Sztuczna inteligencja

**Czy da się opisać ludzką inteligencję wystarczająco precyzyjnie, aby można było ją naśladować przy użyciu maszyn? To pytanie nadal stanowi kość niezgody wśród naukowców. Naukowcy próbujący stworzyć sztuczną inteligencję stosują różne podejścia, wielu jednak sądzi, że kluczem do sukcesu są sztuczne sieci neuronowe. Jak na razie żadne urządzenie zawierające sztuczną inteligencję nie przyszło testu Turinga. Według sławnego brytyjskiego informatyka Alana Turinga, maszyna może zostać uznana za inteligentną, jeżeli użytkownik nie jest w stanie rozróżnić, czy ma do czynienia z maszyną czy z innym człowiekiem. Jednym z możliwych obszarów zastosowań całkowicie autonomicznej sztucznej inteligencji jest wirusologia komputerowa oraz rozwój systemów do zdalnego leczenia zainfekowanych komputerów.**

Głównym zadaniem stojącym dzisiaj przed naukowcami zajmującymi się sztuczną inteligencją jest stworzenie autonomicznego urządzenia, które potrafi uczyć się, podejmować inteligentne decyzje oraz modyfikować własne zachowanie w zależności od zewnętrznych bodźców. Stworzenie takich wysoko wyspecjalizowanych systemów jest możliwe, podobnie jak prawdopodobne jest zbudowanie bardziej uniwersalnych i złożonych urządzeń opartych na sztucznej inteligencji, jednak takie systemy zawsze opierają się na doświadczeniu i wiedzy człowieka w postaci wzorców, reguł i algorytmów zachowania.

Dlaczego tak trudno stworzyć autonomiczną sztuczną inteligencję? Dlatego, że maszyna nie posiada typowo ludzkich cech, takich jak świadomość, intuicja, umiejętność rozróżniania między rzeczami ważnymi i tymi mniej istotnymi - i co najważniejsze – chęć zdobywania nowej wiedzy. Wszystkie te cechy pozwalają człowiekowi rozwiązywać problemy, nawet gdy nie są one linearne. Wykonanie jakiegokolwiek działania przez sztuczną inteligencję wymaga obecnie algorytmów stworzonych przez człowieka. Mimo to, naukowcy wciąż próbują stworzyć prawdziwe sztuczną inteligencję i niekiedy odnoszą pewne sukcesy.

**Koszty nieautomatycznego przetwarzania**

Proces wykrywania szkodliwego oprogramowania i przywracania normalnych parametrów operacyjnych na komputerze składa się z trzech głównych kroków. Nie ma tu znaczenia, kto lub co podejmuje te kroki: człowiek czy maszyna. Pierwszy krok obejmuje gromadzenie obiektywnych danych o badanym komputerze oraz działających na nim programach. Ten krok najlepiej przeprowadzić przy użyciu szybkiego, automatycznego sprzętu, który potrafi generować raporty nadające się do przetwarzania automatycznego oraz działać bez interwencji człowieka.

W drugim kroku zebrane dane są poddawane szczegółowej analizie. Na przykład, jeżeli raport zawiera informację o wykryciu podejrzanego obiektu, taki obiekt należy poddać kwarantannie i dokładnej analizie w celu określenia, jakie stanowi zagrożenie, a następnie trzeba podjąć decyzję odnośnie dalszych działań.

Trzeci krok stanowi rzeczywistą procedurę rozwiązania problemu, dla której można wykorzystać specjalny język skryptowy. Zawiera ona polecenia niezbędne do usunięcia wszelkich szkodliwych plików oraz przywrócenia prawidłowych parametrów operacyjnych komputera.

