych, które będą ewaluowane i selekcjonowane przy okazji poszczególnych wdrożeń. Takie podejście pozwoli w maksymalnym możliwym stopniu uniezależnić się od szczególnej parametryzacji protokołów — unikalnej dla konkretnego wdrożenia. Pozyskani partnerzy wdrożeniowi wspomogą ewaluację wyników projektu w rzeczywistych sieciach automatyki przemysłowej.

Zakończenie

W artykule przedstawiono wybrane aspekty cyberbezpieczeństwa oraz metody zabezpieczenia IK z wykorzystaniem nowoczesnych technologii, m.in. analityki danych. Poznańskie Centrum Superkomputerowo-Sieciowe z sukcesami realizuje prace badawcze nie tylko wpisujące się w ogólne zapotrzebowanie rynku na zaawansowane systemy cyberbezpieczeństwa, ale również w szczegółowe wymagania — zdefiniowane dla tej klasy rozwiązań. Zdaniem autorów współpraca z polskimi jednostkami naukowo-badawczymi w celu podniesienia poziomu cyberbezpieczeństwa krajowej IK jest optymalna pod wieloma względami — w tym choćby w aspekcie możliwości pełnego zaufania w odniesieniu do wytworzonego kodu źródłowego.

Narodowy Program Ochrony Infrastruktury Krytycznej jasno wskazuje, że jednostki i środowisko naukowe są źródłem wiedzy w zakresie

[43] G. Abgarowicz i in., *Bezpieczeństwo infrastruktury krytycznej*..., wyd. cyt., s. 71.

opracowania narzędzi podnoszących efektywność działań w zakresie IK oraz stanowią wsparcie eksperckie — obejmuje ono m.in. prowadzenie badań naukowych i prac rozwojowych w celu określenia nowych technologii i metod analitycznych, które mogą być stosowane przez uczestników programu[44].

Rolę środowiska naukowego w podejmowaniu wyzwań związanych z cyberbezpieczeństwem podkreśla również Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Dokument stanowi, że w związku z radykalnymi zmianami technologicznymi zachodzi konieczność intensyfikacji działań badawczych i rozwojowych oraz wytwórczych w zakresie cyberbezpieczeństwa. W tym celu, wspólnie z Narodowym Centrum Badań i Rozwoju, uruchomiony ma zostać dedykowany program badawczy zmierzający do przygotowania i wdrożenia nowych metod ochrony przed zagrożeniami pochodzącymi z cyberprzestrzeni[45].

Warto również zauważyć, że jednym z celów Strategii na Rzecz Odpowiedzialnego Rozwoju jest trwały wzrost gospodarczy oparty coraz silniej o wiedzę, dane i doskonałość organizacyjną. Z kolei gospodarka oparta na wiedzy może istnieć dzięki współdziałaniu ośrodków naukowych oraz firm, które będą wdrażały nowe technologie[46].

Aktualne spektrum zagrożeń dla IK staje się coraz szersze i bardziej skomplikowane. Klasyczne systemy zabezpieczeń przestają wystarczać do ochrony przed zaawansowanymi atakami ukierunkowanymi. Do budowy kolejnej generacji systemów zaprzęga się rozwiązania analityczne wykorzystujące model Big Data czy analizę behawioralną. Rozwój innowacyjnych systemów zabezpieczeń polskiej IK związany jest z koniecznością wykorzystania potencjału polskiej nauki, co podkreślane jest przez dokumenty strategiczne związane z bezpieczeństwem cyberprzestrzeni, a IK w szczególności.

Słowa kluczowe: cyberbezpieczeństwo, infrastruktura krytyczna, SCADA, uczenie maszynowe, detekcja anomalii

Keywords: Cybersecurity, Critical Infrastructure, SCADA, Machine Learning, Anomaly Detection

Streszczenie: W dobie zagrożeń asymetrycznych cyberbezpieczeństwo infrastruktury krytycznej staje się poważną kwestią, a jednocześnie wyzwaniem dla twórców systemów zabezpieczeń. W niniejszym artykule przedstawiono

Summary: In the world of asymmetric threats, cybersecurity of critical infrastructure has become a serious facet as well as creates a challenge for creators of protection solutions. In this paper certain factors escalating difficulties of

[44] Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej — tekst jednolity*, <https://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-2015-Dokument-G%C5%82%C3%B3wny-tekst-jednolity.pdf>, 3 kwietnia 2018 r.

[45] Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, Warszawa 2017, s. 21–22.

[46] Ministerstwo Inwestycji i Rozwoju, *Strategia na Rzecz Odpowiedzialnego Rozwoju*, <https://www.miir.gov.pl/media/48672/SOR.pdf>, 4 kwietnia 2018 r.

czynniki eskalujące poziom trudności detekcji zaawansowanych zagrożeń, a także, na przykładzie dwóch projektów naukowo-badawczych, opisano realizowane przez Poznańskie Centrum Superkomputerowo-Sieciowe (PCSS) prace podejmujące to wyzwanie. Na przykładzie krajowego projektu SCADvance opisano zastosowanie algorytmów uczenia maszynowego do wykrywania zagrożeń w protokołach sieci przemysłowych. Wskazano również na rolę, jaką środowisko naukowe jest w stanie odegrać w tworzeniu innowacyjnych systemów zabezpieczeń infrastruktury krytycznej, a także na konieczność zastosowania rozwiązań tej klasy dla właściwej ochrony wrażliwych sieci teleinformatycznych.

advanced cyberattacks detection have been defined. Research led by Poznań Supercomputing and Networking Center (PSNC) oriented for that purpose have been also described, exemplified with SCADvance research project, concerning application of machine learning algorithms to detect threats in industrial network protocols. An important contribution of the research community in building advanced threat detection systems is emphasized, as well as the necessity of applying solutions of this class for sufficient protection of sensitive communication networks.