Jeszcze kilka lat temu kroki 2 i 3 były wykonywane jedynie przez analityków firm bezpieczeństwa IT oraz ekspertów działających na wyspecjalizowanych forach niemal bez użycia jakiejkolwiek automatyzacji. Jednak wraz ze wzrostem liczby użytkowników padających ofiarą szkodliwego oprogramowania, a tym samym potrzebujących specjalistycznej pomocy, pojawiło się wiele problemów:

* Jeżeli protokoły i pliki kwarantanny są przetwarzane ręcznie, analityk wirusów otrzymuje ogromne ilości nieustannie zmieniających się informacji, które wymagają zintegrowania i pełnego zrozumienia – taki proces nie może być szybki.
* Człowiek posiada naturalne ograniczenia psychiczne i fizjologiczne. Specjalista może zmęczyć się i popełnić błąd; im bardziej złożone zadanie, tym większe prawdopodobieństwo popełnienia błędu. Na przykład przeciążony pracą ekspert od szkodliwego oprogramowania może pominąć szkodliwy program lub usunąć nieszkodliwą aplikację.
* Analiza plików umieszczonych w kwarantannie jest bardzo czasochłonną operacją, ponieważ ekspert musi przeanalizować unikatowe cechy każdej próbki – tj. gdzie i w jaki sposób pojawiła się i co jest w niej podejrzanego.

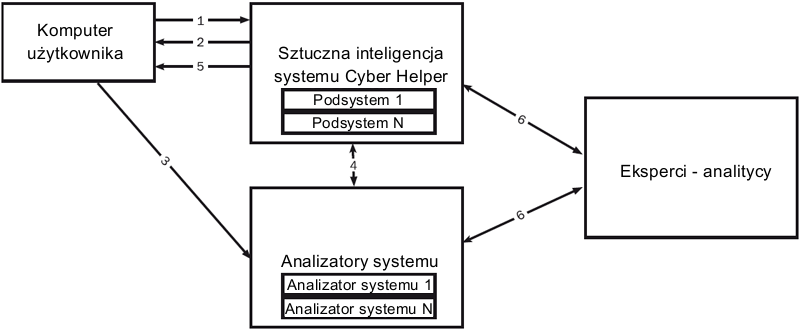
Jedynym rozwiązaniem tych problemów jest całkowita automatyzacja analizy oraz leczenia szkodliwego oprogramowania, jednak dotychczasowe próby wykorzystujące różne algorytmy nie przyniosły pozytywnych rezultatów. Głównym powodem tych niepowodzeń jest nieustanna ewolucja szkodliwego oprogramowania oraz fakt, że każdego dnia w Internecie pojawiają się dziesiątki nowych szkodliwych programów wykorzystujących coraz bardziej wyrafinowane metody osadzania się i ukrywania. Dlatego algorytmy wykrywania muszą być niezwykle złożone. Sprawę komplikuje ponadto fakt, że algorytmy te bardzo szybko dezaktualizują się - należy je nieustannie aktualizować i usuwać z nich błędy. Kolejnym problemem jest to, że skuteczność każdego algorytmu ograniczają umiejętności jego twórców.

Nieco skuteczniejsze wydaje się wykorzystanie do “łapania wirusów” systemów eksperckich. Jednak twórcy antywirusowych systemów eksperckich borykają się z podobnymi problemami do tych wymienionych wyżej – skuteczność takiego systemu zależy od jakości wykorzystywanych przez niego reguł i baz wiedzy. Ponadto, bazy wiedzy muszą być nieustannie aktualizowane, co wymaga inwestycji w zasoby ludzkie.

**Ogólne zasady działania systemu Cyber Helper**

Mimo trudności, z upływem czasu eksperymenty prowadzone na omawianym polu dały pewne pozytywne wyniki. Przykładem jest stworzenie systemu Cyber Helper, który stanowi udany krok w kierunku wykorzystywania w walce ze szkodliwym oprogramowaniem prawdziwie autonomicznej sztucznej inteligencji. Większość autonomicznych podsystemów Cyber Helpera potrafi zsynchronizować się, wymieniać dane i współdziałać ze sobą, jak gdyby były jednością. Naturalnie zawierają one pewne “twarde” algorytmy i reguły - tak jak konwencjonalne programy - jednak w większości działają z wykorzystaniem logiki rozmytej i w trakcie rozwiązywania różnych zadań niezależnie definiują swoje zachowanie.

W samym sercu systemu Cyber Helper znajduje się narzędzie o nazwie AVZ, które zostało stworzone przez autora tego artykułu w 2004 roku. Celem AVZ jest automatyczne gromadzenie danych z potencjalnie zainfekowanych komputerów jak również próbek szkodliwego oprogramowania i przechowywanie ich w postaci nadającej się do przetwarzania automatycznego do użytku innych podsystemów. AVZ tworzy raporty w formacie HTML przeznaczone do analizy przez człowieka oraz w formacie XML - do analizy maszynowej. Od roku 2008 główny program AVZ jest integrowany do rozwiązań antywirusowych firmy Kaspersky Lab.

[](http://www.elektroonline.pl/img/media/4177)  
Ogólny algorytm działania systemu Cyber Helper – kroki 1-6

Algorytm działania systemu składa się z sześciu kroków. W pierwszym kroku główny program AVZ wykonuje skanowanie antywirusowe zainfekowanego komputera, a uzyskane wyniki w formacie XML przesyła do innych podsystemów Cyber Helpera w celu analizy.

## Trudności implementacji

Eksperci przetwarzający protokoły i poddane kwarantannie mogą popełniać błędy lub wykonywać działania, których nie można wyjaśnić logicznie z perspektywy maszyny. Oto typowy przykład: jeżeli specjalista widzi w protokole nieznany plik o nazwie %System32%\ntos.exe, który posiada cechy szkodliwego oprogramowania, usuwa go bez dalszej analizy czy poddawania go kwarantannie, opierając się na swoim doświadczeniu oraz intuicji. Dlatego szczegóły działań wykonywanych przez specjalistów oraz sposób, w jaki doszli do swoich wniosków, nie zawsze można bezpośrednio przełożyć na postać umożliwiającą uczenie maszyny. Informacje dotyczące leczenia często mogą być niekompletne lub sprzeczne. Na przykład, przed poproszeniem o pomoc eksperta użytkownik mógł próbować samodzielnie naprawić problem na swoim komputerze i usunął tylko część szkodliwego programu – przywracając pliki zainfekowanego programu bez wyczyszczenia rejestru. Trzeci typowy problem: podczas procedury analizy protokołu dostępne są tylko metadane z podejrzanego obiektu, natomiast po analizie pliku poddanego kwarantannie - tylko informacje początkowe o podejrzanym obiekcie. Następnie przeprowadzana jest kategoryzacja obiektu – albo jest on szkodliwy, albo “czysty”. Takie informacje są zwykle dostępne dopiero po wielokrotnym uściśleniu i po długim czasie – wynoszącym od kilku minut do kilku miesięcy. Proces definiowana może odbywać się zarówno zewnętrznie, w laboratorium usług analitycznych, jak i wewnątrz własnych podsystemów Cyber Helpera.

Oto typowy przykład: analizator sprawdza plik, ale nie znajduje w jego zachowaniu nic groźnego i przekazuje tę informację do systemu Cyber Helper. Po pewnym czasie analizator zostaje udoskonalony i powtórnie przeprowadza analizę badanego wcześniej podejrzanego pliku, z tym że tym razem wydaje inny werdykt. Podobny problem może dotyczyć wniosków wyciąganych przez wyspecjalizowanego analityka wirusów dla programów, których klasyfikacja jest problematyczna, na przykład programów do zdalnych systemów zarządzania lub narzędzi zacierających ślady użytkownika – ich klasyfikacja może zmienić się po opublikowaniu kolejnej wersji. Ze względu na wspomnianą wyżej właściwość – zmienność i niejednoznaczność parametrów analizowanych programów, wszelkie decyzje podejmowane przez Cyber Helper opierają się na ponad pięćdziesięciu niezależnych analizach.

Na podstawie dostępnych informacji analizator Cyber Helper dostarcza wiele hipotez odnośnie tego, który z obiektów znajdujących się w protokole może stanowić zagrożenie, a który można dodać do bazy “czystych” plików. Na podstawie tych hipotez AVZ automatycznie pisze skrypty odpowiadające za umieszczanie w kwarantannie podejrzanych obiektów. Następnie skrypt jest przesyłany do maszyny użytkownika w celu wykonania. (Krok 2 ogólnego algorytmu działania systemu Cyber Helper).

Na etapie pisania skryptu inteligentny system może wykryć dane, które są wyraźnie szkodliwe. W takim przypadku skrypt może włączyć polecenie usunięcia znanych szkodliwych programów lub odwołać się do specjalnych procedur cofnięcia szkody w systemu. Takie sytuacje mają miejsce dość często i wynikają z tego, że Cyber Helper jednocześnie przetwarza setki żądań; jest to typowe w sytuacjach, gdy kilku użytkowników zostało zainfekowanych tym samym szkodnikiem i ich maszyny proszą o pomoc. Po otrzymaniu i przeanalizowaniu wymaganych próbek z maszyny jednego z takich użytkowników Cyber Helper może dostarczyć innym użytkownikom skrypty leczenia, całkowicie pomijając etap kwarantanny, a tym samym oszczędzając czas użytkownika i zmniejszając ruch danych. Obiekty otrzymane od użytkownika są analizowane pod kontrolą systemu Cyber Helper, a wyniki tej analizy, niezależnie od tego, jakie są, zasilają jego bazę wiedzy. W ten sposób inteligentna maszyna może sprawdzić dowolne hipotezy sformułowane w kroku 1 ogólnego algorytmu działania, potwierdzając lub odrzucając ich wynik.

**Techniczne podsystemy Cyber Helpera**

Główne podsystemy Cyber Helpera to autonomiczne jednostki analizujące pliki programów pod względem zawartości i zachowania. Dzięki nim Cyber Helper może analizować szkodliwe programy oraz uczyć się na wynikach swoich działań. Jeżeli analiza wyraźnie potwierdza, że dany obiekt jest szkodliwy, jest on przesyłany do laboratorium antywirusowego z mocnym zaleceniem umieszczenia go w antywirusowej bazie danych; następnie tworzony jest skrypt leczenia dla użytkownika (krok 5 ogólnego algorytmu). Należy zauważyć, że pomimo analizy obiektu Cyber Helper nie zawsze jest w stanie podjąć kategoryczną decyzję odnośnie szkodliwości obiektu. W takiej sytuacji wszystkie zebrane dane początkowe i wyniki są przekazywane ekspertowi w celu analizy (krok 6). Następnie ekspert dostarcza odpowiednie rozwiązanie. Cyber Helper nie bierze udziału w tym procesie, nadal jednak analizuje otrzymane dane i protokoły, generując raporty dla eksperta, tym samym wykonując lwią część jego pracy.

Obecnie Cyber Helper jest zintegrowany z portalem antywirusowym http://virusinfo.info i stanowi podstawę eksperymentalnego systemu 911 http://virusinfo.info/911test/. W “systemie 911” Cyber Helper komunikuje się bezpośrednio z użytkownikiem: żądając protokołów, analizując je, pisząc skrypty skanowania wstępnego oraz przeprowadzenia analizy plików poddanych kwarantannie. Zgodne z wynikami swojej analizy maszyna może przeprowadzić leczenie zainfekowanego komputera. Co więcej, Cyber Helper pomaga ekspertom w ich pracy, znajdując i eliminując wszelkie niebezpieczne błędy, przeprowadzając wstępne analizy wszystkich plików umieszczonych w kwarantannie przez ekspertów oraz przetwarzając dane zawarte w kwarantannie przed dodaniem ich do bazy „czystych” plików. Technologia, na której opiera się Cyber Helper, jak również jej zasada działania są chronione patentami firmy Kaspersky Lab.

## Wnioski

Współczesne szkodliwe programy działają i rozprzestrzeniają się w niezwykle szybkim tempie. Natychmiastowa reakcja na tego typu programy wymaga inteligentnego przetwarzania dużej ilości niestandardowych danych. Sztuczna inteligencja idealnie nadaje się do tego zadania, ponieważ potrafi przetwarzać dane o wiele szybciej niż człowiek. Cyber Helper to efekt jednej z niewielu udanych prób przybliżenia się do celu, jakim jest stworzenie autonomicznej sztucznej inteligencji. Jako inteligentny twór, Cyber Helper jest zdolny do samodzielnego uczenia się i niezależnego definiowania swoich działań. Analitycy wirusów i inteligentne maszyny rewelacyjnie dopełniają się – dzięki współpracy działają efektywniej i zapewniają użytkownikom większą ochronę.